

Technology Ethics for Law Enforcement

Lieutenant Joe Peny

Armstrong Police Department
11935 Abercorn Street
Savannah, GA 31419, USA.

Abstract

This paper explores the different aspects of ethics and unethical behavior for law enforcement officers at all levels in reference to the use of technology. Technology has enabled law enforcement to respond more quickly to calls for service, use more advanced non-lethal compliance tools, and use the Internet to combat crime. The foundation of ethical practices is based on the Fourth Amendment of the Constitution supplemented by the courts of the United States delivering decisions that affect the use of technology by law enforcement officers and administrators. Using these guidelines, officers are expected to complete their daily duty assignments with the use of technology both legally and ethically. An officer's ethical foundation and training allow them to exercise discretion in the enforcement of laws, sometimes blurring the line between what is ethical and legal.

Keywords: ethics, Fourth Amendment, unethical behaviors

Ethics is the ability to make a distinctive choice between what is right and what is wrong. Law enforcement officers use their discretion when the benefit of society outweighs the letter of the law. When it comes to technology, there is no 'technology ethics', just ethical situations that involve technology (Kallman & Grillo, 1993, p. 3). Technology allows unethical acts to be facilitated faster than before and can be more difficult to detect. Although most ethical values are learned throughout childhood, other ethical values are guided by laws and customs based on the ethical values that are reflected by society's expectation of behavior. A law enforcement officer experiences conflict when his/her personal ethical beliefs contradict or differ with an existing rule or law.

Ethics have always been the foundation of law enforcement. Law enforcement officers use laws and policies to guide their professional behavior but have a great deal of discretion when it comes to enforcing those laws. Officers undergo ethics training due to the nature of this authority and the potential of liability. Law enforcement officers are held to a higher standard by society twenty-four hours a day, seven days a week, and for the remainder of their life. Their actions, if unethical, can damage the public's trust of police and tarnish the profession as a whole (Wyatt-Nichol & Franks, 2009). Unethical behavior can produce civil lawsuits against a department or administration. In *Ohio v. Harris*, 489 U.S. 378 (1989), the United States Supreme Court decided that cities and their administration can be held liable if the violation of someone's constitutional rights occurred from a lack of ethics training (Wyatt-Nichol & Franks, 2009). Members of the law enforcement community believe that ethics training bridges the gap between organizational policy and the actions of the officers, by introducing or reinforcing rules and behavioral expectations (Wyatt-Nichol & Franks, 2009). Proper training of ethics in policing is a vital component of any law enforcement agency and the absence of such training is a poor reflection of the entire policing culture.

Ethics in Technology

A relatively new component of ethics training concentrates on the use of technology. Technology can be seen in the vehicles on the highway, the weapons and tactics that are used by law enforcement, and the way the world communicates. For law enforcement, it also means learning how to investigate crimes in a digital age, legally, as well as ethically. But exactly what is technology? Technology, according to an article in the *Ohio Journal of Science*, transforms the "natural world through innovative processes, systems, structures and devices to extend human abilities" ("What are Science, Technology and Engineering?," 2011, p. 66). With the aid of engineering, technology has defined civilization through the ages, such as the use of stone tools during the Stone Age and the use of iron in the Iron Age ("What are Science, Technology and Engineering?," 2011, p. 66).

Now that we are in the Information Age, information has replaced the natural resources that have shaped our social, environmental, and economic structure. Law enforcements application of technology increases the capability of policing throughout the world. Since the mid twentieth century, technology has played a progressing role in the way officers perform their daily duties. With the invention and adaptation of the motorized vehicle for widespread patrols and the telephone that provided a quicker reporting of crimes, technology has not only aided the police in the execution of their duties, but has provided another avenue in which ethical behaviors have to be monitored (Kappeler, 2006). For example, it would not be ethical for an officer to break the state mandated speed limit while not in the execution of his/her official duties. With every new tool invented, it brings along with it an innate responsibility to use that tool in an ethical way.

Although the advancement of technology is essential for the progression of the social order, society does not view change with open and enthusiastic arms. Most inventors use the technological imperative that simply states that “if it can be done, it will and perhaps should be done” (Kilpatrick, 2010, p. 568). One example of this would be human cloning. By using the technological imperative, human cloning should be done because humankind has the ability to do so. It should not matter who agrees or disagrees, according to this maxim (Kilpatrick, 2010). One of the possible arguments for such an act would be to use the process solely for medical purposes, similar to organ farming (Kilpatrick, 2010). “Faced with possibilities and even probabilities that are unacceptable, we humans must establish widely agreed upon worldwide standards for ethical and moral decision-making in technology”(Kilpatrick, 2010, p. 568).

The role of technology in our society has ethical considerations that are not as unique as one may think. Technology enhances our everyday lives by making tasks convenient. By using technology unethically, crimes such as harassment or bullying have evolved from being confined to a specific location and time to being passed continuously through social media outlets. Instead of stalking an individual from across the street, a predator can stalk his/her prey from afar by utilizing a social network via mobile phone and/or computer. Law enforcement must not only cope with these new avenues of how crimes are committed, but also stay within ethical boundaries during their own use of technology. Using the National Crime Information Center (NCIC) or various states CIC’s to determine the name and address of an individual for personal reasons is not only a violation of the law but also an ethical violation as well.

Tools of Law Enforcement

Among the tools commonly issued to law enforcement officers are the semi-automatic pistol, a collapsible baton, Oleoresin Capsicum spray (commonly referred to as OC spray), and the taser. The pistol that is carried by law enforcement is drastically different than the sidearm that was carried forty years ago. The six shot revolver has been replaced with the fifteen round semi-automatic hand gun. The ‘Billy’ club of old has been replaced with a steel collapsible baton. OC spray is carried by law enforcement and delivers a blast of chemicals to the eyes of a suspect leaving them disoriented and usually compliant. The taser is a weapon that delivers 50000 volts to its target, completely immobilizing the subject until they can be brought under control. With the exception of the pistol, these tools are non-lethal and used at various levels of non-compliance. Each of these tools has unique characteristics that the officer must be trained on, to include their proper and ethical use; although not every legal use is viewed as ethical by society.

Pepper Spray

During the month of November, several peaceful protests around the country were being held as the Occupy Wall Street movement. In Seattle and the University of California, Davis, protesters were sprayed with OC spray during a passive protest. “The use was just absolutely out of the ordinary and it was not in accordance with any training or policy of any department that I know of” (Loghman, 2011 p. 1). There is little doubt that the use of Oleoresin Capsicum can be useful in situations where individuals are violent or have some sort of weapon; however, designating pepper spray where suspects are vocally resistive seems unreasonable and could even be seen as a form of abuse (Otto & Jos 2004).

Taser

In September of 2007, Massachusetts Senator John Kerry was giving a speech at the University of Miami. In attendance at the speech was Andrew Meyer, a University of Florida student who was given the opportunity to ask the senator a question. After asking three questions, he was escorted to the rear of the auditorium by two police officers where he began to passively resist (Wu, 2010).

The officers, three by this time, pinned him to the ground and one of the officers removed his taser from his holster. Meyer screamed that he didn't do anything and "Don't tase me, bro" (Wu, 2010, p. 362). Subsequently, the officer tased and arrested Meyer for resisting arrest and disorderly conduct and spent the night in jail. Upon his release, he apologized and all of the charges were dismissed (Wu, 2010). The legal precedence for tasing did not occur for another two years with *Bryan v. McPherson*, 590 F.3d 767 (2009).

During the summer of 2005, Carl Bryan was driving across southern California when he was stopped by a law enforcement officer for speeding. After receiving his citation from the California Highway Patrol, Bryan continued on his journey to Coronado (Wu, 2010). When Bryan reached Coronado, he was stopped by Coronado Police at a seat belt enforcement check point. Bryan, angry with himself for not placing his seatbelt back on from his previous encounter with law enforcement, got out of his vehicle and began to curse himself. Officer McPherson, who was approximately twenty-five feet away, ordered Bryan to return to his vehicle. He did not comply, so McPherson tased him (Wu, 2010). Bryan fell to the asphalt and broke four of his teeth. The state dismissed the charge of resisting arrest after his trial resulted in a hung jury (Wu, 2010).

Bryan subsequently sued McPherson, the Coronado Police Department, and the city of Coronado for excessive use of force in violation of 42 U.S.C. § 1983. The Ninth Circuit rendered the decision that McPherson's use of the taser was unconstitutional because the officer safety need was not met (Wu, 2010).

Traffic Cameras

One such technology tool is the traffic camera. Traffic cameras are generally located at busy intersection in an effort to capture evidence of traffic violations such as running a red light. The system records the offense, accesses a fixed penalty ticket, and notice of intended prosecution (NIP) that is then mailed to the owner of the vehicle that is involved (Cooper, 2010). The camera does not consider external factors such as weather or traffic conditions. It does not entertain the reasoning behind the exceeding of the state mandated speed limit (Cooper, 2010). The traffic cameras are considered to be fair in the fact that it captures the offense and generates a citation (NIP) without any kind of discrimination that may be perceived by an officer-generated traffic stop. It does not consider age, race, or gender or any relevant explanation or excuse in its decision making process (Cooper, 2010). This robotic approach to traffic law enforcement is viewed by many to be unjust. "This is of importance because the perceived fairness of law enforcement systems is a key factor in shaping public support for both the police service and the criminal justice system itself" (Cooper, 2010, p. 412).

As the procedure progresses, the photographic evidence and the pre-generated citation have already established that the driver is guilty of the offense. The reason citizens express that this is unjust is because they have been labeled as guilty and convicted without due process. The leaflet contains phrases such as "you broke the law" and "no matter how you try to justify it . . . you're about to be prosecuted" (Cooper, 2010, p. 413). This verbiage conveys that the driver has already been tried and convicted of the offense. One way to improve the justness of the process would be to re-word the leaflet that is summarily sent to the registered owner of the vehicle (Cooper, 2010). Perhaps stating that 'your vehicle was involved in a traffic infraction' or that the citation is an administrative ticket and not a criminal ticket and there would be no points against the driver's license would be viewed as less accusatory and offensive. Another suggested way to 'humanize' this procedure is to offer the driver the opportunity to voice their rebuttal and have their say. If given an opportunity to explain their actions, drivers could provide a representation of the circumstances of the incident (Cooper, 2010). Then, if they are found to be guilty, society as a whole would feel less resentful toward the police and the entire criminal justice system (Cooper, 2010).

Truth Serums

Another such technology is the use of truth serum on suspects to gain intelligence. The United States had experimented with administering truth serums in forensic hypnosis by police in the 1970's and by psychotherapists in the 80's and 90's in an attempt to recover repressed memories of child abuse victims (Kaur, 2010). In a report submitted by the United States National Defense Intelligence College in 2006, it stated that although a person under the influence of 'truth' serums became more talkative, there was no evidence that they were providing accurate information (Kaur, 2010).

Even if these ‘truth’ serums produced accurate truths, their use in the United States would violate an individual’s Fifth Amendment right against self incrimination (Kaur, 2010). In 1963, the US Supreme Court ruled in *Townsend v. Sain*, 372 U.S. 293, which confessions produced as a result of ingestion of truth serum were “unconstitutionally coerced”, and therefore inadmissible (*Townsend v. Sain*, 1963). The use of this technology had been suspended but, as a result of the terrorists’ attacks of 9/11, the discussion of the use of truth serum to extract information from terrorists has again brought societal focus to the topic.

In contrast, countries such as India, the usage of narcoanalysis are common. In March 1992, the body of a young nun was found in a well near her convent in Kerala, India. At first it was ruled to be a suicide, but further investigations by the Central Bureau of Investigation (CBI) changed the suicide explanation to homicide. The CBI made three arrests in the case, two priests and one nun. The suspects were interviewed, but only after they received injections of barbiturates (Kaur, 2010). This narcoanalysis uses chemicals such as sodium pentothal that control the nervous system and greatly reduces the ability to make false statements. Dr. B.M. Mohan of the Bangalore Forensic Science Laboratory has stated that this process has between a ninety-six and ninety-seven percent success rate (Kaur, 2010).

Others have argued that the use of narcoanalysis allows the subject to be vulnerable to suggestions (Kaur, 2010). The effects of drugs similar to sodium pentothal have been described as hypnotic, anesthetic, and results in a state of virtual drunkenness (Kaur, 2010). Dr. Amar Jesani wrote in the *Indian Journal of Medical Ethics* that “there is enough scientific evidence to show that a person under the effect of a drug often plays along with the suggestions made by the interrogator” (Kaur, 2010, p. 119). It is for this reason those opposed to the use of truth serums to gain a confession base their objections. Since a person is subject to coercion, false confessions are a possibility. One senior officer for the Indian Police stated that he could get a suspect to confess to anything using this method (Kaur, 2010). Indian officials state that narcoanalysis is only used in high profile cases and consent is given by the subjects (Kaur, 2010).

Undercover Operations

Law enforcement agencies use other forms of technology in the performance of their duties. One such area is commonly known as the investigative division. While the preliminary investigations are conducted by the beat cop, such as taking the initial report and speaking with witnesses, detectives are assigned to perform follow-up investigations as well as processing physical evidence (Joh, 2009). When they are called to a crime scene, detectives process the scene by photographing, seizing, and inventorying any and all evidence. They will dust for fingerprints, collect DNA samples, and track property. Detectives may even need to infiltrate an organization in an effort to gather valuable evidence that can later be admissible in court (Joh, 2009). An undercover operation involves the officer misrepresenting him/herself in order to infiltrate a particular group or organization for the purpose of a criminal investigation (Joh, 2009). This undercover operation, being based on deception, can lead to the officer participating in activities that appear to be or are actually illegal, such as introducing drugs to prisons, laundering money, and committing perjury (Joh, 2009). Tools that are commonly used in these operations include audio and video surveillance in addition to manufactured identification documents and backgrounds (Joh, 2009).

There are basically three basic types of undercover operations: surveillance, prevention, and facilitation (Joh, 2009). The role of surveillance is to gather information about a completed, ongoing, or planned crime (Joh, 2009). Officers may be placed in a particular location and advised to report any suspicious activity to uniformed officers (Joh, 2009). Prevention undercover operations are used to prevent a particular crime from being committed (Joh, 2009). An example of an officer in this prevention undercover assignment may include being inserted in the midst of a protest advocating for non-violence (Joh, 2009). When an officer is involved in the facilitation mode of undercover operations, they are attempting to encourage illegal or illicit behavior (Joh, 2009).

The facilitation phase of undercover investigations is the most ethically challenged (Joh, 2009). Officers may have to commit crimes in an effort to maintain their anonymity. They may have to purchase drugs to convince a dealer that they are not an informant or ‘narc’ or pretend to be a minor on the Internet in order to catch a sexual predator. When these cases are prosecuted, one of the most common defenses is entrapment (Joh, 2009). The defense of entrapment is applicable when a law enforcement officer, or his agent, induces a person to engage in conduct that he/she is not otherwise ready to commit and has the willingness to do (Joh, 2009). In *State v. Bullock*, 153 S.W.3d 882 (2005), the defense of entrapment was used by stating that the defendant was misled by the undercover agent in the solicitation sex from an underage female on the Internet (Joh, 2009).

The defendant was having internet conversations with a sheriff's deputy that was under the guise of a thirteen year old female (Joh, 2009). The Court of Appeals affirmed the conviction stating that entrapment was not committed by the sheriff's deputy in this case because the defendant was willing to commit the acts of statutory rape and solicitation of a minor (Joh, 2009).

Mobile Devices

One clear indicator of progressing technology is the ever changing mobile phones or devices. New and improved smart phones and digital media pads appear on the market nearly every six months. With this technology, these devices can take photographs and record videos, send and receive messages in real time, and surf the Internet almost instantaneously. This rapid exchange of information has presented new dilemmas for law enforcement officers.

In Pennsylvania, a high school teacher confiscated a mobile phone from a student because it violated the school policy that prohibited the display of mobile phones (Zirkel, 2005). Once the phone was taken, the teacher and the assistant principal searched the phones contents to include text message content, voicemail, and contacts (Zirkel, 2005). They also made several calls to other students and sent out Instant Messages via America Online (Zirkel, 2005). Prior to returning the phone, they deleted the phone calls and the messages. The parents of the student sued the teacher, assistant principal, and the school board for violation of their child's Fourth Amendment protection against unreasonable searches and seizures (Zirkel, 2005). As a result, the United States District Court For The Eastern District of Pennsylvania decided that the school system was in violation of the student's Fourth Amendment protection because they had no grounds on which to search the phone (*Klump v. Nazareth Area School District*, 425 F. Supp. 2d 622) (Zirkel, 2005).

Law enforcement officers have been challenged in nearly all aspects of mobile media searches. In *United States v. Quintana*, 594 F. Supp. 2d 1291 (2009), Quintana was stopped for speeding (Warfeild, 2010). Once stopped, the officers could smell the odor of raw marijuana but could not find more than a minute amount. It was discovered that his license had been suspended and he was arrested at the scene (Warfeild, 2010). While in custody, the officers searched his cellular phone in hopes of identifying incriminating evidence against Quintana. Quintana's phone possessed incriminating photographs that lead to a search of his home and the home of a friend (Warfeild, 2010). Quintana's claim that this search was unconstitutional was upheld by the court because the search was not a factor of officer safety or related evidence to the criminal arrest (Warfeild, 2010).

Internet

Technology has aided in the gathering, storing, and sharing of vast amounts of information, unfortunately it has facilitated crimes such as the possession and sharing of child pornography. Prior to the Information Age, sexual deviants that participated in the child pornography trade used mediums like face-to-face meetings and the Postal Service. Photographs that were taken had to be developed in a private dark room to avoid detection. Law enforcement had a difficult time locating the meetings or intercepting the photographs of the young victims. Currently, the Internet is in nearly every home and can be accessed via computer or phone. Information and pictures can be distributed to an infinite number of recipients in a matter of moments. Law enforcement officers are faced with a greater dilemma in their attempt to catch these pedophiles.

The child pornography trade is a global issue as a result of the World Wide Web. Collectors, as they call themselves, reside in possibly every city and country around the world (Wells, 2007). This in itself creates a problem of jurisdiction when investigations are being conducted (Wells, 2007). Another issue is that there is no common definition of the crime and no universal reporting process that provides statistical data in regards to child pornography. Even within the United States, there is no clear uniform definition of child pornography (Wells, 2007). Federal law defines a child as a youth under the age of eighteen (Wells, 2007). Further, child pornography is defined as photographs and videos of conduct that is sexually explicit (Wells, 2007). Some states have adopted similar definitions and the interpretation is broad, causing difficulty in specifically defining the crime (Wells, 2007). Since the exchange of child pornographic material normally crosses jurisdictions, law enforcement officers must find alternate means to combat this predator based crime (Wells, 2007). Agencies must work together on interagency task forces such as the Internet Crimes Against Children (ICAC) that polices the Internet by enhancing the investigative response to technology facilitated crimes against children.

Another way to combat the child porn industry is the use of tip lines such as the Cyber Tipline that was began in 1998 by the National Center for Missing and Exploited Children (Missing kids, 2011). The CyberTipline is Congressionally-mandated and is a means for reporting crimes against children including possession, manufacture, and distribution of child pornography, online enticement of children for sexual acts, child prostitution, sex tourism involving children, extra familial child sexual molestation, unsolicited obscene material sent to a child, misleading domain names, and misleading words or digital images on the Internet (Missing kids, 2011). According to the National Center for Missing and Exploited Children, there have been 1,226,000 reports that involve the possession, manufacture, and distribution of child pornography and various online sexual crimes against children in the United States alone (Missing kids, 2011).

Law enforcement officers utilize tip lines like CyberTipline to initiate child pornography investigations. Officers use both traditional investigative techniques such as responding to reports and the use of undercover operations. In these undercover endeavors, officers may pose as consumers attempting to purchase images, collectors of child pornography images, or attempt to infiltrate a child porn bulletin board service (Wells, 2007). Undercover sting operations have been used successfully in the investigation and prosecution of child pornography cases (Wells, 2007). Officers use deceptive techniques in an effort to gain the trust of the suspected offender and subsequently gather evidence against him. This evidence is then used in the prosecution of the unwary suspect. Although many view that the undercover aspect of police work is unethical, the U.S. Sentencing Guidelines Manual § 2A3.2 was amended in 2000 to read that a victim is an individual who has not attained the age of 16 years of age or an undercover law enforcement officer who represented to a participant to be under or at the age of 16 years, showing governmental support for the deception (Clancy, 2010).

The Fourth Amendment

Whether it is a search of a computer or of a person, the Fourth Amendment of the Constitution is still applicable. The Fourth Amendment states:

The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (United States Constitution).

When considering a case under a Fourth Amendment violation, the following questions must be answered: does the government search or seizure violate a person's reasonable expectation of privacy and is the privacy accepted by society as reasonable (Clancy, 2010).

Full Body Imaging

This has been the focal point of debate against the use of full-body imaging at airports. Since the failed terrorist attempt on December 25, 2009 by Al-Qaida operative Umar Farouk Abdulmutallab, U.S. airports have increased their security measures by installing full-body or Advanced Imaging Technology (AIT) scanners in an effort to detect weapons or explosives (Lombard, 2010). These scanners produce virtually naked images of passengers using either low frequency radio waves or weak X-rays. Commentators have viewed this procedure as a virtual strip search and therefore a violation of their Fourth Amendment right against unreasonable searches (Lombard, 2010).

Despite the Fourth Amendment's requirement of probable cause, the Supreme Court has determined that limited exceptions exist. The airports' administrative searches operate within the guidelines of the Fourth Amendment "as long as they are part of a greater regulatory scheme targeted at a particular group of people instead of a single person" (Lombard, 2010, p. 352). The government may intrude upon individual privacy to conduct an airport search despite a lack of reasonable suspicion, the precursor to probable cause (Lombard, 2010). Accordingly, courts consistently maintain the constitutionality of warrantless airport searches on the basis of administrative necessity (Lombard, 2010). The government must conduct such searches to safeguard the public's safety and to protect the public in instances where the threat of harm is both genuine and substantial. In an effort to curb the privacy issue, legislation has been introduced such as the Whole Body Imaging Limitations Act of 2009 that would make the all-body scans a secondary scan only if the individual was identified by a magnetometer (Lombard, 2010).

The act would also allow the passenger to voluntarily undergo a pat down search and make it a criminal offense for “any government employee who knowingly stores, transfers, shares, or copies images produced by AIT scanners” (Lombard, 2010, p. 343). Since United States citizens have grown accustomed to the heightened security levels at airports and the fact that they choose to use the airline, the courts have determined that by acquiring a ticket and attempting to get on the plane demonstrates implied consent to the strict screening practice (Weinberger, 2010). Case in point is *United States v. Aukai*, 440 F.3d 1168, 1172-73 (9th Cir. 2006). Aukai attempted to withdraw implied consent during a routine airport screening process while attempting to board a plane in Hawaii. The Ninth Circuit Court ruled that he could not revoke consent because consent was not required for the search, it was implied (Lombard, 2010).

Facial Recognition Technology

Another area of controversy is the use of face recognition technology (FRT). This technology can take a photograph of a person, run the image through a database, and access virtually any biographical or financial information once the image has been identified (Hale, 2005). The process begins by seizing the image from a security type camera. The system then measures nodal points on the face such as the shape of the cheekbones, the distance between the eyes, and other facial features (Hale, 2005). Then, these points are compared to images in the database to locate a match. In London, where FRT cameras have been on city streets since 1998, FRT is used to track movements of individuals throughout the city (Hale, 2005). FRT camera systems are used in the United States at major sporting events like the Super Bowl, in casinos to spot cheaters, and in malls around the country (Hale, 2005).

With the increasing use of facial recognition technology, there are those that are worried that this ‘big brother’ syndrome will be an invasion of privacy and prevent society to act with its own free will. Autonomy is the ability to act ethically by one’s own decision to do so (Hale, 2005). The loss of autonomy is inevitable if cameras litter the streets, logging our every move and action, and causing society to act not of its own accord but because of fear of disobeying institutionally enforced laws (Hale, 2005).

Another component of facial recognition technology is the method of microfacial expressions. Paul Ekman, a psychology professor at the University of California Medical School in San Francisco, developed the ‘facial action coding system’ for analyzing human facial expressions that places emphasis on uncontrollable facial movements such as a tensing of the lips or the raising of the brow (Weinberger, 2010). According to Ekman, these movements can be used to determine if someone is telling a lie. The theory is met with much skepticism, but Ekman states that he has a minimum of a seventy percent success rate (Weinberger, 2010).

Global Positioning System

The Global Positioning System (GPS) is another example of tracking technology. The GPS uses satellites to determine location and time of the receiving device. This system has many practical uses in today’s society. It is used by air traffic controllers, military personnel, and citizens on a daily basis when searching for a point of interest or any other destination. Law enforcement can use this technology to track mobile phones in the event of a kidnapping or hostage situation; however, the technology can also be abused. Neither the United States Supreme Court nor Congress has provided clear direction in the use of GPS devices (Smith, 2011). Most federal courts have viewed the use of GPS devices does not invoke the protections of the Fourth Amendment (Smith, 2011). In *United States v. Maynard*, 615 F.3d 544, 566 (D.C. Cir. 2010), the United States Court of Appeals for the District of Columbia took a proactive look and held “that warrantless, prolonged use of a GPS device to track a defendant’s movements violated the defendant’s reasonable expectation of privacy” (Smith, 2011, p. 1244).

History of Electronic Surveillance

The first case involving electronic surveillance reached the United States Supreme Court with *Olmstead v. United States*, 277 U.S. 438 (1928). The Court decided that the tapping of an individual’s telephone lines did not violate the Fourth Amendment (*Olmstead v. United States*, 1928). The reasoning the Court used was that there was no entry made into the dwelling or offices of the defendants; simply, no place was searched and no evidence was seized. It would take nearly fifty years for the Supreme Court to resend their decision (*Olmstead v. United States*, 1928). In 1967, the United States Supreme Court overturned the *Olmstead* decision and decided that Fourth Amendment protection against unreasonable searches and seizures did not protect places, but people.

In *Katz v. United States*, 389 U.S. 347 (1967), Federal Bureau of Investigation agents attached an electronic listening device to a public phone booth and recorded private phone calls. The Supreme Court decided that even though the phone booth was considered public, the person using the booth to either place or receive a telephone call possessed a reasonable expectation of privacy (*Katz v. United States*, 1967). As a result, Congress passed the Omnibus Crime Control and Safe Streets Act in 1968 that prohibited wiretapping and electronic eavesdropping except under strict limitations; however, Title III, Section 2511 allowed warrantless wiretaps for the sake of national security. This form of eavesdropping for the collection of foreign intelligence was distinctly different than what was being done by law enforcement in a criminal investigation (Young, 2011). The national security exception stated that the President could take whatever measures needed to protect the nation from potential attacks, hostile acts, or an attempt to overthrow the government by force or other unlawful means (Young, 2011).

As a result of the federal government's wiretapping of a "domestic radical group in a conspiracy to destroy federal government property" without a warrant, the Congress amended the President's authority with the creation of the Foreign Intelligence Security Act of 1978 (FISA) (Young, 2011, p. 16). This allows for a judicial review and approval for wiretaps and other electronic surveillance used for foreign intelligence gathering (Young, 2011). After the attacks of 9/11, FISA was criticized for not allowing proper intelligence gathering and limiting law enforcement efforts. Congress responded with the PATRIOT Act. The focus of the evidence gathering was changed from a "sole-purpose test" to a "significant-purpose test" (Young, 2011, p. 17). Law enforcement and intelligence gathering could both be used as a result. Online government surveillance is governed by whether the information is within a closed space or a public space (Young, 2011). If in an enclosed space, the 'search' is governed by the Fourth Amendment. If information is in a public space, it does not fall under Fourth Amendment protections (Young, 2011).

The majority of law enforcement officers are considered to be "digital immigrants" (Young, 2011, p. 23). Officers were conducting investigations prior to the Information Age and the technology is a new tool that can be used. On the other hand, the younger "digital natives" have not seen a world without computers, smart phones, and electronic media (Young, 2011, p. 23). With the different views of this technology, there are different interpretations of the protections of the Fourth Amendment. Orin S. Kerr, a professor at George Washington University Law School and a leading authority on computer law, suggests that "Online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private thoughts and speech" (Young, 2011, p. 24). Using this explanation, non-content information would be public, thus not protected by the Fourth Amendment (Young, 2011). The content surveillance should receive the protections of the Fourth Amendment. Unfortunately, whether or not the information is in a private or public place is a difficult distinction for law enforcement to make (Young, 2011).

In *United States v. David*, 756 F. Supp. 1385 (1991), Artem David was indicted on conspiracy charges involving the trafficking of heroin (Kerr, 2009). As part of his plea agreement, David provided information stored in his computer about his narcotics dealings (Kerr, 2009). Once David had accessed the information and turned it over to the agents, he powered down his computer but left it in the possession of the agents (Kerr, 2009). The agents, who acquired David's password without his knowledge or permission, accessed the computer and gathered additional information (Kerr, 2009). A United States Magistrate judge declared that the additional information gathered by the agents after David had powered down his computer was a violation of the Fourth Amendment (Kerr, 2011). Once David withdrew his consent, his expectation of privacy was restored and any further entry into the computer would need the authorization of a signed warrant (Kerr, 2009).

Compstat

Ethical violations do not occur only at the officer or agent level. Compstat was a dynamic approach to crime reduction, personnel and resource management, and improvement in overall quality of life (Eterno, 2010). This was introduced by William Bratton of the New York Police Department in 1995 when he became the Police Commissioner of New York City (Kappeler, 2006). The program involved weekly meetings with NYPD executives and precinct commanders to discuss problems, strategies and tactics to reduce crime and solve problems (Eterno, 2010). Compstat was hailed as the reason for the significant drop of crime rates in New York City (Kappeler, 2006). Critics of this program state that unethical practices played a significant role in the data produced as a result of Compstat (Eterno, 2010). A survey, that was conducted involving players during the Compstat era, show that there were many unethical changes to the reported data (Eterno, 2010).

These changes were influenced by pressure from political supporters as well as promotions and raises (Eterno, 2010). Street officers became weary of taking reports of crimes and complaint reports were ignored or altered because of the effect that it could have on the data (Eterno, 2010). “Usually, the first line of control over the risk of errant conduct by police is to invoke guidelines to contain their use of discretionary authority” (Girodo, 1998, p. 484). When allegations of an officer’s misconduct or unethical actions are made, an investigation is conducted by the department’s Internal Affairs Division or IA (Miller, 2010). IA is tasked with reviewing established guidelines for undercover operations, discovering the facts, and rendering a recommendation to the executives of the department concerning disciplinary or criminal action against the accused. It has been obvious in the past that departments IA divisions have not been entirely ethical themselves (Miller, 2010). “The deficiencies identified have included inadequate planning of investigations, inadequate use of electronic surveillance, failure to interview key witnesses, breaches of confidentiality, and lack of timeliness” (Miller, 2010, p. 29).

Conclusion

Technology has changed in the last twenty years and will continue to advance to the degree that with each passing day, fewer people will remember a time without mobile phones, computers, and email. Ethical dilemmas have been with us since the beginning of societies and will stay indefinitely. The relationship between technology and ethics is increasing with each new smart phone or laptop. Law enforcement officers must continue to stay informed on not only the technology but how that technology affects the job descriptions. Law enforcement officers must be trained in not only the proper handling of new technologically and advanced equipment but also the ethical guidelines that direct their use. Although officers receive yearly ethics training, it is not specific and based on an overall perspective of the lawful execution of their duties. Officers that perform undercover duties must use deceptive techniques in order to catch a criminal or prevent a crime from occurring. The officer sometimes has to break the law that they have sworn to uphold in an attempt to gather evidence or to make an arrest. This is necessary for the completion of the mission. Other covert operatives pose as potential minor victims in an effort to capture online predators.

Law enforcement officers have their ethics tested throughout their career. Searching a suspect’s cellular phone or a subject’s computer without first acquiring a warrant is but one of the overzealous actions of officers, especially the “digital immigrants” (Young, 2011, p. 23). Mobile phones and computers are viewed by the Supreme Court as containers and may have some protection under the Fourth Amendment. Global positioning devices that are being used by law enforcement and warrantless searches of mobile phones are currently under review by the United States Supreme Court.

The Fourth Amendment protects citizens from unreasonable searches and seizures to include technology. One must remember that public information is not protected by the Fourth Amendment but private, personal information is protected. Since 9/11, technology has been implemented in areas such as airports with the use of full body scans. Many argue that this is a clear violation of the Fourth Amendment, but the reasoning is sound. Benjamin Franklin stated that those who give up their liberty for more security deserve neither liberty nor security (paraphrased); however, if everyone was completely free then they would be free from security as well.

When the terrorists’ attacks on the United States occurred, the American public demanded that the government take action and protect this nation. Ten years later, the same citizens are disagreeing with the scanners at the airport or the government monitoring communications from suspected terrorist organizations and locations. Americans do not live in a utopia where days are spent frolicking through a meadow or lying on a beach without a care in the world. This is a harsh world and the role of the law enforcement officer is to maintain the peace and tranquility that is expected by all.

Ethics, legislation, and court decisions guide the actions of law enforcement officers in their deontological performance of their daily tasks. With technology increasing at an exponential rate, the legislative and judicial branches of the government cannot keep the pace. Officers are left with their own utilitarian ethical beliefs and the training they receive in ethical decision making. Street officers more than often have to rely on the expertise of their superior officers, who may be “digital immigrants” (Young, 2011, p. 23). Granted, not every instance of the use of technology by law enforcement is ethically justified; but, depending on the consequences, society wants the best result, even if it does mean bending the rules on occasion.

REFERENCES

- Clancy, T. K. (2010). Digital Child Pornography and the Fourth Amendment. *Judges' Journal*, 49(3), 26-32.
- Cooper, S. (2010). Mechanical Law Enforcement: Speeding and Camera Technology. *Journal of Criminal Law*, 74(5), 409-414. doi:10.1350/jcla.2010.74.5.656
- Eterno, J., & Silverman, E. (2010). The NYPD's Compstat: compare statistics or compose statistics?. *International Journal of Police Science & Management*, 12(3), 426-449. doi:10.1350/ijps.2010.12.3.195
- Girodo, M. (1998). Undercover probes of police corruption: risk factors in proactive internal affairs investigations. *Behavioral Sciences & The Law*, 16(4), 479-496.
- Hale, B. (2005). Identity crisis: Face recognition technology and freedom of the will. *Ethics, Place & Environment*, 8(2), 141-158. doi:10.1080/13668790500237047
- Joh, E. E. (2009). Breaking the law to enforce it: Undercover police participation in crime. *Stanford Law Review*, 62(1), 155-199.
- Kallman, E., & Grillo, J. (1993). Ethics is not a four letter word. In E. Berg (Ed.), *Ethical Decision Making and Information Technology* (p. 3). New York, NY: Mitchell McGraw-Hill.
- Kaur, M. (2010). Truth Be Told? The Use of Truth Serum in Indian Law Enforcement. *Kennedy School Review*, 10118-123. Retrieved from EBSCOhost.
- Kappeler, V. E. (2006). *The police and society, touchstone readings*. (Third ed.). Long Grove, IL: Waveland Pr Inc.
- Kerr, O. (2009). *Computer crime law*. (2nd ed., pp. 309-319). St. Paul, MN: West.
- Kilpatrick, P. (2010). The Relationship Between Technology and Ethics. *Vital Speeches of the Day*, 76(12), 567-570. Retrieved from EBSCOhost.
- Loghman, K. (2011, November 29). Interview by A Goodman [Web Based Recording]. Pepper-spray creator decries use of chemical agent on peaceful occupy Wall Street protesters. , Retrieved from www.democracynow.org/seo/2011/11/29/pepper_spray_creator_decries_use_of
- Lombard, É. (2010). Bombing Out: Using Full-Body Imaging To Conduct Airport Searches in the United States and Europe Amidst Privacy Concerns. *Tulane Journal of International & Comparative Law*, 19(1), 337-367. Retrieved from EBSCOhost.
- Miller, S. (2010). What Makes a Good Internal Affairs Investigation?. *Criminal Justice Ethics*, 29(1), 29-40. doi:10.1080/07311291003654153
- Missing kids. (2011). Retrieved from www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=245
- Otto M.J., A., & Jos, M. (2004). Pepper spray: An unreasonable response to suspect verbal resistance. *Policing*, 27(2), 206-219.
- Smith, K. (2011). Hiding in Plain Sight: Protection from GPS Technology Requires Congressional Action, Not a Stretch of the Fourth Amendment. *Mercer Law Review*, 62(4), 1243-1278. Retrieved from EBSCOhost.
- Warfield, J. (2010). Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones. *American Journal of Trial Advocacy*, 34(1), 165-193. Retrieved from EBSCOhost.
- Weinberger, S. (2010). Airport security: Intent to deceive?. *Nature*, 465(7297), 412-415. doi:10.1038/465412a
- Wells, M., Finkelhor, D., Wolak, J., & Mitchell, K. J. (2007). Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession. *Police Practice & Research*, 8(3), 269-282. doi:10.1080/15614260701450765
- What are Science, Technology and Engineering?. (2011). *Ohio Journal of Science*, 111(2), 66-67. Retrieved from EBSCOhost.
- Wu, S.(2010). When can I tase him, Bro?: Bryan v. McPherson and the property of police use of tasers. *Golden Gate University Law Review*, 40(3), 361-380.
- Wyatt-Nichol, H., & Franks, G. (2009). Ethics Training in Law Enforcement Agencies. *Public Integrity*, 12(1), 39-50.
- Young, M. D. (2011). Electronic surveillance in an era of modern technology and evolving threats to national security. *Stanford Law & Policy Review*, 22(1), 11-39. Retrieved from EBSCOhost.
- Zirkel, P. (2006). Technological Tools -- or Weapons?. *Phi Delta Kappan*, 88(3), 255-256. Retrieved from EBSCOhost.