

Special Report

Automating camera surveillance for social control and military domination

By Andrew Kalukin

Online Journal Contributing Writer

April 29, 2005—Though some organizations have objected to video surveillance of cities and borders, the public is less aware that recent computer vision innovations are making it possible to data mine surreptitiously acquired movie data in possible defiance of the Fourth Amendment.

The United States government has lavished generous funding upon video surveillance technology in hopes of revolutionary advances in data mining and robotic vision that would allow nationwide surveillance of public areas. Defense industries attempt to apply such technology to autonomous, robotic combat vehicles that can fight “bloodless” wars, ostensibly sparing the lives of American soldiers.

Controversial programs such as the Pentagon’s Total Information Awareness program were renamed to escape the scrutiny of Congress and the public. Though the public alarm generated by 9/11 and the USA Patriot Act accelerated the implementation of surveillance technologies such as face recognition, research and development in automated video detection has spanned several decades.

Video surveillance technology and automated face recognition are already in place in major cities in the United States and Europe, sometimes with the approval of residents who have been induced to fear terrorism and crime more than surveillance. The obsession with surveillance has been demonstrated recently by the vigilantism of the Minutemen and the American Border Patrol, self-appointed border patrol agents who use, among other devices, cameras mounted on unmanned aerial vehicles (UAVs) to detect illegal immigrants from Mexico.

To a casual observer, surveillance cameras resemble lampposts. Some of the cameras have a 360° view and magnify by a factor of 10-17 compared to human sight at that range [1]. Some are equipped with night vision; they can zoom in on a target well enough to read text on a written page or look into a building.

In Washington, D.C., for example, most are placed at locations that would not come to mind as primary terrorist targets: Smithsonian Castle, L’Enfant Plaza, the U.S. Department of Labor, Dupont Circle, Union Station, Wisconsin Ave., the Old Post Office, the Banana Republic in Georgetown. Though the targets they view may not stand out as particularly vulnerable to terrorism, the cameras are placed strategically for the purpose of monitoring demonstrations and protests—one of the first occasions for their use was a demonstration in April 2000, against the World Bank and International Monetary Fund. Supplemental data from the U.S. Park police monitoring demonstrations by helicopter are sent as digital feed to the Metropolitan Police Department. The D.C. police, the FBI, the Secret Service, and the D.C. school system agreed to pool data together as needed [2]. Though the police have stated there are only a dozen cameras, these cameras can link to about a thousand other government cameras to make up a network of equipment that might be found in a NASA or defense command center [3].

Similar systems exist in other cities for the same purpose. During antiwar protests in Boston at the 2004 Democratic National Convention, the police informed the media that camera systems would be used to guard against acts of terrorism [4]. According to the antiwar organization A.N.S.W.E.R. (Act Now to Stop

War and End Racism), photographs of protesters from past marches were circulated to bus drivers and other mass transit employees, to train the employees to recognize “terrorists.” In Manhattan, a person walking on a street is always in view of at least one of 2,400 cameras [5]. Chicago officials plan to install by 2006 a highly advanced system of video surveillance that will alert the police to “suspicious” behavior: wandering aimlessly in circles, lingering outside a public building, or pulling over on a highway [6].

In reaction, privacy advocates who view these surveillance measures with alarm have begun to publish the locations of surveillance devices in major American cities, to allow others who object to the technology to chart surveillance-free paths through the streets. Even if someone were willing to take this precaution, there is no guarantee against hidden or fake cameras unaccounted for in planning the route.

The privacy issues surrounding CCTV become more complicated when computer vision technology is applied to surveillance. A controversy resulted in 2001 when authorities used face recognition technology and CCTV at a Tampa Bay Superbowl game to search for criminals and terrorists [7]. The action led to 19 arrests, all of them for petty crimes, with no record of whether these arrests were legitimate. The ensuing public furor led several legislators, such as Dick Armey, to propose laws for protecting privacy and regulating the use of biometric technology. Recent mass breaches of sensitive identification data by large information brokers such as ChoicePoint and LexisNexis imply possible serious compromises in future handling of surveillance data.

When the results of video searches are combined with other existing databases, powerful methods of identification and tracking become possible. Unique body marks make identification much easier. In Fort Worth, Texas, police can track gang members by applying a software package called “GangNet” [8]. By typing a description of tattoos into the database, the software can produce pictures of members wearing those tattoos; similar searches can be performed on nicknames, vehicle numbers, telephone numbers, or partial license plate numbers. Salinas, California, received federal funding for a Geographic Information System to carry out crime tracking of gangs [9]. In Manalapan, Florida—one of the nation’s wealthiest cities—cameras and computers have been set up to run background checks on every car and driver that enters [10]. The system alerts a 911 dispatcher if the car is stolen or the driver is suspected of a crime. Infrared cameras record each car’s license tag number, and other cameras photograph the driver.

Sensor mobility adds another dimension. In 2003, Ohio transportation officials began testing the use of unpowered aircraft equipped with video, infrared cameras, and other sensors, to monitor traffic jams [11]. The information from aerial monitoring is intended to help police looking for the best route to an accident scene, as well as traffic planners, emergency workers, truck companies and commuters. Some of the planes—“drones”—are as small as model aircraft.

The military can use drones to send back real-time images of battle to commanders. In November 2003, the CIA used a drone to fire a missile into a car containing six alleged al-Qaida members. Unmanned aerial vehicles—UAVs—have attacked high-priority targets in Afghanistan and Iraq [12].

In December 2002, Senate Armed Services Committee Chairman John Warner (R, VA) indicated interest in using drones for homeland security [13]. In January of 2003, as a cost-saving measure, a US Congressional Research Service report suggested replacing manned fighters flying combat air patrols (CAP) over US cities with UAVs armed with air-to-air missiles. It is unclear whether the FAA would have authority over the UAVs in such a program. Furthermore the UAVs may be too small to be seen and fly too low to be detected by radar; the possible use of UAVs to deliver biological and chemical attacks has been a concern of the federal government [14].

Though the cameras used in unmanned aircraft have been remotely piloted vehicles (RPVs) unequipped with artificial intelligence processing, efforts to develop robotic autonomous vehicles are being funded by DARPA [15]. The Future Combat Systems program of the army advertises as one of its missions the development of Reconnaissance and Surveillance Vehicles (RSVs) supporting advanced sensors that detect, track, locate, classify, and identify targets under all climatic conditions, day or night.

Military and local law enforcement agencies already use video surveillance to automate threat response. In Broward County, Florida, Port Everglades selected ObjectVideo VEW software to protect its perimeter [16]. The software contains a tripwire feature that allows security personnel to create virtual perimeters on land and water by drawing a box on a digital view of what the camera is observing. Unknown people or vehicles crossing the tripwire boundaries signal an alert.

Archival video data are vulnerable to the same trends in industry and government that have led to information being sold as a commodity. Information about individuals is sold and traded routinely for marketing, charity solicitations, and political polling. Individuals may find more difficulty controlling the distribution of archived surveillance imagery, where the data are more likely to be collected surreptitiously. The breakdown of privacy in the trade of personal information already makes it possible for government agencies, such as the FBI, to bypass the government ban against information collection for people who are not targets of investigation, by simply accessing personal information that is already commercially available.

Some of the controversies of video surveillance came to public attention during the congressional discussion of the proposed Total Information Awareness (TIA) research programs of the Pentagon. Several research programs in TIA exploited video pattern recognition. HumanID included research projects to recognize humans from a distance based on face and gait recognition, along with other biometric tools. Though public outcry caused the TIA budget to be canceled by Congress in September 2003, some of the programs continued under other cover, such as Novel Intelligence from Massive Data (NIMD), Non-Obvious Relationship Awareness (NORA), Adaptive Concept Understanding from Modeled Enterprise Networks (ACUMEN), Computer-Assisted Passenger Prescreening System (CAPPS II), and Multi-state Anti-Terrorism Information Exchange (MATRIX).

Among the pattern matching efforts was a project known as Video Analysis and Content Exploitation (VACE). The goal of VACE was automatic content detection and recognition in “video scenes of various indoor and outdoor activities involving people, meetings, and vehicles, and TV news broadcasts,” according to the Advanced Research and Development Activity (ARDA) website. Research goals included recognition of people, event detection and understanding, video query, multi-modal video data mining, and object identification from motion. The VACE solicitations have closed, but as of December 2003, plans for workshops in VACE and other programs were still on the calendar for 2004.

Another military project for widespread video collection was offered as a DARPA BAA solicitation in May 2003—Combat zones That See (CTS). The goal of CTS is to develop video understanding of multiple data feeds arriving from many sources, to support military operations in urban terrain. The military is interested in tracking vehicles moving from one camera location to another. It is easy to see that the same techniques will be useful for tracking individuals walking across a city.

The ability to extract information from video images is so widely sought in the scientific community that the complete discontinuation of funding for similar programs seems unimaginable. The National Geospatial-Intelligence Agency has plans to post solicitations for geospatial information visualization and to award \$2.5 million in FY05 and FY06.

Military applications of pattern recognition and video data mining continue to be developed by means of Department of Defense solicitations to contractors in the form of BAA, SBIR, and STTR awards. These programs include efforts at automating algorithms for detecting human intentions in subjects appearing in video films, for distinguishing decoys from targets, and for synchronizing many UAVs to carry out simultaneous reconnaissance and attack.

It is possible that in the future, covert or privatized TIA-like programs may escape the scrutiny of Congress. It also seems certain that computer vision will find increasing applications in autonomous vehicles, and that efforts will be made to find the limits in the abilities of robotic devices to carry out automated warfare.

Though video surveillance is a passive activity, the data mining of video records to profile individuals is surreptitiously invasive. Given the difficulty of detecting video surveillance systems hidden on the ground or in the air, it would be difficult to enforce restraints against misuse of such data by either private agents or governments. Most cameras and UAVs are invisible to casual observers. Though the components of surveillance equipment and software are cheap, the infrastructure to support exchanges of information across many databases and networks could be afforded only by large corporations or government institutions—this implies a potentially asymmetrical situation in which surveillance becomes a weapon of class warfare [17]. Hierarchies of privilege favoring race or class are built implicitly into existing surveillance systems—for example, homeless residents of a city are more often targeted by video surveillance systems than are other citizens.

Recent developments in computer vision, robotics, and pattern matching increase the possibility of drastic social transformations. The application of data mining methods to massive video data sets enables a sufficiently organized power to outmatch humans in carrying out surveillance. Though the robot soldier and the robot policeman are not yet reality, present technological achievements can lead to this future possibility.

In case these apprehensions seem too dire, it is worth remembering how easily other invasions of privacy such as drug testing have come to be accepted generally, even when they require active awareness by participants. Polls show that people are often willing to give up some privacy in exchange for the perception of better security [18]. Fears of terrorism, appeals to patriotism, economic incentives, and the insidiousness of visual surveillance prevent many people from questioning misuses of similar technology—especially when the government and corporations shroud their research and development.

Fortunately, there are alternatives to passive acceptance of a surveillance state. Early in 2005, top Senate Democrats criticized some secret satellite surveillance programs as wasteful and of doubtful benefit with respect to national security. The House of Representatives in Montana recently passed a resolution that strongly criticized the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act). Similar resolutions have passed in hundreds of other cities and counties in the United States.

Public awareness and grassroots resistance against implementations of automated video surveillance that are not accountable to public scrutiny will motivate politicians to legislate against misuse of surveillance technologies. Now that Attorney General Gonzales is willing to at least debate the removal of several insidious provisions in the USA PATRIOT Act, it may be an auspicious time for congressional discussion about the constitutionality and wisdom of implementing automated video surveillance on a wide scale.

Notes:

1. Progressive Review, April 10, 2002
2. <http://www.observingsurveillance.org/>
3. Washington Post, Feb. 17, 2002
4. Ralph Ranalli, Rick Klein, "Surveillance targeted to convention," The Boston Globe, July 18, 2004
5. Erik Baard, "Routes of Least Surveillance," Wired News, Nov. 28, 2001
6. Stephen Kinzer, "Chicago Moving to 'Smart' Surveillance Cameras," New York Times, September 21, 2004
7. John D. Woodward, *Biometrics*, 2003
8. Deanna Boyd, "Gang members tracked by new software," Fort Worth Star-Telegram, July 15, 2004

9. Marcus Nieto, "Public video surveillance: is it an effective crime prevention tool," California Research Bureau, CRB-97-005, June 1997, p. 10.
10. USA TODAY, 4/27/2004
11. Carl Weiser, "Drone research looks at traffic applications," The Enquirer, May 26, 2003
12. John Keller, "Unmanned vehicles: one of the hottest technologies going," Military & Aerospace Electronics, July 2004, p. 3.
13. Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," January 2003, ACLU Technology and Liberty Program
14. Bret Baier and Liza Porteus, "Iraq Drones May Target U.S. Cities," Fox News, February 24, 2003
15. Jean Kumagai, "Sand Trap," IEEE Spectrum, June 2004, pp. 44-50.
16. Brad Grimes, "Smart video surveillance making gains," Washington Technology, June 4, 2004
17. Michael Perelman, *Class Warfare in the Information Age*, Palgrave Macmillan, January 15, 2000
18. Marcus Nieto, Kimberly Johnston-Dodds and Charlene Wear Simmons, "Public and private applications of video surveillance and biometric technologies," California Research Bureau, CRB-02-006, March 2002, p. 6

Andrew Kalukin is a scientist in Arlington, Virginia, who researches automated detection in video camera data. He can be reached at kalukin_99@yahoo.com. He publishes the website [Automated Surveillance](#).