Summer 8-2017

Are DHS technology grants for local police departments an effective tool against terrorism?

Erika McGinty
CUNY John Jay College, rikkimc@gmail.com

Are DHS technology grants for local police departments an effective tool against terrorism?

A thesis presented in partial fulfillment of the requirements for the degree of Master of Arts in Criminal Justice, John Jay College of Criminal Justice, City University of New York

Erika McGinty

July 2017

Abstract

This paper examines the effectiveness of allocating funds to the nation's police departments for the prevention of domestic terrorism, as is done annually through the Department of Homeland Security's Homeland Security Grants Program. The program, administered by the Federal Emergency Management Administration, has distributed billions of dollars since its 2003 inception in equipment, software, and technology services based on the recipient police agencies' own risk assessments of local terrorism. Much of the technology desired by police consists of systems of mass surveillance; this thesis focuses on implementations of surveillance video cameras or CCTV, license plate readers, and unmanned aerial vehicles. Drawing on academic studies, government watchdog reports, media coverage, police manuals, nonprofit publications, and sociological texts, research is guided by the hypotheses that mass surveillance is not suited for the prevention of terrorism and that grant recipients are requesting and implementing technology for purposes other than terrorism prevention. Using the *Technology Policy Framework* issued by the International Association of Chiefs of Police in 2014 to assess these implementations, findings include that an approach of surveillance policing is at odds with both the fundamental policy of policing as crime prevention and the principal tenet of maintaining citizens' trust in the police. This thesis reveals a lack of empirical research on anti-terrorism measures and insufficient evidence that current surveillance methods prevent crime. Furthermore, due to the recognized low probability of terrorism, police departments are utilizing grant funds for investigative purposes as well as the everyday pursuits of retrieving stolen vehicles and monitoring traffic accidents.

Introduction

Within days of the September 11, 2001, terrorist attacks in the U.S., American lawmakers began to craft anti-terrorism legislation intended to address the conditions that enabled these attacks and to prevent future incidents of domestic terrorism. Six weeks later, the USA PATRIOT Act was unanimously agreed upon by the Senate Judiciary Committee. When spelled out, the title of the USA PATRIOT Act, passed by Congress on October 26, 2001, reveals an emphasis not on the *goal* to reduce the risk of terrorism but on the chosen strategy to do so:

> Uniting and Strengthening America to *Providing Appropriate Tools* Required to Intercept and Obstruct Terrorism. (*Emphasis mine*)

Some of the tools chosen for inclusion in the Act consisted of legislation that dramatically expanded the powers of federal and local law enforcement and curtailed civil liberties and privacy protections (de la Peña, 2004). According to then-Senator Bob Barr (R-GA), the bulk of the document placed before the full Senate comprised legislation that had previously been rejected by Congress, such as the expansion of police powers and other items that were unrelated to domestic terrorism. For on the day of the full House and Senate vote, the version of the USA PATRIOT Act agreed by the Senate Judiciary Committee the evening before was replaced at 3:45am with one prepared in secret by Attorney General John Ashcroft, the Vice President, and the President (2004). When accused by members of the Senate Judiciary Committee of switching versions, Ashcroft responded, “To those who would scare peace-loving people with phantoms of

lost liberties, my message is this: Your tactics only aid the terrorists" (2004). In spite of not having read the proposed legislation before them, seemingly cowed by the threat of appearing pro-terrorist, the country's elected representatives passed the Act the same day.

Even before the passage of the USA PATRIOT Act, President Bush created, by executive order, the Office of Homeland Security on October 8, 2001, with former Pennsylvania governor Tom Ridge as its director (Congressional Research Service, 2002). Not satisfied with that response, then-Senator Joe Lieberman (Ind-CT) introduced legislation just days later calling for the establishment of a federal department dedicated to homeland security. On July 16, 2002, the term "homeland security" entered the body politic through publication by the President's Office of Homeland Security of *The National Strategy for Homeland Security*, a 90-page document announcing the formation of a new federal department. The Department of Homeland Security was to facilitate information sharing among intelligence agencies and to fund local, regional, tribal, and federal domestic terrorism prevention efforts. *National Strategy* included the President's definition of *homeland security*, a term heretofore unfamiliar to the public:

> Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (2002, p. 2)

The Department of Homeland Security (DHS), launched in early 2003, was intended as the main tool to intercept and obstruct terrorism, specifically anti-American terrorism in the U.S. itself. Enacted by the *Homeland Security Act* in November 2002,

DHS was meant to remedy the situation that led to 9/11; for example, to "streamline information sharing" – widely believed to be a problem between FBI and CIA and pinpointed as a reason for the success of the 9/11 attacks (9/11 National Commission, 2004). With the enactment of the USA PATRIOT Act, states the *National Strategy for Homeland Security*, "Congress took important steps toward identifying and removing some barriers to the exchange of intelligence" (as cited in Congressional Research Service, 2002, page 48). The USA PATRIOT Act had already provided broad legal support to the nation's police departments and, according to prominent police experts such as William Bratton and George Kelling, local law enforcement was in the best place to detect terrorist activity (Newman & Clarke, 2008). This was later restated by Michael McCaul (R-TX), chairman of the House Committee on Homeland Security, and senior Committee member Bill Keating (D-MA):

> [S]tate and local police know their city's streets and residents better than anyone. This knowledge makes them a force multiplier for federal law enforcement's efforts. Their insight and impact are huge considering that nationwide there are just under 14,000 FBI agents, while in New York alone there are almost 35,000 NYPD officers. Clearly, utilizing local law enforcement expertise will ultimately result in keeping more Americans safe and mitigating the risk of terrorist attacks (2014).

DHS quickly followed up its launch with financial support for the police by establishing the Homeland Security Grants Program, which has allotted billions in

equipment, software, training, and vendor services to branch offices in all 50 states and the U.S. territories since 2003 (DHS, 2017). In addition, the new department created a portfolio of grants for parties other than law enforcement, such as public transit agencies and nonprofit organizations. According to the Congressional Research Service, between 2003 and 2011, DHS distributed over $40 billion in grants on homeland security (Reese, 2012).

Much of the funding received by police agencies from the Federal Emergency Management Administration – the DHS organization that administers the grants allocated for homeland security – goes toward the purchasing of general surveillance systems that observe the public and can capture various forms of personal data. By looking at implementations of three such technologies – surveillance video cameras, license plate readers, and unmanned aerial vehicles – this thesis seeks to challenge the effectiveness of DHS's police grants based on two hypotheses: 1) general surveillance is a strategy not suited for the prevention of terrorism, and 2) police departments are using their grant allocations for purposes other than the detection of terrorists and terrorist activity.

Methodology

As a prism through which to view the research collected to examine my hypotheses, this paper leverages a policy framework created by representatives of the police themselves. In January 2014, the International Association of Chiefs of Police (IACP) published its first guide to formulating policy for the implementation and use of technological systems. The IACP's "Policy Mandate" is clear and comprehensive and reflects an institution that serves the public:

> Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and maintain community trust (2014, p. 2).

"Just because a technology *can* be implemented does not mean that it *should* be." This core tenet is part of the *Technology Policy Framework* by the IACP (p. 1). A nonprofit membership organization comprised of current and former police leaders, it was founded in 1893 to advance the "science and art of police services" by conducting research – often in collaboration with federal agencies and academic institutions – and issuing evidence-based policy guidelines for technical, administrative, and conduct-related police practices (IACP.org, 2016). In light of the rapid evolution of technologies capable of recording and identifying personal data that have been made available to law enforcement, IACP recognized the need of providing a comprehensive technology policy framework as a resource to individual police departments. Using this framework, each would be able to create policies governing its use of technologies that would ensure these new tools deliver value toward policing goals while safeguarding the necessary trust and cooperation of the public (IACP, 2014).

The *Framework* identifies those technologies whose use is of particular concern to the public and most likely to be subject to legislative action, namely those that "have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time,

data, and geographic location where the data were captured" (p. 3). Examples include the three that form the focus of this thesis: surveillance video cameras, license plate readers, and unmanned aerial systems. All three constitute devices for general, or mass, surveillance; they are deployed by police in public locations – in stationary or mobile form – and are trained on the public without any individualized suspicion that may require a search warrant. At the same time, each captures visual, geographical, and chronological data points that can reflect personally identifiable information, even – given a sufficient amount collected over time – a history of destinations, habits, and affiliations.

Despite the capacity to develop knowledge of individuals and their behavior, this thesis argues that general surveillance modalities are unsuited as a prophylactic against terrorism. Foremost among President Bush's three goals of homeland security is to prevent terrorism, and surveillance is inherently reactive – that is, its use is limited by the need to have already recorded an incident. In addition to limiting the type of technologies examined here, research for this paper focuses on implementations funded by DHS grants designated exclusively to local or regional law enforcement, which are the State Homeland Security Grant Program, the Urban Areas Security Initiative, and the far less prevalent Operation Stonegarden – together, these make up the Homeland Security Grants Program.

Information on grant allocations, installations, and performance was drawn from a variety of sources to represent different perspectives and target audiences; these include academic journals, reports by government agencies such as the Government Accountability Office, articles from police news mailings such as the Federal Law

Enforcement Training Center's *TechBeat*, publications from civil liberties nonprofits, research studies from institutions such as George Mason University's Center for Evidence-Based Crime Policy and RAND Corporation, manuals from police organizations such as COPS, items from topical online portals such as Homeland Security Today, investigative journalism, and DHS.gov. These sources were monitored and studied over a period of over four years to examine the steps taken by police departments to identify the anti-terrorism equipment or systems to be covered by the Homeland Security Grants Program as well as the process of implementation and the outcome of these innovations. The analysis required to arrive at this paper's conclusions and recommendations was based on the guidelines comprising the IACP's framework; specifically, the "universal principles" that each police agency should adhere to when deciding to acquire new technology (*see Table 1 in* Appendix).

These principles, or procedural steps, begin with the need to specify the objectives of the desired technology, which should align with the objectives of the agency, as well as what is required to implement and maintain it; for example, calculating total costs and identifying necessary staffing and skills training. Use and storage policies need to be documented and distributed regarding the data that is collected – be it video camera footage or license plate scans – including where and how long it will be kept, how it may be accessed and by whom; these rules should be shared with the public, providing transparent privacy policies.

Framework principles further emphasize the importance of continually monitoring whether equipment and data collection are serving a purpose and achieving stated objectives, which requires defining in advance what metrics will be used to evaluate

performance. “Agencies should regularly monitor and evaluate the performance and value of technologies,” reads the document, “to determine whether continued deployment is warranted …” (p. 3). Police departments must implement adequate technical and infrastructural security against breach of data and identify what actions should be taken if in case of failure. Finally, the IACP demands that each department’s sworn or civilian personnel as well as possible contractors and volunteers are held accountable to its technology policies as well as the law, and that violations are officially sanctioned as determined in advance.

How and whether these universal principles are applied as revealed in the literature sampled for this thesis addresses the hypotheses that surveillance technology is inherently unfit for the prevention of terrorist incidents, and that police agencies are relying on DHS grant allocations to fulfill objectives other than terrorism prevention.

Risk- and performance-based grant allocation

As part of delivering on its mission of homeland security, DHS assigned to the Federal Emergency Management Administration (FEMA) the responsibility of distributing funding to local and state government agencies; these funds are available through FEMA’s Preparedness, or Non-Disaster, grants programs toward the National Preparedness Goal of a “secure and resilient Nation” (FEMA.org, 2017). There are eight such programs, ranging from the Emergency Management Performance Grant Program with a 2017 budget of $350 million to the Nonprofit Security Grant Program, whose $10 million budget has been allocated almost exclusively to Jewish advocacy organizations, to the Port Security Grant Program with a 2017 budget of $100 million targeted at the “highest-risk” ports in the U.S.

Largest among the grants programs by far is the Homeland Security Grants Program (HSGP), whose 2017 allocations amounted to over one billion dollars, bolstering DHS policy of having local police constitute the "front line" in detecting homegrown terrorist threats against America (*see Table 2*). HSGP consists of three types of homeland security grant types exclusively available to law enforcement, targeted at state agencies, urban agencies, and border-area agencies, respectively: the State Homeland Security Program; the Urban Area Security Initiative; and the far smaller Operation Stonegarden, intended for police in states neighboring national borders to assist in DHS border security responsibilities.

Table 2. Homeland Security Grants Program, FY 2011 – 2017 (in $ millions)

Program	2011	2012	2013	2014	2015	2016	2017
State Homeland Security Program	526.8	294.0	354.6	401.3	402.0	402.0	402.0
Urban Area Security Initiative	662.6	490.4	558.7	587.0	587.0	580.0	580.0
Operation Stonegarden	54.8	46.6	55.0	55.0	55.0	55.0	55.0
TOTAL	1,244.2	831.0	968.3	1,043.3	1,044.0	1,037.0	1,037.0

Source: DHS.gov, 2017

The Homeland Security Act of 2002 stipulated that federal funding was to be distributed according to the level of risk of a terrorist attack. However, according to repeated evaluations by the Government Accountability Office, DHS has struggled to determine standard risk assessment formulae and the responsibility of assessing risk fell to the police agencies themselves (2007; 2008; 2013). FEMA, a long-established federal institution, had no previous experience with issues of terrorism and relied on these self-

assessments in approving grant requests. Additionally, legislation outlined that each state and territory receive a portion of the anti-terrorism funds regardless of risk. As a consequence, appropriations per state through the State Homeland Grant Program have not reflected even basic common sense; with Wyoming topping state anti-terrorist spending in 2011 at $9 per resident, for example, while New York was last at $4.70 per resident (*see Table 3*).

Table 3. Top 10 DHS Grant Recipients, in dollars per capita

1	Wyoming	$9.00
2	District of Columbia	$8.60
3	Vermont	$8.20
4	North Dakota	$7.50
5	Alaska	$7.10
6	South Dakota	$6.20
7	Delaware	$5.70
8	Montana	$5.10
9	Rhode Island	$4.90
10	New York	$4.70

Source: Stateline, 2011 (as cited in O'Sullivan, 2014).

South Dakota received $100 million in the decade from the grants' launch in 2003 to 2013, making the state sixth in per-capita spending, despite being one of 15 states that U.S. intelligence agencies rated in 2010 as having "no specific foreign or domestic terrorism threat" (O'Sullivan, 2014). South Dakota has acquired equipment to detect

IEDs, surveillance camera systems for schools, and electronic fingerprinting technology based on the alleged threats of white supremacists and environmental terrorists targeting the Keystone XL pipeline (2014). In Texas, where the Department of Public Safety was designated in 2003 to administer the Homeland Security Grants Program, each of the more than 1,400 county, city, and tribal jurisdictions submit grant requests to FEMA every year (Stewart & Oliver, 2014).

It was only three years into the FEMA grants program that DHS added the requirement for applying agencies to provide "investment justifications" that would be used to inform funding decisions (GAO, 2007). Also in Fiscal Year 2006, DHS made public its risk assessment method used to determine which cities would be eligible for Urban Areas Security Initiative grants; the number of recipients had grown from an initial seven to 43 in FY 2005. The new risk analysis would comprise components threat, vulnerability, and consequences (2007). However, the GAO found in 2008 that DHS assigned every state and urban area the same vulnerability score, as though they were equally vulnerable to a terrorist attack; this significantly undermined the credibility of the department's risk assessments (GAO, 2008). A study conducted in 2007 of Texas police chiefs established that it was the receipt of homeland security funds that drove local agencies to implement anti-terrorism initiatives and not a perceived risk of terrorism; that in fact, only 42 percent of grant applicants had conducted a risk assessment of their locale (Stewart & Oliver, 2014).

In 2012, FEMA released a self-assessment toolkit for HSGP applicants called Threat and Hazard Identification and Risk Assessments (THIRA) to help police departments identify possible terrorist targets in their areas, opportunities for terrorism,

and the likelihood of attacks being staged. THIRA was not intended for use in FEMA's evaluation of funding proposals (GAO, 2013). Instead, the mechanism was supposed to be matched with "national capability performance requirements and measures" for longitudinal success evaluations; these, however, had not been developed.

Without assessing the risk of terrorism to an individual locale and without assessing the effectiveness of the technology requested to reduce that risk level, grants are awarded primarily based on the self-reported needs of police applicants. As a consequence, Dillingham, Alaska – a town of 2,400 – received a $202,000 grant for surveillance cameras, claiming that being a port city it was attractive to potential terrorists (Earle, 2006). In his 2012 report, *Safety at Any Price*, Senator Tom Coburn (R-OK) examined the performance of FEMA's largest individual homeland security grant program, UASI, and concluded that "With so few accountability measures in place, there is almost no way to ensure taxpayers are getting value for their money, and more importantly, whether they are safer" (p. 5). He noted that among the $7.1 billion spent through UASI grants to date, $98,000 had gone toward an underwater robot for Columbus, Ohio, to assist in rescue missions. Keene, NH, with a population of 23,000 had not only been designated a high-risk urban area but had secured a UASI grant for a BearCat armored vehicle to protect the town's annual pumpkin festival (Coburn, 2012).

Referring to the Homeland Security Grants Program as a whole, DHS's own Inspector General reported in 2012 that FEMA did "not have a system in place to determine the extent that Homeland Security Grant Program funds enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters and other emergencies" (DHS OIG, 2012, p. 1).

FEMA's lack of performance measures makes it unable to hold police departments accountable for their investments, or even to control whether the funds received are being spent on anti-terrorist technology. Regardless of the basis for receiving DHS funds, spending them is under the purview of the individual police departments. In the absence of procedures to evaluate police implementations to counter threats, police officials can choose to spend awards according to their own preferences and goals.

Former New York police commissioner William Bratton has exhibited arguable disregard of the DHS mission of terrorism prevention. "One of the great benefits New York gets out of being the most likely terrorist target," he boasted in 2014, "is that the funds that come in help us on the more prevalent issue of day-to-day crime" (Smith, 2014). While this may align with the IACP *Framework*'s first universal principle of making technology use align with departmental objectives, it violates the intent and purpose of the federal homeland security grants.

Prevention in policing

Given the amount of grants available, the flexibility in their allocation, and the low likelihood of a terrorist attack in any domestic locale, it is no wonder that state and local police agencies are seeking to use new tools to meet longstanding objectives such as countering crime rather than terrorism. Some policing experts argue that – whether in preparation for an attack or merely for survival – potential terrorists are likely to commit "ordinary" crimes such as robbery and drug dealing, even that terrorism itself is just another type of crime (Newman & Clarke, 2008). Addressing police executives in particular, the Office of Community Oriented Police Services (COPS) emphasizes, however, that any changes made in their new role of policing terrorism "put a premium

on prevention, on service to the community" (2008, Brief 02) – requirements that uphold the oldest and founding principles in police work.

When post-industrialization London began to experience increasingly violent protests by factory workers and city residents perceived a rise in crime, recently appointed Home Secretary Sir Robert Peel was chosen to design the first modern police department (Johnson, 1981). At its launch in 1829, Peel issued to all officers a handbook that stated, "The object to be attained is the prevention of crime" (Reith, 1948, p. 62). He designated prevention policing a better method to keep citizens and property safe than would be the arrest of offenders after the fact. On foot patrol around the clock, police officers in the U.K. and – beginning in the 1840s – in the U.S. mingled physically with community members, gaining familiarity and trust with their constituents, and were thus able to preserve order and dissuade troublesome incidents (Johnson, 1981). "The test of police efficiency," informs Peel's *Nine Principles of Policing*, "is the absence of crime and disorder, and not the visible evidence of police action in dealing with them" (Reith, 1948).

Key to prevention policing was the police uniform, whose deterrent function arguably makes it the first example of policing technology. The uniform also contributed to the accountability of individual officer as it identified him as a member of the police force to the public and forced him to behave professionally and in accordance with the law. Ironically, many police recruits initially protested against wearing the uniform, claiming it "smacked of subordination and tyranny" (Johnson, 1981, p. 28), not realizing how quickly it was to become a symbol instead of power and authority over regular

citizens. This has been especially true in the U.S., where police officers officially carry firearms, thereby exacerbating the power inequity with civilians.

Peel's paradigm of prevention policing is best represented by the 20th century's community policing, which was heavily infringed by the surge in the 1990s of "broken windows" and "zero-tolerance" methods that relied largely on making arrests. The anathema of arrests to crime prevention is argued by researchers Cynthia Lum and Daniel Nagin of the Center for Evidence-Based Crime Policy, who cite both financial and social costs (2015). When interactions with the police began to generate overwhelmingly negative output – arrests and searches – the relationships with especially black and Hispanic neighborhoods soured, a phenomenon that Lum and Nagin seek to reverse in their blueprint (2015). Echoing the COPS and Peel directives to serve and earn respect from the public, they make inextricable the principles of crime prevention and "citizen reaction matters"; i.e., that regardless of the effectiveness of a given policing method, it must be reconciled with the community (2015). This is not merely to provide the positive quality-of-life outcome, as is associated with community policing (Kelling & Moore, 1988), but also to ensure success of mutually agreed-upon crime prevention tactics. RAND policy analysts add another benefit to "seeking the input of ordinary citizens," namely that this "confers local police with greater authority and legitimacy" (Treverton, Wollman, Wilke, et al, 2011, p. 25) – precisely what is needed to sustain cooperation.

Crime prevention can take many forms, including environmental design, structural design, and target hardening – the defining characteristic is that it inhibits undesired action. Increased street lighting has been shown widely to reduce crime – both violent and property – as well as make people feel safer (Welsh & Farrington, 2008).

When plane hijackings started to take place in the 1970s, the installation of metal detectors was able to reduce their occurrence (Lum, Kennedy, & Sherley, 2008); post-9/11, airline manufacturers undertook widespread action to thicken cockpit doors to be resistant to attack. Crime prevention through environmental design (also known as CPTED) can be accomplished by simple changes to property through landscaping, adding fences, or removing thick hedges that serve to hide trespassing. Prickly vegetation underneath low-level windows can serve as a natural deterrence to would-be burglars (DesignOutCrime.com, 2011). These efforts can be undertaken by individual residents or by communities in collaboration with their local police departments as part of community policing, with its focus on prevention and transparency. The Los Angeles Police Department, for example, has an extensive CPTED initiative in place that was forged in partnership with consultancy Design Out Crime and can be explored on the department's Web site (LAPD, 2016).

After the 2001 terrorist attacks, however, over 80 percent of local law enforcement agencies responding to an IACP survey reported shifting their focus and efforts away from crime prevention in favor of counterterrorism (as cited in Kim & de Guzman, 2012).

Anti-terrorism implementations

> [O]nly those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value. (IACP, 2014, p. 3)

To justify the expense of the terrorism prevention system to be implemented, of training and human resources, and of maintenance, storage, and monitoring, as well as the potential shift in agency focus, the unknown latent consequences such as impact on community relations, the potential dependence on third-party manufacturers or contractors, and other eventualities, it would seem like commonsense to have evidentiary grounds to believe in the system's success. Yet a comprehensive review of terrorism research revealed an almost complete lack of scientific study (Lum, Kennedy, & Sherley, 2008). A 2003 search across 17 literary databases and multiple disciplines returned 14,000 articles containing references to terrorism, spanning a period from the early 1960s through 2002. Of the peer-reviewed articles, which one might assume would be likely based on empirical, if not quantitative, analysis, only three percent were.

Over half of the 40 years of pieces were written in just two years, 2001 and 2002, clearly as a result of the 9/11 terrorist attacks; still, 96 percent constituted "thought pieces," offering no evidentiary basis for the terrorism prevention policies that were forged during these and the following years (Lum, Kennedy, & Sherley, 2008). Most importantly, in the context of this thesis, none of the empirical or evaluation anti-terrorism studies were conducted on the use of surveillance technologies, despite them having been available long before 2001. The only studies involving law enforcement were of airport security measures such as metal detectors; only 0.6 percent of peer-reviewed articles concerned themselves with domestic terrorism (2008, Table 1, p. 37).

These results appearing during precisely the time that DHS was created and its missions articulated, and the overall fear of another incident of domestic terrorism, do not indicate a timely shift in research toward identifying working prevention mechanisms. In

a 2007 survey of local law enforcement agencies, only 11 percent reported any interactions with the research community (Lum & Fachner, as cited in Lum, Haberfeld, Fachner, & Lieberman, 2011). This strongly indicates that the choices by police and sheriff departments of surveillance video cameras, license plate readers, and unmanned aerial vehicles as preventive tools against domestic terrorism have been based largely on factors other than proven effectiveness. Referred to as "general surveillance" because they monitor the public at large based only on geographic location, these technologies generate records that must first be interpreted by humans before any intervention can take place; general surveillance is inherently a reactive mechanism, which makes it of questionable use for the prevention of crime or terrorism.

Surveillance video cameras or CCTV (closed-circuit television)

> CCTV advocates have successfully marketed limited evidence of success in very specific areas (parking lots) as an effective crime prevention strategy for both violence and property crime prevention in ALL public places. (Haggerty, as cited in Byrne & Marx, 2011, p. 22)

Surveillance cameras are deployed for generally three purposes: to deter criminal activity, to investigate crimes and identify suspects, and to instill a feeling of safety among citizens. When visible, the cameras intend to deter individuals from engaging in unwelcome activity by presenting the possibility of getting caught; second, to apprehend suspects identified on tape, which can serve as evidence in court; and finally, to reassure residents they can move safely, without threats posed by unmonitored individuals.

CCTV is best known for decades of permeating Britain as a response to wide-spread bomb attacks by Northern Ireland's IRA. British police reported that although the cameras had been implemented with deterrence in mind, reality had shown them to be purely investigatory. "There's no fear of CCTV," stated Detective Chief Inspector Mick Neville at London's Metropolitan Police. "Why don't people fear it? [They think] the cameras are not working" (Bowcott, 2008).

This is not an unreasonable assumption. A 2004 $45 million UASI grant went to Chicago's Cook County to launch "Project Shield," which was to outfit two police vehicles in each of the 128 suburbs with surveillance cameras feeding live video to a data analysis command center; in addition, the suburbs themselves were to have mounted cameras in place (Marin & Moseley, 2012). Three years after the project went into implementation, reports emerged of fraud and mismanagement by contractor IBM. In 2012, an investigation found that cameras were not being maintained, many had not been tested before implementation and had never worked, and police had selected locations for the mounted cameras of "questionable homeland security benefits" – namely, facing police parking lots and inside precinct lobbies. Project Shield was scrapped as a total failure, leading then-Representative Mike Quigley to address the Government Accountability Office: "We have spent hundreds of millions of dollars across the country on homeland security. If Project Shield is any indication, we are less safe" (Marin & Moseley, 2012).

As a method to deter violent crime, surveillance cameras have shown little success. In repeated studies with convicted armed robbers and thieves, participants were asked to rank a list of crime prevention methods in order of deterrence. All placed

surveillance cameras near or at the bottom; police patrol figured among the top deterrents (Schlosberg & Ozer, 2007). Participants said they were not afraid of cameras because they "knew" nobody was watching. Video footage witnesses activity; it has not been shown to be useful as a deterrent. A 2002 study of 22 implementations of CCTV in both Britain and the U.S. concluded that "while cameras could have a marked effect on reducing vehicle crime, there was little evidence they prevented violent crime" (BBC, 2002). In fact, follow-up reports found that street lighting was more effective in preventing violent crime and property crime (2002). Yet in 2009 London alone had one million cameras installed, according to an internal police report, and even when used for investigative purposes, CCTV could claim but one crime solved annually per 1,000 cameras (BBC, 2009).

In spite of dubious success abroad and very little research on implementations in the U.S., local police departments continue to request systems that are almost certainly not going to detect terrorist activity and are dramatically invasive. The Boston Metropolitan Transportation Authority, having saturated its subway system, successfully applied for a DHS grant for $6.7 million to equip its buses with surveillance cameras, which now record two-thirds of Boston's bus trips (Powers, 2014).

The remote and reactive properties inherent to CCTV arguably present a hazard to public safety in that the installations of such systems allow local law enforcement to rely on them to replace the need for human patrol. NYPD chief Bratton might want to reevaluate New York's anti-terrorist preparedness in light of what took place on July 22, 2014. In the early hours of the morning, a group of artists walked onto the Brooklyn Bridge, replaced the U.S. flags with white ones, and left the scene without being detected

or apprehended (Schneider, 2014). They were able to carry out this stunt despite the 2011 installment of 1,800 surveillance cameras in Manhattan, at the cost of nearly $200 million to DHS (Kappstatter, 2011). In its failure to avert what could have been a successful terrorist attack, New York City's surveillance system demonstrated the ineffectiveness of surveillance video for that purpose. In its first eight months, the *Ring of Steel*, as dubbed by then-police commissioner Ray Kelly, had enabled the arrest of 100 suspects of crimes such as assault and purse-snatching, according to the NYPD. Kelly pointed out the Ring's accomplishments of detecting "bags left on the sidewalk," which he claimed could be indicators of terrorism, and said the city would soon double the amount of cameras (2011).

Based on the examples discussed in this section it is apparent that surveillance camera installations in the U.S. have not had a measurable impact on preventing terrorism. CCTV is a surveillance technology that has limited, post-facto applications, mainly in investigative policing.

License plate readers

From 2006 through 2011, DHS awarded over $50 million in grants to local police departments for purchasing license plate readers (LPRs); recipients included Los Angeles; a Georgia county of 23,000; and municipalities of varying sizes in between (Angwin & Valentino-Devries, 2012). LPR technology falls under "general surveillance" because, like video cameras, it surveys the public indiscriminately. However, while camera networks continuously videotape without predefined data points, license plate readers are manufactured to grab individual "scans" of all license plates within its range,

along with the time and location of each capture, and can run these through a database to identify matches. License plate readers have traditionally been "portable," meaning they are installed onto a law enforcement vehicle. Police purchasers have the option of "mobile" readers – units that can be moved among vehicles. Location information is recorded using GPS in the case of LPRs affixed to these vehicles; for stationary or mounted LPRs, it is recorded according to reader location; e.g., in the form of a particular street intersection.

In a 2004 study, the Ohio State Highway Patrol – in partnership with LPR manufacturer Remington-Elsag – mounted LPRs at Ohio Turnpike toll booths to scan the license plate of each vehicle driving onto the Ohio turnpike (OSHP, 2005). OSHP had a "hot list" of 345,000 license plate numbers tied to stolen automobiles or wanted felons, most of which had been provided by the National Crime Information Center, with 8,000 being Ohio license plates. By the end of the four-month research period, the LPRs affixed to the three toll booths had stored almost 1.9 million scans; according to toll booth operators, this amount meant that the devices had failed to scan 14 percent of total turnpike entries during this period. Moreover, not all scans were of license plates; some were of strings of numbers from elsewhere on a vehicle. Altogether, the scans generated 3,286 alarms, of which only 108 were considered "positive" in that both state and license plate number matched state and license plate number of the entry on the hot list (*see Figure 1*). Ultimately, only 17 scans triggered valid alarms, meaning that they led to an arrest; this translates to one valid alarm in 194 alarms registered by the LPR system. Despite automation, it is clear that the use of LPRs requires significant police work in comparing scans to hot list entries for verification. Meanwhile, the deterrence effect of police officers patrolling an area for stolen vehicles is disabled.

Figure 1. Alarms per LPR scans

Category	#	Rate per scan	Rate per alarm	Rate per positive alarm
Passive Scans	1,875,231			
Total Alarms	3,286	1 in 571		
Positive Alarms	108	1 in 17,364	1 in 31	
Valid Alarms	17	1 in 110,308	1 in 194	1 in 7

Source: Ohio State Highway Patrol, 2005

Because LPR scans can recognize specific identifiable information, if monitored in real time, officers can apply the data immediately to pursue the vehicle identified. Whether this technology is more effective than patrol officers working off a hot list has been tested. The Police Executive Research Foundation and the Mesa, Arizona, police department collaborated on a 48-week study to compare the results of LPR technology with those of manual license plate checks (Taylor, Koper, & Woods, 2010). Although LPRs resulted in more immediate arrests and locating stolen cars, the areas monitored by police patrol showed a long-term decrease in thefts, suggesting that the visibility of police officers busily checking plates worked as a deterrent (Vergano, 2011). Consequently, it would seem that the immediate recognizable benefit LPRs provide to conventional local law enforcement is retrieval of stolen automobiles, which is unlikely to be of use in the detection of terrorists.

IACP project manager Meghann Tracey confirms that the primary driver for police to purchase LPR systems is to retrieve stolen cars (2010). Officers are also attracted to LPRs because they allegedly allow for efficiency in traffic stops to capture lapsed registrations, revoked licenses, and persons with outstanding arrests: “The quantity of stops has gone down,” claims one state trooper, “because the quality of stops has gone

up" (2010). However, Tracey says, the technology's real strength lies in assisting investigations through the storage of license plate scans over time, allowing police to reconstruct the before and after movements of a person under suspicion of a crime that has already occurred.

If there is an argument for LPRs as crime prevention method, it remains elusive. By gathering license plate scans and storing them for analysis, police departments across the country are feeding information to regional data centers for intelligence agencies to possibly spot a pattern indicating terrorist intent. Police departments have come to view surveillance not as a tool to prevent or intervene in unlawful activity, but as a reactive mechanism to record all activity for undetermined and indeterminate use. The use of LPRs for building databases of license plate scans presents an enhanced ability to spy on individuals; the police department in Milpitas, California, with a population of 67,000, has stored 4.7 million license plate scans, meaning that residents are recorded over and over, providing an itinerary of their lives (Angwin & Valentino-Devries, 2012).

Unmanned aerial vehicles

Known more popularly as "drones," unmanned aerial vehicles have long been used by the military for surveillance and dropping bombs the world over. In the late 2000s, manufacturers such as AeroVironment, the U.S. military's largest supplier of unmanned aerial vehicles, began to eye the domestic market and identified local law enforcement as a potentially lucrative customer base (Gunderson, 2012). Unlike the Predator, made by defense contractor General Atomics, AeroVironment's UAVs are primarily "MAVs" – micro aerial vehicles such as the Qube, Wasp, and Raven. MAVs have wingspans of only

a few feet, weigh between one and four pounds, and are small enough to fit in a backpack or car trunk. While they are not weaponized, they are outfitted for surveillance with zoom lenses, infrared or thermal imaging cameras, and the capabilities to house radar and video analytics such as facial recognition (Stanley & Crump, 2011). These devices – other manufacturers include Honeywell and Draganfly Innovations – require far more hands-on operation, staff, and training than most sheriffs and police chiefs realize, and they are bound to specific flying rules. Departments seeking a cheaper and more nimble tool than a helicopter must consider that a UAV of this type – which costs between $40,000 and $200,000 – may fly at a maximum altitude of 400 feet and requires a trained pilot to operate the vehicle. Operators must follow the FAA's "line-of-sight" provision: the UAV must always remain in sight of its pilot (2011). Moreover, UAVs are prohibited in airspace over populated areas, airports, or harbors. MAVs are also limited to smooth sailing – they cannot withstand windy weather and many cannot fly at night or during low clouds. Flight time capabilities range from 10 to 110 minutes (2011; Gunderson, 2012; Thompson, 2012).

The first and to date primary use of UAVs in the U.S. has been by federal agencies such as Customs and Border Protection, the Drug Enforcement Administration, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives for surveillance – or *situational awareness* – along the U.S. border with Mexico. Police departments themselves most commonly first cite purposes of assisting in finding missing persons and monitoring traffic accidents. When Medina County, Ohio, was cleared to deploy a 2.2-pound drone in early 2013, the county sheriff Tom Miller offered the following justification: "About two or three times a year, we have maybe kids or seniors with

Alzheimer's who have walked away" (Nethers, 2013). Drones granted to Arlington, Texas; counties in northern Virginia; and elsewhere have all been funded with DHS anti-terrorist grants to police departments who did not articulate an anti-terrorist need. Instead, police officials tend to cite the protection of community members – even as they request technology that has to date only been used *against* people. For example, the deputy sheriff of Montgomery County, Texas, used a $300,000 DHS grant to purchase a Shadowhawk drone, made by military supplier Vanguard Defense Industries (Langford, 2011). He, too, cited the location of missing persons as an objective, as well as directing firefighters during forest fires. The Shadowhawk is weaponized for use in Iraq and Afghanistan and, while Deputy Sheriff Randy McDaniel insisted the county's version would not be, Vanguard can provide law enforcement the use of tear gas canisters, flares, smoke, and beanbag projectiles (2011).

Without the adherence to the simple IACP principle that requested technology comply with state law and regulations, many police departments eager to use UASI grants for UAVs may be unable to use them. In 2011, an unmanned aerial vehicle was purchased by Honolulu contractor responsible for port security to patrol the city's harbor without seeking permission from the Federal Aviation Administration (Dooley, 2012). The $75,000 drone had to be relegated to storage due to FAA guidelines that forbade UAVs from entering harbor airspace. In 2014, the San Jose, California, police department purchased a UAV with a $7,000 UASI grant, knowing full well it would not be able to use it because the department had yet to fill out an application with the FAA. The San Jose PD does already know how it will utilize its homeland security purchase: to help Bay Area bomb squads conduct threat assessments and to "inspect state parks and

wilderness areas for illegal vegetation" (Farivar, 2014). For its part, Arlington, Texas, received permission from the FAA to fly its two drones from Leptron Industrial Helicopters that it purchased with a UASI grant (Govers III, 2013). Home to the Dallas Cowboys, the Arlington police department requested the grant to provide security during potential Superbowls; however, it is against FAA rules to fly UAVs above crowds for safety reasons (Thompson, 2012). More everyday missions for the Leptron Avengers would be to locate missing persons and to take crime scene photos – neither having any preventive underpinning (Govers III, 2013).

Policing the public

> If [citizens'] trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe. (IACP, 2014, p. 2)

In the years after the 2001 terrorist attacks, police departments saw their funding from COPS eclipsed by funding from DHS; in 2008, according to the Office of Management and Budget, overall federal spending on counterterrorism led federal spending on crime prevention by 15 billion (as cited in Stewart & Oliver, 2014). A tendency to deemphasize public partnership as a paradigm was perhaps to be predicted. Post-9/11, policing mentality and tactics seem to have morphed from community policing to policing the community. Criminal justice researchers Kim and de Guzman believe the so-called "war on terror" awakened a paramilitary mindset among officers and paved the way for a shift to *homeland security policing* (2012, p. 323) – the current policing era.

Like previous major shifts in police strategy, this shift correlates with, and may be largely due to, new technology.

After the 9/11 terrorist attacks, the Homeland Security Grants Program spawned the implementation of general surveillance in every region of the country, regardless of risk, and usually without the transparency and approval of the public that research and the IACP *Framework* so emphatically recommend. Many urban ethnic and religious communities experienced additional invasive policing methods such as infiltration and street searches, which broke trusting relations established between community leaders such as imams and law enforcement (de la Peña, 2004). Considering also the bruised relationship between minority populations and the police sustained through previous policing methods, officers have arguably lost significant public trust in 21st century America, and thereby a crucial partner in preventing crime. A recent Gallup poll write-up titled "Confidence in Police Back at Historical Average" reported that 57 percent of Americans have confidence in the police (Norman, 2017). However, this headline and percentage reflects a growth only among older white Conservatives and Republicans. Confidence among blacks is at 30 percent and among Hispanics 45 percent; moreover, the past two years have seen drops among Liberals, Democrats, and 18- to 34-year-olds with confidence percentages of 39, 44, and 44, respectively (2017). This thesis does not mean to attribute these confidence level changes to surveillance technology usage but to point out that the trust considered vital to police functions, such as detection of terrorist activity in the community, is lacking.

The technological advancements introduced over the 20th century may have planted the seed for the remote and reactive policing favored today. The rise of telephone

dispatch encouraged motorized patrol, for example; instead of the community beat cop being on-site to deter crime, police car patrol became a mechanism of waiting to respond to crime (Byrne & Marx, 2011). Even at rest, automobiles introduced a physical barrier to the individual citizen and the lack of everyday interaction enabled a change in perception among officers and civilians from "us and them" to "us versus them." The introduction of general surveillance deepens the divide; civilians *en masse* have become police targets through the lens of assorted cameras permeating their neighborhoods and business districts. Police surveillance underlines the appearance that officers view the community primarily as a body of potential wrongdoers.

Surveillance technology manufacturers and law enforcement are quick to remind citizens they do not have a right to privacy in public. License plate readers record what is exposed on public streets. People cannot expect to be protected from video surveillance if visible to passers-by. However, the Fourth Amendment adds to a person's expectation of privacy that it be *reasonable*. Justice Harlan first articulated a "constitutionally protected reasonable expectation of privacy" in *Katz v. United States* (1967). Justice Harlan's two-fold test is "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable." People videotaped through open windows by police in a publicly parked car cannot reasonably expect privacy. If they retire to their bedroom, which faces the backyard, and see a five-pound, camera-equipped police quadcopter hovering at their open window, they may not be legally entitled to privacy, but it is hard to imagine that anyone would consider this reasonable.

Police chiefs have now had years of experience witnessing the pitfalls of deploying new police technology outside of a formal process such as the one proscribed by the IACP *Framework* (2014). Not involving the public in purchasing decisions and roll-out requirements, for example, and not making plain what purposes a given device might have, has in places caused anger and distrust among affected citizens toward local law officers. One week after the Seattle Police Department abandoned its plan to fly two unmanned aerial vehicles purchased with HSGP funds due to public outcry (Thompson, 2012; Clarridge, 2013), Seattle Mayor Mike McGinn invited the public to comment upon the purchase of 30 surveillance video cameras through a $5 million DHS grant (Clarridge, 2013b). The cameras had already been designated to shore up security along the city's waterfront and had already been installed; however, the mayor insisted on delaying their activation until Seattle residents could weigh in.

A better example of police-community collaboration is Oakland's 2014 creation of a Privacy Commission, an advisory body to guide City Council decisions on surveillance technologies proposed by law enforcement (Hofer, 2016). After participating in the decision to purchase such a system, Commission members work together with the Oakland Police Department in formulating transparency and privacy policies governing its implementation (2016).

Summary of main findings

The research conducted for this thesis illuminated that general surveillance does not function as a reliable deterrent of especially violent crime; surveillance cameras have in select studies shown small results in thwarting property theft, particularly of

automobiles. Instead, police implementations are using their new technology to add to their toolbox for the investigation of crime and locating already-identified suspects. According to a multi-site study on police implementations of technology in 2015,

> The effectiveness of technology is most often measured in the same way police effectiveness more generally is measured, by the ability to identify people to solve cases and make arrests. (Koper, Lum, Willis, et al, 2015, p. 144)

Police officers are also feeding the terabytes of data generated across the nation's LPR and CCTV systems as well as footage from the occasional UAV mission to the data centers established by DHS and manned by intelligence analysts seeking clues to terrorist activity. This does not make these technologies preventive of terrorism; rather, it makes local law enforcement into information providers for federal prevention efforts.

We have also witnessed how police agencies are responding to the availability of the Homeland Security Grants Program by applying because it is there and not out of perceived risk of terrorism to their locale. Because of lacking oversight and performance measures from FEMA, local police have had trouble neither in securing grants without showing cause nor in translating their funding into the gadgets they desire. These other objectives may align with policing principles but do not align with the mandate of DHS. With these results, it seems clear that instruments of public surveillance are not effective in achieving homeland security, even while in isolated cases they can serve as a deterrent to select crimes. It would seem that police are aware of the large gap between probability

of terrorism and the need for preventive measures and are taking advantage of DHS's police grants to serve other purposes.

Conclusion

Even though the terrorists' success in attacking the World Trade Center and the Pentagon that fateful Tuesday was widely blamed on the lack of cooperation between FBI and CIA (9/11 Commission, 2004) and even though it was an FBI field agent who wrote the Phoenix Memo to headquarters that warned of the strange behavior of Saudi Arabian flight school students in Minnesota (2004), Congress decided through the USA PATRIOT Act that, in the "war against terror," it was the role of local police officers that needed to be enhanced.

When lawmakers identified local police officers as best positioned to discover homeland threats, they argued it was because police officers are in touch with the people who live in the homeland. Street cops are physically present to witness human interaction and everyday routines. It is ironic, therefore, that the awards issued to local police departments have only served to create distance; sitting in cars, precincts, and fusion centers watching screens makes officers just as remote as the legislators in Washington. What local law enforcement agencies in cities, towns, even rural regions are paying ever-closer attention to is the data output of general surveillance devices – the reams of footage of innocuous activities and interactions of everyday citizens. Lacking real-time monitoring, the purpose of this output is to feed local DHS data centers, which does not benefit the communities being recorded. Stored data cannot deter crime or intervene where dangerous situations emerge, as a beat cop might. Remote and reactive technology

cannot serve as a "force multiplier" or replacement for human street patrol when the goal is prevention. The function of deterrence in crime-fighting is neglected – it does not serve the purpose of collecting personally identifiable data. If the goal is enhancing data profiles, preventive strategies are beside the point.

The finding that homeland security grants are obtained largely without believing in a local risk of terrorism ought to be discouraging for DHS and a reason to formulate better processes of evaluating grant proposals and risk assessments. It would also make sense to recognize that police are not terrorism experts – hardly anyone is, and given the lack of terrorism science, there is no basis for having law enforcement officials conduct their own risk assessments. Further, there is no basis for law enforcement to choose surveillance mechanisms for prevention; should surveillance be valuable for other policing purposes, that argument must be made through evaluation research, cost-benefit analyses, and consider Lum and Nagin's "citizen reaction matters" factor. Grounded in the IACP principles that demand the police act on behalf of the citizenry is the recommendation to return to an era of police officers enjoying the popularity of foot patrol (Kelling & Moore, 1988) and the deterrent effect of the uniform (Johnson, 1981) and getting to know their constituents. As Peel pointed out, police cannot execute their functions without "public approval of their existence, actions and behaviour" (Reith, 1948), and much of the public, particularly minority populations, lacks the requisite faith in today's policing.

Good policies governing the use of technology are anchored in public service and democratic principles, as proscribed by Peel (1829), COPS (2008), Lum & Nagin (2015), and the IACP (2014) to name but a few of those focusing on outcomes rather than output.

Innovation – whether in technology or policy – should advance goals of the people, not alienate them. “The core values that define us as a country are what make us strong as a nation,” says ACLU Chairman Anthony Romero (de la Peña, 2004). “They’re not a weakness.”

References

Angwin, J., & Valentino-DeVries, J. (2012, September 29). New tracking frontier: Your license plates. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB10000872396390443995604578004723603576296

BBC News. (2002, August 14). *CCTV not a crime deterrent*. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/2192911.stm

BBC News. (2009, August 24). *1000 cameras solve one crime*. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/england/london/8219022.stm

Bowcott, O. (2008, May 5). CCTV has failed to slash crime, say police. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2008/may/06/ukcrime1

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing: A review of the research on implementation and impact. *Journal of Police Studies 3*(20), 17–40.

Clarridge, C. (2013, February 7). Seattle grounds police drone program. *Seattle Times*. Retrieved from http://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program

Clarridge, C. (2013, February 15). City says it won't turn on 30 new cameras without public comment. *Seattle Times*. Retrieved from http://www.seattletimes.com/seattle-news/city-says-it-wonrsquot-turn-on-30-new-cameras-without-public-comment

Congressional Research Service. (2002, August 7). Homeland Security: Department Organization and Management Summary. Washington, DC: Library of Congress.

de la Peña, N. (Director). (2004). *Unconstitutional: The war on our civil liberties* [DVD]. New York: The Disinformation Company.

DHS Office of the Inspector General. (2012). *FEMA's requirements for reporting Homeland Security Grant Program achievements* [Report]. Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2012/OIG_12-92_Jun12.pdf

Dooley, J. (2012, April 10). State surveillance drone has never left the ground. *Hawaii Reporter*. Retrieved from http://www.hawaiireporter.com/state-surveillance-drone-has-never-left-the-ground/123

Earle, G. (2006, April 3). Mooseland security: Alaska town gets terrorcams while New York begs. *New York Post*. Retrieved from nypost.com/2006/04/03/mooseland-security-alaska-gets-terrorcams-while-n-y-begs

Farivar, C. (2014, July 30). Rare cop-owned drone in California could fly over Bay Area soon. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2014/07/rare-cop-owned-drone-in-california-could-fly-over-bay-area-soon

Govers, III, F. X. (2013, March 19). *FAA grants Arlington Police Department permission to fly UAVs*. New Atlas. Retrieved from http://newatlas.com/arlington-tx-police-uav-faa/26665

Gunderson, D. (2012, January 31). *Unmanned aircraft a controversial surveillance tool for N.D. law enforcement*. Minneapolis Public Radio. Retrieved from https://www.mprnews.org/story/2012/01/30/unmanned-aircraft-police

Hofer, B. (September 21, 2016). *How the fight to stop Oakland's Domain Awareness Center laid the groundwork for the Oakland Privacy Commission*. American Civil

Liberties Union of Northern California. Retrieved from https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission

International Association of Chiefs of Police. (January 2014). *IACP Technology Policy Framework*. Retrieved from http://www.theiacp.org/Technology

Johnson, D. R. (1981). Police reform: 1829–1860, in *American law enforcement: A history*. Wheeling, IL: Forum Press.

Kappstatter, B. (2011, July 29). Expanding network of security cameras is valuable crime-fighting tool. *NY Daily News*. Retrieved from http://www.nydailynews.com/news/crime/expanding-network-security-cameras-valuable-crimefighting-tool-nypd-commissioner-kelly-article-1.155861

Kelling, G. L., & Moore, M. H. (November 1988). *The evolving strategy of policing*. Washington, DC: Office of Justice Programs, National Institute of Justice.

Kim, M., & de Guzman, M. C. (2012). Police paradigm shift after the 9/11 terrorist attacks: The empirical evidence from the United States municipal police departments. *Journal of Crime, Law and Society*, *25*(4), 323–42.

Koper, C. S., Lum, C., Willis, J. J., Woods, D. J., & Hibdon, J. (December 2015). *Realizing the potential of technology in policing: A multisite study of the social, organizational, and behavioral aspects of implementing policing technologies* [Report]. Fairfax, VA: George Mason University Center for Evidence-Based Crime Policy.

Langford, C. (November 23, 2011). Unmanned drone is coming to Texas. *Courthouse News Service*. Retrieved from http://www.courthousenews.com/2011/11/23/41685.htm

Los Angeles Police Department. (nd). *Crime prevention: Design Out Crime*. www.lapdonline.org/crime_prevention/content_basic_view/8852

Lum, C., Haberfeld, M., Fachner, G., & Lieberman, C. (2011). Police activities to counter terrorism: What we know and what we need to know, in *To protect and to serve: Policing in an age of terrorism* (eds. Weisburd, Feucht, Hakimi, Mock, & Perry). New York: Springer Verlag.

Lum, C., Kennedy, L. W., & Sherley, A. (2008). Is counter-terrorism policy evidence-based? What works, what harms, and what is unknown. *Psicothema, 20*, 35–42.

Lum, C., & Nagin, D. (2015, June 24). *Reinventing American policing*. The Crime Report. Retrieved from https://thecrimereport.org/2015/06/24/2015-06-reinventing-american-policing-a-seven-point-blueprin/

Marin, C., & Moseley, D. (2012, January 9). Feds find failures in Cook Co. homeland security project. *Chicago Sun-Times*. Retrieved from https://www.prisonplanet.com/feds-find-failures-in-cook-co-homeland-security-project.html

McCaul, M., & Keating, B. (2014, March 27). How did Tsarnaev go off FBI radar? [Op-Ed]. *Boston Globe.* Retrieved from http://www.bostonglobe.com/opinion/2014/03/27/missed-opportunities-lessons-learned-year-after-marathon-bombings/ztVLvM1SFyzaVtf1oI6AyN/story.html

Nethers, D. (2013, February 12). Drone technology authorized for use by local police. *Fox 8 News*. Retrieved from http://fox8.com/2013/02/12/drone-technology-for-police-authorized

Newman, G. R., & Clarke, R. V. (2008). *Policing terrorism: An executive's guide.* Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.

Norman, J. (2017, July 10). *Confidence in police back at historical average* [Poll]. Gallup. Retrieved from http://www.gallup.com/poll/213869/confidence-police-back-historical-average.aspx

Ohio State Highway Patrol Research and Development. (February 2005). *Automatic license plate reader technology* [Report]. Ohio State Highway Patrol.

O'Sullivan, J. (2014, June 8). State gets millions in homeland security grants, but where does it go? *Rapid City Journal*. Retrieved from http://rapidcityjournal.com/news/local/state-gets-millions-in-homeland-security-grants-but-%20where-does/article_1be9acf1-b8e6-5bdb-a01d-5d2e4e2362ca.html

Office of Homeland Security. (July 16, 2002). *National Strategy for Homeland Security*. Washington, DC: The White House. Retrieved from https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

Office of Senator Tom Coburn. (December 2012). *Safety at any price* (Report). Retrieved from http://info.publicintelligence.net/SenatorCoburn-UASI.pdf

Powers, M. (2014, February 11). New cameras keep watch on MBTA buses. *Boston Globe*. Retrieved from http://www.bostonglobe.com/metro/2014/02/11/begins-installation-bus-security-cameras/Z1QwILHvLb3TgsgOPXa9yM/story.html

Reese, S. (2012, February 3). *Is DHS Effectively Implementing A Strategy to Counter Emerging Threats?* [Testimony]. Congressional Research Service. Retrieved from http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Reese_0.pdf

Reith, C. (1948). Peel's principles of policing, in *A short history of the British police*. London: Oxford University Press.

Schlosberg, M., & Ozer, N. A. (August 2007). *Under the watchful eye: The proliferation of video surveillance systems in California* [Report]. ACLU California. Retrieved from https://www.aclunc.org/publications/under-watchful-eye-proliferation-video-surveillance-systems-california

Schneider, J. (2014, July 22). *NYPD's Miller: No likely terror connection in Brooklyn Bridge white flag placement*. CBS 2. Retrieved from http://newyork.cbslocal.com/2014/07/22/police-investigating-mysterious-white-flags-on-brooklyn-bridge

Smith, G. B. (2014, July 8). Behind the smoking guns: Inside NYPD's 21st Century arsenal. *New York Daily News*. Retrieved from http://creative.nydailynews.com/smokingguns

Stanley, J., & Crump, C. (December 2011). *Protecting privacy from aerial surveillance: Recommendations for the government use of drone aircraft*. ACLU. Retrieved from aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Stewart, D. M., & Oliver, W. M. (2014). The adoption of homeland security initiatives in Texas police departments: A contextual perspective. *Criminal Justice Review*, 1-

19. Retrieved from https://doi-org.ez.lib.jjay.cuny.edu/10.1177/0734016814551603

Taylor, B., Koper, C., & Woods, D. (2010). *Combating auto theft in Arizona: A randomized experiment with license plate recognition technology*. Washington, DC: Police Executive Research Forum.

Thompson, L. (2012, May 2). Police apologize for not keeping council in loop on new drones. *Seattle Times*. Retrieved from http://www.seattletimes.com/seattle-news/police-apologize-for-not-keeping-council-in-loop-on-new-drones/

Treverton, G. F., Wollman, M., Wilke, E., & Lai, D. (2011). *Moving toward the future of policing*. Santa Monica, CA: RAND Corporation.

Tracey, M. (June 2010). *Using license plate readers to fight crime* [IACP presentation]. Washington, DC: National Institute of Justice. Retrieved from https://nij.gov/multimedia/pages/audio-nijconf2010-license-plate-readers.aspx

U.S. Government Accountability Office. (February 2007). *Homeland security grants: Observations on process DHS used to allocate funds to selected urban areas* [Report GAO-07-381R]. Retrieved from http://www.gao.gov/products/GAO-07-381R

U.S. Government Accountability Office. (June 2008). *DHS risk-based grant methodology is reasonable, but current version's measure of vulnerability is limited* [Report GAO-08-852]. Retrieved from http://www.gao.gov/products/GAO-08-852

U.S. Government Accountability Office. (March 2013). *National Preparedness: FEMA has made progress in improving grant management and assessing capabilities,*

but challenges remain [Report GAO-13-456T]. Retrieved from http://www.gao.gov/products/GAO-13-456T

Vergano, D. (2011, December 27). Auto-theft cops go head-to-head with license plate readers. *USA Today*. Retrieved from content.usatoday.com/communities/sciencefair/post/2011/12/license/1

Welsh, B. C., & Farrington, D. P. (2008). *Effects of improved street lighting on crime*. Oslo, Norway: The Campbell Collaboration. Retrieved from https://www.campbellcollaboration.org/media/k2/attachments/Welsh_Streetlight_review_corrected.pdf

9/11 National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. New York: W. W. Norton & Company.

Appendix

Table 1. *IACP Technology Policy Framework*: Universal Principles		
1	Specification of use	Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2	Policies and Procedures	Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3	Privacy and Data Quality	The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4	Data Minimization and Limitation	The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be

		deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5	Performance Evaluation	Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6	Transparency and Notice	Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are practical and legal exceptions to this principle for technologies that are lawfully deployed in undercover investigations and legitimate, approved covert operations.
7	Security	Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks

		and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI's CJIS Security Policy), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.
8	Data Retention, Access, and Use	Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9	Auditing and Accountability	Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-

		compliance should be defined and enforced.
Source: IACP, 2014		