Evil Eye

London-style video surveillance systems are planned for a number of U.S. cities. Their effectiveness is not clear, but their threat to our constitutional rights is.

By William S. Sessions

The benefits of video surveillance were revealed to the world after the London bombings in July 2005. Within days authorities had identified the bombers, retraced their paths, and detained suspected accomplices, thanks in part to footage from the world’s largest and most elaborate public video surveillance system.

Thus, it is tempting to believe that surveillance systems can prevent terrorism, especially when terrorists have access to the latest technologies for the planning and implementation of attacks. But the same attack also revealed the limitations of video surveillance. The system in London failed to prevent the attacks in the first place. The British agency responsible for internal affairs spends nearly three-quarters of its crime prevention budget on the administration, operation, and maintenance of the cameras—one for every 14 inhabitants of the United Kingdom—despite internal research concluding that they have had “no effect on violent crimes.”

In addition, and perhaps more importantly, pervasive video surveillance threatens fundamental tenets of our democratic society: individual rights, autonomy, and freedom from government intrusion.

Nonetheless, communities all across the country are installing video surveillance systems. New York has announced a plan to construct a network that would rival that of London. Dubbed the Lower Manhattan Security Initiative, the plan would add more than 3,000 cameras, at a cost of $90 million, to the existing network of 4,200 public and private security cameras in the city. Some experts are calling it the most extensive urban counterterrorism operation in the world. Other cities, such as Baltimore and Newport, Rhode Island, have installed similar, albeit smaller, camera networks. Mayor Cory Booker of Newark recently announced a plan—given the Orwellian moniker “Community Eye”—to install more than 120 public security cameras in the city as a response to a series of gruesome execution-style murders this past August. The program calls for a concentration of 50 surveillance cameras, equipped with “gunshot detection technology,” installed over an area covering seven square miles.

The rapid expansion of public video surveillance has been energized and facilitated by an influx of federal antiterrorism grants from the U.S. Department of Homeland Security. More than $1.4 billion will be made available for antiterrorism projects this year. This, in turn, has opened up the market for video surveillance systems, as corporations compete for homeland security funds. Some of the most powerful new technologies are a product of competition among these providers of video surveillance services. The new technologies make it clear that video surveillance systems could quickly become a standard and permanent feature of America’s public space.

There are a number of qualitative differences between today’s complex video surveillance systems and the simple closed-circuit television systems of the past. Early closed-circuit cameras could “see” about as far as a human eye, but only within a narrow visual field. Modern cameras can pan and tilt in almost any direction chosen. Optical and digital magnification can greatly improve the detail captured. Other observation technology allows modern cameras to create usable images in very low light, and infrared technology can render useful images with no visible light whatsoever.

Once the video is captured, it can be manipulated and indexed. A database of video footage could be searched for specific individuals or activity matching a specified pattern, or used to create a “digital dossier” about an individual. Networks can also track one person’s movement across multiple cameras. Today’s systems can provide a unified, virtual-reality perspective of a monitored area, allowing an operator to automatically follow an object as it moves from camera to camera.
it moves from camera view to camera view. Finally, facial recognition systems are steadily improving in quality and may one day be used to quickly and cheaply create a catalog of an individual’s every movement.

Does video surveillance threaten constitutional values? At a minimum, unchecked video surveillance endangers individual privacy rights, or what Justice Louis Brandeis famously called “the right to be left alone.” As a practical matter, people in public spaces routinely engage in activities that, though legal, are ones that they expect and desire to keep private. A compromise has developed between the private and the public that permits the activities to occur while still allowing individuals to enjoy a zone of privacy. But the law has not kept pace with technology. Recent technological advances in the fields of video capture and image processing have disrupted a tenacious compromise.

In addition, the U.S. Supreme Court has recognized that an individual is free to remain anonymous while exercising certain constitutionally protected rights in public places. But any expectation of anonymity is destroyed when video surveillance systems capture footage of private activities that require the use of public spaces. Entering a building to attend an Alcoholics Anonymous meeting, visit a psychiatrist, or seek treatment at a fertility clinic might be made dependent on a person’s willingness to sacrifice anonymity.

Surveillance systems can impair rights to free association and expression. For example, the Supreme Court has held that political or religious expression is not “free” if speakers are required to disclose their identities, and thus individuals may not be required to identify themselves before distributing campaign literature. Similarly, political and advocacy organizations like the NAACP cannot be compelled to disclose their membership lists. A pervasive system of cameras that tracks individuals’ movements throughout the community would eliminate this ability to freely engage in these activities.

Finally, without proper restrictions on their use and measures that ensure accountability, video surveillance systems are prone to troubling abuse. The vast potential for discriminatory use of video surveillance systems against certain classes of people—whether religious, racial, or ethnic—threatens due process and equal protection rights.

A significant shift in our understanding of the technical and legal freedoms and restrictions that come with video surveillance is needed to protect these constitutional rights. What is urgently required is a set of core principles governing the creation, design, and use of surveillance systems. These principles should be followed by each jurisdiction that wants to implement video surveillance.

The Constitution Project’s Liberty and Security Committee—a bipartisan, blue-ribbon coalition of political leaders, policy experts, and legal scholars, of which I am a member—has issued “Guidelines for Public Video Surveillance,” which provides specific, carefully defined policy recommendations for cities considering such systems. These guidelines assist communities both in determining whether a system is needed and, if so, in designing and operating that system. The guidelines encourage public participation at every stage; an elected or otherwise publicly accountable body should undertake the analysis and the deliberations of this body should be open to public review and commentary.

If the need for rapid deployment or secrecy makes public participation impossible, a city could rely on judicial approval processes. This more streamlined approach would bypass public participation but still require judicial approval after a showing that the proposed system will be temporary and that it requires speed or secrecy to be effective.

The first question any community must answer is one of need. Many communities will find that cameras are unlikely to prevent a devastating terrorist attack, and that petty crime is more easily checked by less-expensive and less-intrusive measures, such as installing street lights or hiring more patrol officers. Camera networks are expensive to install, and their continued operation and maintenance can also be costly. Their operation diverts precious law enforcement dollars and officers from other duties, in some cases leaving a community more exposed to the very crimes it sought to prevent.

If a community concludes that cameras can complement and improve its existing security efforts, that community should consider how best to avoid impacting residents’ civil liberties. It is critical that communities engage in a “civil liberties impact assessment” before the first camera is installed. This assessment will not only ensure that civil liberties are protected, it will help lessen the risk that the intrusive nature of a new technology will give rise to costly litigation.

System designers should make every effort to limit the scale of the network. First, the system’s scope and the geographic territory covered should be no greater than necessary. The ability to observe unnecessary areas, such as the windows of private residences, should be minimized. Also, the cameras should be equipped with facial recognition technology.

Second, access to footage should be limited. Regulations should be established to limit both retention of and access to the data. If footage is retained beyond an initial period needed for routine review, law enforcement should be required to obtain a warrant for the use of such “archival” footage, so that this retention exception does not become the rule. Access limits can be achieved through the use of encryption technologies that protect against unauthorized access and digital watermarks that clearly show when and where records were accessed. Data sharing should also be limited.

Third, communities should develop procedures to protect the identities of individuals whose images are captured on video surveillance footage. Data sharing, taking place outside of the system’s original purpose, should in most cases require the consent of individuals who are identified. Injured parties could also be provided with a private right of action to bring suit against law enforcement officials who abuse the system.

No matter how much time and diligent effort goes into the creation and design of the system, some abuses are bound to occur, even under the watch of well-intentioned officers. An effective regulatory framework will reduce the potential for misuse of the system, and accountability measures will ensure that community residents have some recourse if their rights are violated.

American cities, large and small, are grappling with post–9/11 security threats and with rapidly evolving new technologies. But in their attempts to combat crime and the threat of terrorism, local governments should not move too quickly. The law has lagged far behind the available technology. Lawmakers need to be aware that what they can do differs from what they should do. They should act in a way that preserves liberty while maximizing security. Liberty is as essential to security as security is to liberty. Public video surveillance systems only preserve both when they are well regulated and well planned.

William S. Sessions was director of the Federal Bureau of Investigation from 1987 to 1993. Before that, he was the U.S. attorney and the chief U.S. district court judge in the Western District of Texas. He is currently a partner at Holland & Knight in Washington, DC.