SOMEBODY'S WATCHING ME!
SMART SURVEILLANCE CAMERAS KNOW WHAT YOU ARE DOING

by

Gary Worrall
Buena Park Police Department

April, 2012

COMMAND COLLEGE CLASS 50

The Command College Futures Professional Article is a study of a particular emerging issue of relevance to law enforcement. Its purpose is not to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the professional article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

© Copyright 2012
California Commission on Peace Officer Standards and Training

SOMEBODY'S WATCHING ME!
SMART SURVEILLANCE CAMERAS KNOW WHAT YOU ARE DOING

Surveillance cameras are everywhere. The likelihood that your activities will be captured by a video surveillance camera sometime today is nearly certain. Private entities use surveillance cameras for security and to protect their interests. Governments are turning to surveillance cameras in the name of homeland defense and law enforcement. The diminishing costs associated with the hardware and software necessary to create a complex surveillance system has facilitated the proliferation of these devices.

The explosion of video surveillance cameras has led many civil libertarians to warn about the risks of a surveillance society. Many view the government's use of video surveillance as intrusive. Others accept the implementation of video cameras as a necessity for the higher purpose of safety. The challenge will be to balance the security and safety needs of a government with the people's civil liberties. This is particularly imperative given recent advancements in more precise and what some may see as more invasive biometrics surveillance technologies.

These technologies are making their way into modern police work. Cameras with artificial intelligence may one day be called upon to police our society, forever changing how police work will be done. Science has provided future generations with some wonderful technologies. We must examine the pros and cons of the use of these technologies and how best to consider their use as we work to create a desirable future.

These things are everywhere!

The number of cameras in use in the United States is growing. There are an estimated 30 million surveillance cameras in the United States, shooting four billion hours of video footage each week (Vlahos, 2009). Private and public entities continue to see the installation of video surveillance cameras as a cost-effective means to diminish expenses associated with theft, vandalism, and even more sinister crimes. For instance, retailers use increasing numbers of surveillance cameras to combat patron and employee theft. Communities experiencing chronic graffiti problems use cameras to detect and deter vandalism. And, cameras are being used to protect critical infrastructure from acts of terrorism in places like Cleveland to monitor water facilities, and in Arizona to monitor electrical facilities (Security Info Watch, 2011).

Since 9/11, the nation has spent an estimated $635 billion on homeland security (Stone, 2011). Federal and state governments are spending about $75 billion a year on domestic security to implement homeland defense measures, including complex video surveillance systems (Murphy, 2011). Some of these new systems incorporate a biometrics application, such as facial recognition. Critical infrastructure such as airports have been incorporating cutting edge technologies with video surveillance since the 9/11 attacks. Immediately after the 9/11 attacks, the Federal Aviation Administration, with support and guidance from the Department of Defense, established the Aviation Security Biometrics Working Group. The efforts of this group have advanced biometric science and enhanced federal operations (Biometrics in Government, 2008). TSA screening devices are a direct result of this early effort. In another effort to streamline DHS processes, DHS

has created an Automated Biometric Identification System (IDENT). This system checks each person's biometrics against a watchlist of more than 5.2 million known or suspected terrorists, criminals, and immigration violators identified by U.S. authorities and Interpol (DHS, 2009). Additional technologies on the horizon include facial lie detection kiosks, biometric passports, and advanced explosives detection systems.

To support the electronic monitoring of persons in public places, the American Recovery and Reinvestment Act of 2009 committed more than three billion dollars for homeland security projects through the Department of Homeland Security and the General Services Administration (DHS, 2009). This investment has already yielded technologies that have trickled down to the municipal level, such as facial recognition and license plate reader equipment. These technologies are typically funded by Urban Area Securities Initiatives (UASI) grants. Because of these grants, local governments have been able to benefit from high tech securities technologies at virtually no cost. This trend is likely to continue, even as the technologies improve.

Even municipalities responsible for drinking water, electricity, or mass transit systems are taking advantage of newer video surveillance technologies, some including biometrics, to guard their essential services. Facial recognition has been used by air marshals to surreptitiously photograph people in airports. Private entities are using facial recognition software integrated with video surveillance to protect their interests. Facial recognition cameras are being used by casinos to spot known card counters and other

unwelcome gamblers (Frank, T., 2007). Facial recognition cameras have also been put to use to monitor crowds at the Super Bowl since 2001 (Woodward, 2001).

In 2011, the FBI announced a nationwide face recognition service to allow local police to identify suspects. The system will be activated in Michigan, Washington, Florida and North Carolina. In 2012, the system will be offered to other justice professionals across the country in 2014. Analysts will be able to upload a photograph, and generate a list of potential matches within minutes (McQueeney, 2011). In Orange County, California, Department of Homeland Security funds have been procured to implement a facial recognition system for use by local law enforcement (Homeland Security Newswire, 2011). Select cities in that County were chosen implement a beta test. These cities collected booking photographs to build a data base for later comparisons with the hopes the system will become fully integrated in a few years. Entrepreneurs have even started to market real-time facial recognition. Face.com offers this app for any smartphone user at a nominal cost, offering some incentives for no cost (Wauters, 2011). This app is touted to be more accurate over time as it grows accustomed to spotting the same faces. Essentially, the program is learning through its built-in artificial intelligence.

Far beyond the limited sophistication of Face.com's app, advanced artificial intelligence integrated with video surveillance advancements may forever change how police work is done. Imagine policing a community through the use of video cameras that think. Police officers would no longer need to patrol a traditional beat. They could be stationed at strategic locations, awaiting an alert from a watchful computer. Currently, in the U.K.,

particularly in and around London, most police work is done by persons monitoring video cameras. Advances in processing power and software allow computers to overcome the greatest limitation to traditional surveillance – the ability of human beings to observe the activities on a multitude of computer screens simultaneously (Vlahos, 2009).

In the wake of London's riots last August, police used footage from some of the thousands of closed circuit TV cameras, employing a facial recognition system designed for use during the 2012 Olympic Games to identify law breakers. James Orwell of London's Kingston University is developing the recognition and tracking systems that help authorities make more efficient use of the increasing volume of video surveillance. Orwell's technology makes it possible to search video for specific actions, such as people running or cars pulling over to a curb. It can even search for content-based metadata such as a guy in a red tracksuit (Jones, 2011). Eventually, this technology will be integrated into video surveillance systems in real-time.

It may seem far fetched, but emerging biometric surveillance technologies may actually be able to know what you are thinking. Cameras can be taught to recognize certain visual cues, which could then alert authorities to further investigate the person or incident being captured on video. The cameras could literally become mechanized police officers, patrolling their beats and looking for something amiss. Teaching surveillance cameras to recognize suspicious behaviors has resulted in several interesting potential biometrics applications. Cameras have been taught to recognize a person's gait. Specifically, the camera will recognize walking, suspicious walking behavior, and running. Cameras are

even being taught to recognize anxiety. Perhaps a suicidal person anxiously awaiting the arrival of a train could be stopped before doing something tragic.

Cameras can be programmed to detect a particular object, and even follow it while it moves. These cameras can even auto focus on the object, regardless of the surroundings. A blanket of surveillance cameras positioned throughout a community and wirelessly connected can be taught to follow a person or vehicle from camera to camera as it makes its way around town. Police pursuits may become a thing of the past because the cameras could simply pursue the vehicle and direct officers to its ending point.

The future of video surveillance cameras includes the added dimension of artificial intelligence. Next generation video surveillance cameras can be taught to learn "normal" human behavior patterns in a specific location, and reveal and record the behaviors of individuals who act in unusual or suspicious ways. According to Prescient Group, LLC co-founder and President Charles Barber, iSentry is the most technologically advanced proactive security software in the industry today. iSentry learns normal behavior by observation and detects unusual activity using advanced artificial intelligence software. (Aving, 2008). iSentry detects unusual activity by filtering out over 95% of so-called normal motion video. iSentry can analyze and manage multiple cameras and control active pan/ tilt/ zoom (PTZ) autonomously for tracking. iSentry can then conduct pre-programmed responses, such as email notifications, lockdowns, and notification of security personnel. iSentry has the ability to effectively filter out changing

environmental abnormalities and identify true security issues in real time. This technology will no doubt make its way into municipal law enforcement.

No peeking!

Imagine the existence of an intricate surveillance camera system with requisite hardware and software to recognize someone doing something so dangerous to society that the camera responds with deadly force. Society will be compelled to reconcile with their government being policed by these elaborate technologies. The most critical question will be whether or not a government should regulate society at the cost of privacy.

Civil libertarians view the proliferation of video surveillance cameras as a governmental intrusion. And, like any intrusive technology, the benefits must be balanced against the dangers. According to Suzanne Ito of the ACLU, proponents of more invasive governmental securities initiatives are asking the wrong question. Instead of asking how much privacy people should be willing to trade for more security, the right question is whether the surveillance technologies actually work. Of course, the ACLU maintains that often times, the answer is no (Ito, 2008).

The ACLU and similar advocacy groups may view integrating video surveillance camera systems with emerging biometrics technologies as a more significant encroachment upon people's civil liberties. And, the significant advancements in facial recognition and other biometrics in conjunction with the propagation of video surveillance cameras will no doubt lead to increased concerns regarding their use, thus requiring agencies desirous of

their use to consider they will have to deal with the political implications of such choices in addition to the logistical ones of cost, placement and specific use.

Arguments against video surveillance include: ineffectiveness, susceptibility to abuse, lack of limits or controls, and a possible adverse affect on public life (What's Wrong with Public Video Surveillance, 2002). Indeed, a video surveillance system integrated with biometrics technologies could become a cause for civil libertarian concern. The effectiveness of these systems will likely be improved upon as the technologies advance; but many of these biometrics technologies are still fairly new and untested. All other similar government systems have had an inherent potential for abuse; but appropriate safeguards have been established to mitigate this susceptibility. Clearly, limits and controls will need to be established to ensure these technologies do not become too pervasive.

A possible adverse effect on public life may be the only irreconcilable consequence of such a government surveillance system. It has already been established that people may tend to act differently if they know they are being watched. Studies of cameras in Britain found that persons who appeared out of time or out of place with the surroundings were subjected to prolonged surveillance (What's Wrong with Public Video Surveillance, 2002). Knowing you are being watched by the government may cause people to be careful about their activities. People may put more thought into how they dress, so they don't look like a terrorist, a gang member, or criminal. It's possible the proliferation of

video surveillance cameras could cause people to act differently, causing a complete shift in public life.

A government's omnipresent use of surveillance technologies to monitor its citizens may also seem Orwellian to many in the community. Despite the concern that our government might be too intrusive, an ABC News/Washington Post poll in July of 2007 found that 71 percent of Americans favor increased video surveillance (Vlahos, 2009). Clearly, Americans have prioritized security over privacy for the time being. People value privacy, particularly here in the United States. But, a good majority of Americans worry more about safety; and if a system existed that could find a missing child, catch a murderer, or thwart a terrorist attack, society seems willing to sacrifice a modicum of privacy for that desired end.

While this may seem like a desirable and safe future, there are skeptics. A proliferation of cameras designed to monitor citizens will surely meet with resistance. Similar, though, to concerns regarding the collection and use of DNA (which was originally considered too intrusive) initial objections will most likely give way to widespread acceptance once such system's actual performance and outcomes are known. Society has experienced video surveillance and its outcomes for decades; in fact, much of what will emerge in the near future will be incorporated seamlessly into existing systems with no or little notice.

Do you see what I see?

Fixed post and vehicle-mounted video license plate readers have become quite common in law enforcement. The character recognition technology utilized by these devices has progressed into a highly dependable and accurate system adopted by many police agencies throughout the country. These license plate readers look for stolen vehicles, persons who are wanted and are associated with a vehicle, and other wants concerning cars. Then, the device alerts police to the presence of the vehicle. These devices have the capability of running thousands of license plates during a police officer's shift, far more than the dozen or so using traditional means.

Video surveillance cameras utilizing automated license plate reader technologies are most prolific in the Washington D.C. area. Scores of cameras strategically placed throughout the District capture 1,800 images a minute to help build a rapidly expanding archive that can pinpoint peoples' movements throughout the area. Experts believe that if this technology had existed at the time of the Washington area sniper shootings in 2002, the attacks could have been stopped sooner, and lives may have been saved (Klein, A. and White, J., 2011).

The City of Dallas also monitors much of its downtown area with more than 100 surveillance cameras. Dallas Police Department touts a 30 percent reduction in crime and credits the system with more than 2,500 arrests last year. Dallas PD plans to improve upon this system with the implementation of technologies deployed around facial recognition and repetitive pattern recognition (Today's Wireless World, 2011). It is

evident the cameras are working; and the city of Dallas is at the forefront of biometrics-enhanced video surveillance systems.

Facial recognition is the most obvious way to track people. After all, this is how humans do it (Yang, C., 2005). Facial recognition software is no longer in its infancy. Increased resolution of cameras has paved the way for more accurate face recognition. In fact, some facial recognition programs boast up to 95% accuracy, even if the image is corrupted or the face is obscured (Gardiner, 2008). Much like fingerprint and DNA biometrics, facial recognition will likely make significant gains in accuracy in the future and gain acceptance as a legitimate biometric marker. And, there are innovative new biometrics applications on the horizon that may take surveillance to a whole new level.

Another advancement in video monitoring is a facial biometrics surveillance camera system combined with gunshot detectors. Under this combined system, ballistic acoustic sensors can immediately pinpoint the source of a gunshot and direct a high resolution camera to zoom in on the exact location. The shooter's face is captured and processed by facial recognition software in real time (Facial Biometrics Meet Gunshot Detectors, 2012). An operator is then alerted to the incident and a police response can be directed. Because this system is web-based and IP accessible, police officers responding to the incident can access video surveillance of the incident as it is happening and coordinate their response accordingly. This application will add a whole new dimension to police work. In fact, systems with equally as remarkable capacity are already in use.

An excellent example of a system of video surveillance cameras integrated with artificial intelligence exists on Liberty Island. The Statue of Liberty is an endearing and very well guarded landmark, which is protected by a state-of-the-art video surveillance system. Liberty Island's video cameras feed into a computer system that is capable of analyzing images and alerting human monitors to suspicious events. The software can spot when someone abandons a bag. It can discern types of boats approaching the island. It can count bodies to ensure the same number of patrons leave the island that arrived on a given day. And, it can detect if people are grouped too closely – indicative of a possible fight or gang activity (Ibid).

Casinos have been using facial recognition to recognize cheaters and card counters since 1999 (Grady & Felzien, 2004). Now, banks have begun utilizing facial recognition systems to build facial templates for persons entering their branches. If someone were to cash a check that was later determined to be stolen or fraudulent, the person's face can be flagged in the system. The next time this person enters any of the company's banks, the system will alert tellers. Recently, in Pennsylvania a person using a fictitious driver's license was caught trying to defraud a credit union (Like, 2011). Advocates claim this technology has been successful many times. This same system can be used to help deter bank robberies. In time, other businesses will likely incorporate such mechanisms to diminish losses. Retail establishments may want to share this technology to thwart would-be shoplifters.

The Defense Advanced Research Projects Agency (DARPA) develops technologies for fighting wars. However, one of their unclassified projects, “Combat Zones That See” may be the genesis for an all-encompassing urban video surveillance system. The centerpiece to this project is computer software capable of automatically identifying vehicles by size, color, shape and license; and identifying drivers and passengers by face. This system is the first multi-camera surveillance system that uses automatic analysis of live video to study vehicle movement and significant events across an extremely large area (Another Tool for Big Brother, 2003). DARPA is not the only federal agency working on technologies of a similar nature.

Recently, the Department of Homeland Security developed the Future Attribute Screening Technology (FAST). The technology uses thermal cameras, microphones and laser radar that can measure heart rate and perspiration. FAST is designed to surreptitiously scan airport travelers for nervous behaviors, such as rapid blinking or any other signs that might indicate suspicious intentions. This is essentially a mind-reading machine (Rennie, J., 2011). These cameras do know what you are thinking!

What’s next?

Biometric surveillance technologies have filtered down from military applications to civilian uses. Private and government entities are developing technologies utilizing software algorithms designed to automatically monitor audio and video feeds from multiple surveillance cameras, and then flag suspicious activities in real time

(Ingebretsen, M., 2010). The implementation of artificial intelligence into video surveillance may greatly impact law enforcement.

This is a significant change that will likely emerge in the next ten years. Advancements in these technologies are rapid and gaining momentum. These changes will alter traditional police staffing and deployments. It seems reasonable to assume because cameras have been shown to diminish crime, crime will likely diminish. This in turn may mean fewer police officers. Cameras owned and operated by private entities may cause the proliferation of privatized police agencies. As cameras begin to permeate densely populated urban areas, police deployments will likely be pushed to outlying areas. The connectivity of these systems may propagate the regionalization of police services. The daily activity of the individual police officer will be greatly impacted. Police officers will "patrol" their beat via a laptop from the front seat of their police car.

Advancements in surveillance technologies have piggybacked on developments in other biometrics fields. Scientists are exploring the use of bodily scents and secretions as a form of biometric identification. Other emerging technologies include: artificial noses that sniff explosives, cameras that identify you by your ears, or that analyze the halo of heat you emit (Yang, 2005). If all of these video surveillance technologies could be integrated and made to work through artificial intelligence technologies, police officers would need to adapt to a completely different way of doing business.

The future…

Stewart Brand (2000) wrote, “This present moment used to be the unimaginable future.” It may be difficult to envision or comprehend, but one day cameras may one day effectively police our society. Cameras taught to detect suspicious persons or unusual behavior may be placed strategically to monitor segments of a community for the sole purpose of keeping order. Web-based surveillance systems policing a community may signal the end of a traditional police station house and other long held police customs. The manner in which police officers do their jobs will be forever changed with the advent of these biometrics enhanced video surveillance systems.

REFERENCES

Another Tool for Big Brother (2003). Retrieved February 24, 2012 from http://www.wired.com

Aving (2008). Aving.net. *Prescient Group, LLC To Introduce iSentry, Groundbreaking Artificial Intelligence Video Surveillance Technology, at 15th World Congress of Intelligent Transport Systems Meeting*. Retrieved March 16, 2012 from http://us.aving.net

Biometrics in Government Post-9/11 (2008). National Science and Technology Council retrieved on March 9, 2012 from http://www.biometrics.gov

Brand, Stewart. (2000). *The Clock of the Long Now: Time and Responsibility*. Retrieved May 6, 2011 from http://longnow.org

Department of Homeland Security (2009). *Secretary Napolitano Announces More than $335 Million in Recovery Act Funding for Airport Security Projects.* Retrieved March 6, 2011 from http://www.dhs.gov

Department of Homeland Security (2009). *Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger, Screening Coordination, and Director Robert A. Mocny, US-VISIT, National Protection and Programs Directorate, before the House Appropriations Committee, Subcommittee on Homeland Security, "Biometric Identification"*. Retrieved March 16, 2012 from http://www.dhs.gov

Facial Biometrics Meet Gunshot Detectors (2012). Retrieved February 16, 2012 from http://www.homelandsecuritynewswire.com

Frank, T. (2007). *Face Recognition Next in Terror Fight*. Retrieved on February 24, 2012 from http://www.usatoday.com

Gardiner, B. (2008). *Engineers Test Highly Accurate Face Recognition*. Retrieved February 17, 2012 from http://www.wired.com

Grady, T. & Felzien, K. (2004). Ethica Publishing. *Privacy and Casinos: What They Know About You.* Retrieved March 20, 2012 from http://www.ethicapublishing.com

Homeland Security Newswire. (2011). *Facial Recognition Systems for Orange County, California*. Retrieved on March 20, 2012 from http://www.homelandsecuritynewswire.com

Ingebretsen, M. (2010). *Researchers Add Artificial Intelligence to Video Surveillance.* Retrieved January 26, 2011 from http://www.hsoutlook.com

Ito, S. (2008). ACLU. *Surveillance State Blues.* Retrieved March 20, 2012 from http://www.aclu.org

Jones, W. (2011). IEEE Spectrum. *The Future of Riots*. Retrieved March 16, 2012 from http://spectrum.ieee.org

Klein, A. and White, J. (2011). The Washington Post. *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns.* Retrieved on February 24, 2012 from http://www.washingtonpost.com

Lipke, M. (2011). Reuters. *When Financial Fraud Meets Facial Recognition, the Jig May Be Up.* Retrieved on March 9, 2012 from http://www.reuters.com

McQueeney, K. (2011). *Face Recognition Software to be Launched by FBI to Help Police Catch Wanted Criminals*. Retrieved February 16, 2012 from http://www.dailymail.co.uk/news

Murphy, K. (2011). Los Angeles Times. *Is Homeland Security Spending Paying Off?* Retrieved March 16, 2012 from http://articles.latimes.com

Rennie, J. (2011). *Dishonesty Detectors: A Criminally Flawed Technology*. Retrieved on February 24, 2012 from http://www.smartplanet.com

Security Info Watch. (2011). *Success Stories: Critical Infrastructure*. Retrieved on March 20, 2012 from http://www.securityinfowatch.com

Stone, A. (2011). Emergency Management. *10 Years After 9/11: How Far Did 635 Billion Spent on Homeland Security Go?* Retrieved March 16, 2012 from http://www.emergencymgmt.com

Today's Wireless World. BearCom Wireless Worldwide (2011). *IP Video Surveillance Cameras: Video Surveillance Systems Take a Bite Out of Crime*

Vlahos, J. (2009). *Surveillance Society: New High-Tech Cameras Are Watching You*. Retrieved February 22, 2012 from http://www.popularmechanics.com

Warning over 'Surveillance State' (BBC News, 2009). Retrieved February 15, 2012 from http://news.bbc.co.uk

Wauters, R. (2011). Tech Crunch. *Face.com's API Now Lets Developers Scan 5,000 Photos Per Hour, Free of Charge*. Retrieved March 16, 2012 from http://techcrunch.com

What's Wrong with Public Video Surveillance? The Four Problems with Public Video Surveillance (2002). Retrieved from http://www.aclu.org on February 16, 2012

Woodward, J. (2001). *Super Bowl Surveillance, Facing Up to Biometrics.* Santa Monica: Rand. Retrieved January 26, 2011 from http://www.rand.org

Yang, C. (2005). *The State of Surveillance.* Bloomberg Businessweek. Retrieved March 6, 2011 from http://www.businessweek.com