2016

Drones and Machine Learning Analytics – The Best Way to Provide Privacy Safeguards on Drone Surveillance is with Technology, not Law

Victoria Dorum

Drones and Machine Learning Analytics – The Best Way to Provide Privacy Safeguards on Drone Surveillance is with Technology, Not Law.

By Victoria Dorum

I. INTRODUCTION

"Mr. Marks, by mandate of the District of Columbia Precrime Division, I'm placing you under arrest for the future murder of Sarah Marks and Donald Dubin that was to take place today, April 22 at 0800 hours and four minutes."[1]

Imagine a world were crime could be predicted. Where you knew ahead of time who the perpetrator will be. That world may not be as far away as a figment of Hollywood's imagination. Predictive policing is no longer a scientific concept society contemplated only possible in movies, it is as real as wireless communication and thermal imaging technology – all common things we now take for granted that used to be a thing futuristic imagination that society was not even sure is possible. Other technologies that people do not think of as groundbreaking anymore are NSA surveillance and targeting advertising practices. These kinds of collections of information, data mining and machine learning techniques are now old news and though they are still subject of widespread controversy, we accept them as part of the world we live in. Soon, we may think the same way about another type of technological advance that stems from the latter two things - predictive policing using drone surveillance.

Drones have many beneficial uses, including search-and-rescue missions, scientific research, mapping, disaster relief and more.[2] But deployed without proper regulation, drones

[1] Minority Report (Amblin Entertainment 2002)

[2] Atmel Staff, *18 awesome ways drones are being used today*, August 8, 2014, available at http://blog.atmel.com/2014/08/08/18-awesome-ways-drones-are-used-today/.

equipped with facial recognition software, infrared technology, and speakers capable of monitoring personal conversations, would cause unprecedented invasions of individuals' privacy rights. Interconnected drones could enable mass tracking of vehicles and people in widespread areas. Tiny drones could go completely unnoticed while peering into the window of a home or place of worship. Thus, when it comes to drone surveillance, drones have been getting a lot of backlash from civil liberty groups like ACLU, criticism from scholars, lawyers and other members of society and perhaps fear from some of the legislators. While not without great constitutional concerns, the benefits of the use of drones for surveillance purposes greatly outweigh the risks when the risks are addressed and balanced out by a proper legislative framework that takes into account considerations of the precedent so far and the capabilities of current technology. Considering that some savvy criminals already posses sufficient control and command of this emerging technology to aid their criminal activities, failing to arm law enforcement officials with the same technological advancements as is available to civilians, in hopes of not just apprehending the criminals but also preventing crime and saving lives, because of lack of sufficient knowledge or misunderstanding of the current technological landscape would be equivalent to tying law enforcement's hands while providing ammunition to their antipode.

Part II of this paper briefly discusses current legislative background of drone surveillance with examples of legislations that have already been passed on law enforcement's use of drones for surveillance purposes. Existing drone legislation is examined to determine what has been done by the states so far, the differences between legislations are examined to give a background for the discussion of what could or should be done differently in crafting future legal framework for drone legislation. Current legal background of other technologies that are used for surveillance purposes is discussed in Part III to introduce the bounds that are already established by past legislation and case law. It discusses cases and some legislation related to different types of surveillance such as aerial and aural surveillance to determine where drones fit in our existing legal framework and what are the boundaries that are already created for drone surveillance. Part IV examines current machine learning analytics technology and how it is currently used with considerations of existing legal framework in mind, this part sets out recommendation for a legislative framework for drone surveillance in law enforcement taking into account current and emerging technologies. This part provides recommendations for the most efficient and effective use of current and future technologies that would balance concerns expressed by the courts in cases that are examined in Part III of the paper and current criticisms by civil liberty organizations. It also focuses on emerging technologies that are expected to emerge in the next ten years to account for the changing landscape and evolution of technological advancement and provide an up to date legislation. Part V is titled Concerns, this part will analyze what concerns will be difficult to address with the proposed legislative framework and the policy issues that the courts and legislators will likely still face in light of this unexplored area of law.

II. LEGISLATIVE BACKGROUND

Since the beginning of 2013 legislative sessions, state lawmakers have considered many pieces of legislation addressing the use of drones. In 2015, 45 states have considered 168 bills related to drones and at least 41 states have considered drone legislations in 2016.[3] Twenty states–Arkansas, California, Florida, Hawaii, Illinois, Louisiana, Maine, Maryland, Michigan, Mississippi, Nevada, New Hampshire, North Carolina, North Dakota, Oregon, Tennessee, Texas,

[3] *Current Unmanned Aircraft State Law Landscape*, NATIONAL CONFERENCE OF STATE LEGISLATORS, available at http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

Utah, Virginia and West Virginia–have passed 26 pieces of legislation.[4] Four other states–Alaska, Georgia, New Mexico and Rhode Island–adopted resolutions related to drones.[5] Georgia's resolution established a House study committee on the use of drones and New Mexico adopted memorials in the house and senate requiring a study on protecting wildlife from drones.[6] Rhode Island's resolution created a legislative commission to study and review regulation of drones.[7] Additionally, Virginia's governor signed an executive order establishing a commission on unmanned systems (as drones are often referred to).[8] Florida and Kentucky have pre-filed bills for the 2016 legislative session.[9]

Currently, 17 states have legislation relating to use of drones. Of those 17 states, 14 have legislation limiting how police can use drones.[10] Members in the House and Senate introduced bills in the previous Congress that would have required police everywhere in the country to obtain a warrant before using drones for surveillance, but the bills died at the end of the year.[11] "In the states that don't require warrants, it's pretty much a Wild West" in terms of what's allowed, says Jay Stanley, senior policy analyst at the American Civil Liberties Union.[12] "There's nothing stopping a police department from using [drones] in all kinds of ways to spy, except for the Constitution."[13]

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] State Regulation, *Domesticating the Drone Evaluating Privacy Policy in the Use of Unmanned Aircraft Systems Within the US*, INSCT (September 24, 2015), http://uavs.insct.org/state-regulation/.
[8] *Id.*
[9] *Id.*
[10] Waddell Kaveh, *Few Privacy Limitations Exist on How Police Use Drones*, NATIONAL JOURNAL (February 5, 2015) available at http://www.nationaljournal.com/daily/2015/02/05/few-privacy-limitations-exist-how-police-use-drones#!.
[11] *Id.*
[12] *Id.*
[13] *Id.*

In current regulations, states, however, tend to border on extremes. In their complicating legislatives frameworks, states either ban unwarranted use of drones with very limited exceptions thus hindering law enforcement's ability to use technology in conducting surveillance that it is otherwise allowed to conduct lawfully without the use of drones or states fail to regulate drone surveillance at all resulting in the ability to conduct drone surveillance without any kind of safeguards at all. For example, Idaho's law restricting the government's use of drones appears to impose strict restrictions on government drone use, but it contains some notable loopholes.[14] Law enforcement officers are generally required to obtain a warrant before using drones to gather information.[15] However, it is unclear how this use of a drone is an effective way to conduct surveillance, since law enforcement officers would first have to engage in surveillance without a drone to obtain enough information to demonstrate probable cause so that they could obtain a warrant for use a drone to gather information. If the government fails to obtain a warrant and violates the statute, anybody whose image is wrongfully recorded by the drone can claim statutory damages in the amount of $1,000.[16] But what is more interesting is that warrants are not required when the government is responding to an emergency or is carrying out a controlled substances investigation.[17] This leaves a broad and unclear exception up to law enforcements' interpretation, if there is a halfway house or an area or neighborhood where there is a prevalent use and sale activities of controlled substances, is law enforcement then allowed to use drones in that area pervasively? Can a drone be operated to conduct continuous surveillance of an individual who is subject to a controlled substances investigation without a warrant? And lastly,

[14] IDAHO CODE ANN. § 21-213(2) (2013).

[15] *Id.*

[16] IDAHO CODE ANN. § 21-213(3) (2013). The statute's restriction on drone use and the statutory damages provision applies to both the government and to private parties.

[17] IDAHO CODE ANN. § 21-213(2) (2013)

why did Idaho legislation decide that there is a compelling need for drones to be allowed to be used sans warrant in controlled substance investigations, but not in investigations of violent crimes or any other types of crimes?

Florida's law prohibits the use of drones by law enforcement without a warrant from a judge unless several narrow exceptions apply.[18] Officers can use drones without a warrant when there is a significant risk of a terrorist attack, or when law enforcement officers are reasonably certain that the use of a drone is necessary to prevent imminent physical harm or the imminent escape of a suspect.[19] These restrictions prevent law enforcement from using the help of a drone to conduct public surveillance in a lawful manner that they are otherwise allowed to conduct. The law further provides that any evidence obtained in violation of the law will be inadmissible in a criminal prosecution.[20]

Illinois's law regulating government drone use is similar to Florida's law as outlined above.[21] However, Illinois has several other exceptions to the warrant requirement, including provisions permitting law enforcement agencies to use drones without a warrant to locate missing persons, or to survey a crime scene or the scene of a traffic collision.[22]

Indiana generally requires law enforcement officers to obtain a search warrant before using drones.[23] However, officers do not need to obtain a warrant when: exigent circumstances exist; there is a "substantial likelihood of a terrorist attack;" in disaster-response situations; in rescue operations; in circumstances where the person observed has given consent; and in other surveillance activities that are not related to criminal investigation.[24]

[18] FLA. STAT. § 934.50(3)–(4) (2013).
[19] *Id.*
[20] FLA. STAT. § 934.50(6) (2013)
[21] 725 ILL. COMP. STAT. 167/10, 167/15(1)–(3) (2015).
[22] 725 ILL. COMP. STAT. 167/15(4)–(5) (2015)
[23] IND. CODE § 35-33-5-9(a) (2014)
[24] IND. CODE §§ 35-33-5-9(b)(1)(A)–(E), 35-33-5-9(b)(2) (2014).

Oregon restricts law enforcement agencies' use of information gathered by drones and provides that information obtained in violation of its laws will not be admissible in judicial proceedings.[25] This information can be used at trial, however, when: a judge has issued a warrant; there is probable cause to believe that a crime has been committed and exigent circumstances exist; the person or people observed have consented; the information has been collected during a response to an emergency; or the government has used the drones to observe and reconstruct a crime scene.[26]

Tennessee's law explicitly states that the government's use of a drone to collect information is a search within the meaning of the Fourth Amendment as well as the Tennessee Constitution, and that evidence collected in violation of the statute is inadmissible in court.[27] Like many of the statutory schemes described in this subsection, Tennessee's law goes on to state a number of exceptions to its warrant requirement, including: terrorist attack scenarios; situations where there is a risk of imminent harm to somebody's life; and missing person searches.[28]

Texas law prohibits the collection of images of a person or a person's property with a drone if those images are collected with "the intent to conduct surveillance" on that individual or property.[29] If images are collected in violation of the law, they may not be used as evidence at trial.[30] Texas's law provides for many exceptions to this warrant requirement, including situations when: the person observed consents; officers are pursuing a suspect; officers are

[25] OR. REV. STAT. § 837.310 (2013)

[26] OR. REV. STAT. § 837.320(1)(a) (2013); OR. REV. STAT. § 837.320(1)(b) (2013); OR. REV. STAT. § 837.330 (2013); OR. REV. STAT. § 837.335 (2013); OR. REV. STAT. § 837.340 (2013).

[27] TENN. CODE ANN. § 39-13-609(g) (2013)

[28] TENN. CODE ANN. § 39-13-609(d)(1), (3)–(5) (2013)

[29] TEXAS GOV. CODE ANN. § 423.003 (2013). The term "surveillance" is not defined.

[30] TEXAS GOV. CODE ANN. § 423.005 (2013)

searching for a missing person; and officers are documenting a crime scene, or engaging in a "high-risk tactical operation that poses a threat to human life."[31]

One of the jurisdictions that has been in a dire need of the benefits provided by drone technology but unable to implement it due to the legislators' difficulties in finding the proper balance for the legislative framework is California. While law enforcement in California has been using drones since 2006, California has been unable to pass legislation that will allow law enforcement to effectively utilize drones and protect civilian's personal liberty interests.[32]

Lawmakers came close on September 8, 2014, when the California Assembly presented AB 1327 to the governor for approval.[33] The bill allowed law enforcement to use drones without a warrant in emergency situations involving an imminent threat to life or great bodily harm. [34] The proposed legislation also required public agencies to give the public reasonable notice before deploying unmanned aircraft systems. [35] The bill would also have required that images, footage, or data gathered from drones be destroyed within one year.[36] Governor Brown, however, vetoed the bill because it was too narrowly drawn and would "impose requirements beyond what is required by either the Fourth Amendment or the privacy provisions in the California Constitution. "[37] While the bill accounted for agency oversight and regulation, similar to existing legislations, it did not adequately address the real life implications of law enforcement

[31] TEXAS GOV. CODE ANN. § 423.002(a)(6)–(9) (2013).

[32] Xeni Jardin, *Launching 'Big Brother' Flying Drones Over L.A.*, NPR (Apr. 6, 2006, 1:00 PM). More recently, the Seattle Police Department gave the Los Angeles Police Department (LAPD) two Draganflyer X drones. News Release, Los Angeles Police Department, Office of Inspection General to House Two Unmanned Aerial Vehicles While Policy is Reviewed (Sept. 15, 2014) http://www.lapdonline.org/newsroon/news-view/56930. *See* David Kravets, *California Cops Don't Need Warrants to Surveil with Drones*, ARS TECHNICA (Sept. 29, 2014, 9:25 AM), http://arstechnica.com/techpolicy/2014/09/california-cops-dont-need-warrants-to-surveil-with-drones/.

[33] Unmanned Aircraft Systems, A.B. 1327, 2013-14 Leg., Reg. Sess. (Cal. 2013-2014).

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

operations. [38] The Governor's comments concerning his veto were brief, but his veto may suggest that drone laws should allow for reasonable suspicion as a justification for the use of drones. [39] California's attempt to restrict drone usage shows the importance of privacy rights for citizens, but perhaps the Governor's view is the more realistic one. After all, "[s]uch a restriction [for law enforcement] may mean that the police will never be able to develop the probable cause necessary to get a warrant . . ."[40] However, as discussed in Part IV of this paper, one way to account for existing technology and address implications for law enforcement operations while still placing necessary safeguards against privacy concerns is to pair drone technology with machine-learning algorithms to meet the probable cause requirement currently favored by the legislators.[41]

III. CURRENT SURVEILLANCE STATE

The first step to creating an effective drone surveillance legislative framework is to analyze what case law currently limits the use of drone technology and what the law currently permits in relation to drone surveillance based on previous technologies. Although there have been major developments in technology over the last few years, umanned aircraft systems or as they are commonly called "drones" are not a completely novel phenomenon. Aerial surveillance methods have been employed by law enforcement for decades and have led to some very significant precedent.

[38] *See* Zusha Elinson, *Brown Vetoes Bill Requiring Warrants for Drone Surveillance*, WALL ST. J., http://www.wsj.com/articles/california-governor-vetoesbill-requiring-warrants-for-drone-surveillance- 1412007285 (last updated, Sept. 29, 2014, 6:15 PM).

[39] Unmanned Aircraft Systems, A.B. 1327, 2013-14 Leg., Reg. Sess. (Cal. 2013-2014).

[40] Gregory S. McNeal, *Poorly Drafted Drone Laws May Shield Crimes From View*, FORBES (July 8, 2014, 6:55 AM), http://www.forbes.com/sites/ gregorymcneal/2014/07/08/anti-drone-legislation-protects-animal-abuses-and-othercrimes/.

[41] *See* Part V *infra*, discussion on page 39-40.

Aerial observations of the curtilage of a home are generally not prohibited   by the Fourth Amendment, so long as the government is conducting the surveillance from public navigable airspace, in a non-physically intrusive manner, and the government conduct does not reveal intimate activities traditionally associated with the use of the home. The U.S. Supreme Court addressed the issue of aerial surveillance in a series of cases in the late 1980s:

In *California v. Ciraolo* the Supreme Court held, "The Fourth Amendment was not violated by the naked-eye aerial observation of respondent's backyard."[42] In *Ciraolo*, the police received a tip that someone was growing marijuana in the backyard at Ciraolo's home.[43] A police officer attempted to observe what was growing, but a six-foot high outer fence and a ten-foot high inner fence obscured his observations.[44] The officer, suspicious that the fences might be intended to hide the growth of marijuana, obtained a private plane and flew over the backyard of Ciraolo's property at an altitude of 1,000 feet.[45] That altitude was within the FAA's definition of public navigable airspace.[46] The Supreme Court found that this was not a search, and therefore was not prohibited by the Fourth Amendment.[47] In so finding, Chief Justice Burger stated that in erecting a 10-foot fence, Ciraolo manifested "his own subjective intent and desire to maintain privacy as to his unlawful agriculture" but his "intent and desire" did not amount to an expectation of privacy.[48] The Court stated, "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000

[42] California v. Ciraolo, 476 U.S. 207 (1986)
[43] *Id.* at 210.
[44] *Id.*
[45] *Id.*
[46] *Id.* at 213.
[47] *Id.* at 214.
[48] *Id.* at 211.

feet."[49] The Court noted that the fence "might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus."[50] Accordingly, "it was not 'entirely clear' whether [Ciraolo] maintained a 'subjective expectation of privacy from *all* observations of his backyard,' or only from ground level observations."[51] The Court believed that it was unreasonable for Ciraolo to expect privacy in his backyard when a routine over flight, or an observation "by a power company repair mechanic on a pole overlooking the yard" would reveal exactly what the police discovered in their observation during the flight.[52]

At the same time that *Ciraolo* was decided, the Court in *Dow Chemical Co. v. United States* articulated a similar theme, holding that the use of an aerial mapping camera to photograph an industrial manufacturing complex from navigable airspace similarly does not require a warrant under the Fourth Amendment.[53] In *Dow Chemical Co.*, the Supreme Court did acknowledge that the use of technology might change the Court's inquiry, stating, "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[54] But then the Court dismissed the notion, stating "[a]ny person with an airplane and an aerial camera could readily duplicate" the photographs at issue.[55] In short, the Court stated, "of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[56]

[49] *Id.*
[50] *Id.*
[51] *Id.* at 212.
[52] *Id.* at 214-215.
[53] Dow Chemical v. United States, 476 U.S. 227 (1986).
[54] *Id.* at 238.
[55] *Id.* at 231.
[56] *Id.* at 239.

Shortly after *Ciraolo* and *Dow Chemical Co.*, the Supreme Court analyzed the use of helicopters for aerial surveillance. In *Florida v. Riley*, the Supreme Court held that "the Fourth Amendment does not require the police traveling in the public airways at an altitude of 400 feet to obtain a warrant in order to observe what is visible to the naked eye."[57] The *Riley* court found that the rule of *Ciraolo* controlled.[58] Riley, just like Ciraolo, took measures that "protected against ground level observation" but "the sides and roof of his greenhouse were left partially open" just as the sky above Ciraolo's yard, allowed one to look directly down into his yard.[59] In *Riley*, the police flew a helicopter over Riley's land, and observed marijuana plants growing in Riley's greenhouse.[60]

The Court in *Riley* found that "what was growing in the greenhouse was subject to viewing from the air."[61] The police conduct in *Riley* was acceptable because the police were flying in publicly navigable airspace, "no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury."[62] The Court continued, "[a]ny member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more."[63] In an important passage, concurring in the judgment, Justice O'Connor noted "public use of altitudes lower than [400 feet]—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police

[57] Florida v. Riley, 488 U.S. 445 (1989)
[58] *Id.* at 449.
[59] *Id.* at 450.
[60] *Id.* at 448.
[61] *Id.* at 450.
[62] *Id.* at 452.
[63] *Id.* at 451.

surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA air safety regulations."[64]

Thus, the law for at least the last 25 years has allowed the police to fly aircraft over private property, backyards, factory farms, industrial plants, and any other place where the average citizen may be able to see the property by the same means. The police may make observations from the air, just like a person on a commercial flight inbound to an airport can look down and observe the yards of people below and just like a utility worker on a pole can look down into an adjacent yard. Armed with that information, the police can use it to get a warrant to go in on foot and investigate what they previously observed from a lawful vantage point without a warrant.

For more than two decades, the police have not been required to turn a blind eye to evidence of criminality merely because they observed it from the air, they similarly should not be required to ignore evidence of criminality merely because they witness the crime through the eyes of a drone. One important limitation on the use of the drone, however, should be a restriction to only allow the drone to be used in the public space, pursuant to the public view doctrine. Legislation should mandate for drones to be equipped with geofencing, which would block out people's windows out of the view of the drone curtailing individual's privacy concerns. Geofencing is a type of virtual barrier created by "a software program that uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries.[65]

Another important body of law that was developed around use of technology for law enforcement surveillance is in the area of aural surveillance. Some of the current drone

[64] *Id.* at 455.
[65] WhatIs.com, available at http://whatis.techtarget.com/definition/geofencing.

technology is extremely small in size and can be equipped with high quality audio and video capabilities.[66] The ability to capture audio during drone surveillance can be equivalent to traditional wiretapping that has been used by law enforcement in the past and presently, especially if the subject of surveillance is unaware that he is being observed by a drone.

One of the most notable Fourth Amendment cases involving wiretap is *Katz v. United States*.[67] *Katz* involved the wiretapping of a telephone conversation made by the defendant while in a phone booth.[68] The Court stated: "What a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[69] From *Katz*, the Court's current approach to determining the Fourth Amendment's applicability emerged – the reasonable expectation of privacy test.[70] The test, articulated in Justice Harlan's concurrence, asks whether (1) a person exhibits an "actual or subjective expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable'."[71]

One year after *Katz*, in 1968, Congress vastly expanded its statutory protections against electronic surveillance. Title III of the Omnibus Crime Control and Safe Streets Act extended the reach of wiretap regulations to state officials as well as to private parties.[72] Despite its profound increase in the extent of protections, Title III had important limitations. It applied to the

[66] In a study described by a freelance writer, Nsikan Akpan, it was revealed that drones already have technological capabilities such as "handling more than 7 g's on a sharp turn to soaring at speeds up to 56.2 kilometers per hour" and further this technology is being developed to imitate birds so that drones are light enough and autonomously precise to be able to "[land] on a wire without stalling or navigating a tree-filled forest without crashing." Editor's Note, *Contemplating the coming of drones*, Science News, SOCIETY FOR SCIENCE AND THE PUBLIC, Feb. 7, 2015.
[67] Katz v. United States, 389 U.S. 347 (1967)
[68] *Id.* at 349.
[69] *Id.* at 351.
[70] *Id.* at 360.
[71] Katz, 389 U.S. at 361 (Harlan, J., concurring)
[72] 18 U.S.C. §§ 2510-2522

interception of aural communications; it did not apply to visual surveillance or other forms of electronic communication.[73]

Cases involving communications made between parties in person, as opposed to electronic mail, messaging or telephone fall under the ambit of "eavesdropping" cases. The admissibility of evidence secured by mechanical or electronic eavesdropping is dependent upon the fundamental principle that any evidence that is secured through the violation of certain constitutional rights, such as that pertaining to unreasonable search and seizure, is inadmissible as having been illegally obtained.[74] While many of the cases antedating the formulation of this principle took a contrary view, the courts are now fairly uniform in holding that evidence need not be excluded merely because it was secured by means of mechanical or electronic eavesdropping so long as the circumstances attending the use or installation of the eavesdropping device did not involve such unlawfulness as contravened the rule against illegal obtention.[75]

Many states have their own eavesdropping laws and restrictions on law enforcement and private eavesdropping. For example, California makes it a crime to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation.[76] The statute applies to "confidential communications" -- i.e., conversations in which one of the parties has an objectively reasonable expectation that no

[73] *See* § 2510(1)

[74] *See* Am Jur, Evidence (1st ed §§ 393 et seq.) and Mapp v Ohio (1961) 367 US 643.

[75] While the foregoing statement finds almost unanimous support in the majority opinions of the courts, the vigorous dissents in the United States Supreme Court decisions on the general question of electronic surveillance are indicative that the rule of admissibility is by no means "well settled." Beginning with Justice Holmes's dictum in Olmstead v United States (1928) 277 US 438, 72 L ed 944, 48 S Ct 564, 66 ALR 376, characterizing the entire practice as "dirty business," and culminating in Lopez v United States (1963) 373 US 427, 10 L ed 2d 462, 83 S Ct 1381, reh den 375 US 870, 11 L ed 2d 99, 84 S Ct 26, where four members of the court agreed that the rule of admissibility should not be "revitalized," arguments that the practice reeks of police state tactics and should be completely abolished have been in conspicuous evidence. A general discussion of the policy factors involved in the arguments for and against admitting evidence obtained by electronic surveillance would range far beyond the scope of this treatment but it should be noted that the very foundation of the rule of admissibility is still a matter of considerable argumentation. See the extended discussion of the general question in 44 Minn L Rev 813.

[76] *See* Cal. Penal Code § 632.

one is listening in or overhearing the conversation.[77] A California appellate court has ruled that this statute applies to the use of hidden video cameras to record conversations as well.[78] Thus, although helpful in police investigations, drones should be equipped with aural surveillance capabilities only if state legislations already allow such use of technology.

IV. APPLYING MACHINE LEARNING ANALYTICS TO DRONE TECHNOLOGY

Some states have adopted legislations enabling law enforcement to use drones pursuant to certain limitations, many states cannot keep up with the rise of drone use by both law enforcement and recreational users, which has thus far been very loosely regulated.[79] Although tracking drone sales has proven to be a difficult task, it is estimated that about 500,000 drones have been sold in 2014.[80] Some of recreational drones are already in use and they have already been used to assist bad faith users in a number of criminal activities. For example,

> [i]n Latin America, the Revolutionary Armed Forces of Colombia (FARC) has been collaborating with narcocartels to create remote-controlled drug-smuggling submarines capable of transporting 1,800 kilos of cocaine more than 1,000 miles (1,600 km) without refueling. In 2011, an al-Qaeda affiliate named Rezwan Ferdaus planned to launch an attack on the Pentagon and Capitol buildings using a remote-controlled drone aircraft laden with explosives until the FBI intercepted the plot. And just last year, criminals piloted a $600 remote-controlled quadcopter over a Brazilian prison fence to deliver cell phones to the incarcerated, as was also done in a 2009 attempt involving a drone to deliver drugs to prisoners in the U.K. A 50-ft. (15 m) electric fence may keep criminals in, but won't keep a UAV drone out.
>
> Flying robots open up new opportunities for crime. Camera-equipped drones can and will be used for everything from the theft of industrial secrets to voyeurism by creepy neighborhood Peeping Toms. Some parents might use drones to follow their kids to school to ensure their safe arrival, but others will

[77] *See* Flanagan v. Flanagan, 41 P.3d 575, 576-77, 578-82 (Cal. 2002).

[78] *See* California v. Gibbons, 215 Cal. App. 3d 1204 (Cal Ct. App. 1989).

[79] *Drone regulations should be considered for use now and in the future*, The Times Editorial Board, LOS ANGELES TIMES, available at http://www.latimes.com/opinion/editorials/la-ed-adv-drone-regulation-20151213-story.html.

[80] Jason Reagan, *Drone Sales Figures for 2014 are Hard to Navigate*, DRONE LIFE, Jan. 24, 2015, available at http://dronelife.com/2015/01/24/drone-sales-figures-2014-hard-navigate/.

> exploit the technology to stalk ex-husbands and ex-wives. Worse yet, hobbyists have been attaching guns to quadcopters for at least five years. [81]

And yet current legislation for use of drones is either very cautious of giving the right to use drones to police in any meaningful way or fails to regulate law enforcement's use of drones altogether leaving concerns for civil liberties completely unaddressed. To ban the use of drones by police enforcement is equivalent to giving criminals the advantage of sophisticated technology while denying it to law enforcement that is tasked with catching those criminals. This type of approach will not only be unfair but also impractical. On the other hand, allowing drone surveillance to go unregulated poses serious threats to individuals' privacy and may result in unconstitutional surveillance practices. To ensure most effective and practical use of drones for surveillance purposes within the ambits of law, it is essential to define and identify what that specifically entails. Thus, the need for a comprehensive legislature for allowing the use of drones by police enforcement with important safeguards on the civil liberties, that this technology is criticized for encroaching, is instrumental. They key in allowing and implementing drone surveillance in a practical and most efficient way and addressing citizens' privacy concerns raised by this technology is to make sure that drones are used not in a broad general way, but rather in a controlled environment. Using drone surveillance in conjunction with machine learning analytics may be the only effective way to identify that environment while balancing police and citizens' concerns.

Drone surveillance can bring insurmountable benefits to law enforcement. The most important advantage to implementing drone use in police surveillance is the technology's potential to increase both officer and civilians' safety and its ability to save lives. Policing is a

[81] Mark Goodman, *Criminals and Terrorists Can Fly Drones Too*, TIME, Jan. 31, 2013, available at http://ideas.time.com/2013/01/31/criminals-and-terrorists-can-fly-drones-too/.

dangerous job. There are over 100 officer fatalities every year and about 14,000 to 16,000 officers are injured annually due to assaults.[82] In neighborhoods where violent crime is most prevalent and officers feel unsafe, fear is getting in the way of policing.[83] For example, in 2014 following an assassination of two patrol officers, NYPD police was unwilling to make arrests or write summonses for minor crimes due to fear for their safety.[84] "'I'm not writing any summonses. Do you think I'm going to stand there so someone can shoot me or hit me in the head with an ax?'" a police officer told The Post.[85] "'I'm concerned about my safety,' the cop added. 'I want to go to home to my wife and kids.'"[86] The violent environment that police officers are subjected to in the line of duty feeds into the "us versus them" mentality, akin to a warzone, that is employed by some of the officers.[87] Police officers' unwillingness to patrol the streets also causes fear and distress among the residents of crime-ridden neighborhoods.[88] In a public housing development of Brooklyn, New York where police patrol decreased following the assassination of NYPD officers, some of the residents expressed increased fear for their safety.[89]

[82] National Law Enforcement Officers Memorial Fund, available at http://www.nleomf.org/facts/officer-fatalities-data/daifacts.html.

[83] *See* Larry Celona, Dana Sauchelli, Shawn Cohen, Bruce Golding, *Wary NYPD Cops letting minor crimes slide*, NEW YORK POST, December 29, 2014 available at http://nypost.com/2014/12/29/wary-cops-letting-minor-offenses-slide/. In response to murder of two police officers in December of 2014, many officers were turning a blind eye to crime for fear of violence.

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] In his book Rise of the Warrior Cop, author and Huffington Post columnist Radley Balko critiques modern domestic police era as becoming militaristic. "My argument is that this battlefield mindset is the product of a generation of politicians telling police that they're at war with things — drugs, terrorism, crime, etc. — and have then equipped them with the uniforms, tactics, weapons, and other accoutrements of war." Balko then goes on to talk about a comment by a SWAT police officer left in response to Balsko's book embracing the combat mentality of law enforcement, comparing police work to war and encouraging other cops to do the same. Radley Balko, *SWAT Cop Says American Neighborhoods Are 'Battlefields,' Claims Cops Face Same Dangers As Soldiers In Afghanistan*, THE AGITATOR, August 21, 2013 available at http://www.huffingtonpost.com/2013/08/18/swat-cop-says-american-ne_n_3776501.html#comments.

[88] *See* Emily Fritter, Luciana Lopez, *In poor New York neighborhoods, residents ask: Where are the police?* Reuters, Jan. 9, 2015, available at http://www.reuters.com/article/us-usa-police-minorities-insight-idUSKBN0KI27320150109.

[89] *Id.*

One of the residents stated that "[i]n the past, if she needed to send her teenage daughter to the corner store, she would wait until she saw a cop on the street. Now, she doesn't feel safe sending her daughter out alone any more."[90]

On the west coast, in one of the most violent neighborhoods dubbed as "the death valley," police presence does little to prevent crime.[91] On Vermont Avenue of L.A.'s Westmount neighborhood violence is an everyday occurrence.[92] "In a county of 10 million people, Westmont is among the deadliest places to live. In the last seven years, 100 people — nearly all of them male — have been killed in the 1.8 square miles wedged between the city of Los Angeles and Inglewood.[93] Times analysis of homicide data collected in that time found Westmont's rate of killings to be the highest overall."[94] The streets of Westmont are not safe for anyone: not the adults and children who live there, not the police officers who patrol the neighborhood and not the nonprofit groups that try to remove the gang painted graffiti.[95] According to the live data published by Los Angeles Times' Homicide Report, 670 people were murdered in L.A. County in the past 10 months as of March 27, 2016.[96] 466 of those were killed by gunshot.[97]

Violence is not the only reason police officers are hesitant to patrol dangerous areas. Baltimore residents saw a decline in police patrol following the controversial police brutality case of Freddie Grey who died while in police custody in 2015.[98] While distrust of police grows

[90] *Id.*

[91] Nicole Santa Cruz, Ken Schwencke, *South Vermont Avenue:L.A. County's 'death alley'*, LOS ANGELES TIMES, Jan. 19, 2014, available at http://homicide.latimes.com/post/westmont-homicides/.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *The Homicide Report*, LOS ANGELES TIMES, March 27, 2016, available at http://homicide.latimes.com/year/all.

[97] *The Homicide Report*, LOS ANGELES TIMES, March 27, 2016, available at http://homicide.latimes.com/cause/gunshot.

[98] Leah Barkoukis, *Baltimore Residents Who Decried Police in Their Neighborhoods Now Want Them Back*, TOWNHALL, May 28, 2015, available at http://townhall.com/tipsheet/leahbarkoukis/2015/05/28/im-afraid-baltimore-residents-now-want-police-to-do-more-after-arrests-plunge-violence-soars-n2005126; Justin Fenton, Justin George,

in the wake of publicized police brutality cases, officers claim that they are hesitant to do their job for fear of prosecution pursuant to a violent encounter at the time of an arrest.[99] After the Baltimore riots in protest of police brutality following Freddie Grey's death, violence in West Baltimore has surged.[100] Baltimore experienced 40 shootings in less than a one week period resulting in 15 homicides.[101] After the spike in violence, some residents wish for police to come back to the area.[102] Antoinette Perrine, a West Baltimore resident "has barricaded her front door since her brother was killed three weeks ago on a basketball court near her home… She already has iron bars outside her windows and added metal slabs on the inside to deflect the gunfire. 'I'm afraid to go outside,' said Perrine, 47. 'It's so bad, people are afraid to let their kids outside. People wake up with shots through their windows. Police used to sit on every corner, on the top of the block. These days? They're nowhere.'"[103]

The deployment of drones will not solve all of the social problems and tensions that exist between police and civilians, but within a carefully crafted legislative framework, they can be the key to minimizing the safety risks of everyone involved. It is necessary, however, for legislators and citizens to understand that the effective use of drones will inevitably result in some privacy encroachments, but how far those encroachments will go and how necessary and justifiable they are should be determined keeping in mind the purpose of the use of drones - the prevention of violent crime.

Violence surges as Baltimore police officers feel hesitant, THE BALTIMORE SUN, May 8th, 2015, available at http://www.baltimoresun.com/sports/bs-md-ci-police-prosecutors-morale-20150508-story.html.

[99] *Id.*

[100] *Id.*

[101] Justin Fenton, Justin George, *Violence surges as Baltimore police officers feel hesitant*, THE BALTIMORE SUN, May 8th, 2015, available at http://www.baltimoresun.com/sports/bs-md-ci-police-prosecutors-morale-20150508-story.html.

[102] Leah Barkoukis, *Baltimore Residents Who Decried Police in Their Neighborhoods Now Want Them Back*, TOWNHALL, May 28, 2015, available at http://townhall.com/tipsheet/leahbarkoukis/2015/05/28/im-afraid-baltimore-residents-now-want-police-to-do-more-after-arrests-plunge-violence-soars-n2005126.

[103] *Id.*

Furthermore, there is a big difference in crafting a legislative framework for drone surveillance in response to crime that has already been committed and doing the same with the purpose of preventing violent crime. While employing a legislative framework where drones are used solely pursuant to warrants and emergency exceptions would permit a responsive method of policing by law enforcement, it would hinder proactive, preventive method of policing since officers will be restricted to the use of drone surveillance only after the crime has occurred or if it is already ongoing. Given the responsibilities and duties that local and state police is given today, preventive policing in not only desirably by society but is expected of law enforcement, however, current framework does not allow drone surveillance to be used for preventive purposes. In the wake of local violence and the global war on terror, preventing violent crimes is becoming the forefront of policing. "Traditionally, local law enforcement has concerned itself primarily with preventing and solving crimes such as burglary, theft, and robbery — crimes that have an immediate and visible impact on the local community and affect citizen quality of life. In the face of unknown future terrorist threats, however, local law enforcement organizations will have to adapt existing policing strategies to fulfill the requirement of homeland security."[104]

Public events that draw large congregations of people are especially vulnerable to terrorist threats and other widespread violence. Populated events such as Christmas tree lighting ceremonies, marathons, parades and conventions have previously been targeted with threats of violence, some of which have and some of which regrettably haven not been prevented.[105]

[104] Docobo, Jose. *Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level*, Homeland Security Affairs 1, Article 4 (June 2005). https://www.hsaj.org/articles/183.

[105] In November 2010, a 19-year old Somali-American was arrested for attempting to denote a bomb in Portland, Oregon during a Christmas tree lighting ceremony. U.S. District Court for the District of Oregon, "Arrest Warrant: United States of America v. Mohamed Osman Mohamud," November 26, 2010, available at http://www.justice.gov/usao/or/Indictments/11262010_Complaint.pdf. "When a pressure cooker bomb exploded in April 2013 during the Boston marathon, three people were killed and hundreds were injured. Had a drone been employed to watch over the race, it is possible the attack could have been prevented, said one unmanned aerial vehicle expert." Yasmin Tadjdeh, *Drones Could Mitigate Terrorist Attacks*, June 2015, available at

Therefore drone use in those instances should be allowed with minimal restrictions. Law enforcement should be able to use drone surveillance of the immediate and surrounding areas at the time and in the hours before any public event.

Use of drones in crowded places will give law enforcement an advantage over on-foot patrolling as it would give officers greater visibility and will allow them to move over crowds with ease, but simply using a drone camera to spot suspicious activity may not be the most efficient and effective method of preventing crime. Drone footage may be extremely helpful in identifying suspects after a crime was committed, but spotting suspicious activity among a large group of people is still a difficult task to complete if officers are simply using it in the same manner as a surveillance camera. When drafting drone legislation it is necessary to anticipate the technology that is probable and highly efficient for law enforcement to use in conjunction with drones. In this case, drones equipped with high-resolution cameras should be allowed to be used with analytics and biometrics software that identifies objects and people. Instead of officers looking through the footage captured by a drone, it is considerably more efficient for a drone camera to run its footage through analytical software. Modern biometrics systems and neural networks are highly accurate. At a GPU Technology Conference in 2015 when presenting research about machine learning technologies, one biometrics technology was found to have only a 0.15% error in a sample of 6,000 images. [106] This is a highly accurate outcome in a technology

http://www.nationaldefensemagazine.org/archive/2015/June/Pages/DronesCouldMitigateTerroristAttacks.aspx. Two were shot dead and four wounded in a shooting right after a Mississippi Mardi Gras Parade in February 2016. Nicole Hensley, *Two killed and four wounded as gunfire erupts after Mississippi Mardi Gras parade*, NEW YORK DAILY NEWS, February 9, 2016, available at http://www.nydailynews.com/news/national/killed-gunfire-erupts-mardi-gras-parade-article-1.2525050. In August 2004, two individuals were arrested for plotting to bomb a subway station near Madison Square Garden in New York City before the Republican National Convention. News release, *Shahawar Matin Siraj Convicted of Conspiring to Place Explosives at the 34th Street Subway Station*, U.S. Attorney's Office Eastern District of New York, May 24, 2006, available at http://www.usdoj.gov/usao/nye/pr/2006/2006may24.html.

[106] GPU Technology Conference 2015 day 3: What's next in Deep Learning, YouTube Video, Nov. 20, 2015 available at https://www.youtube.com/watch?v=qP9TOX8T-kI.

that is still evolving everyday. Using this analytics technology and the help of drones, potential known suspects or wanted criminals can be identified in the masses of people at which point, if identified, a drone could stay with that person and follow him until the suspect is apprehended by officers.

Also dangerous objects such as guns could be identified using neural network technology and nearby officers could get alerted with an image and location of the suspect until the suspect is apprehended or until the drone is given a signal that the suspect is not of interest so that the drone can move on in its surveillance.[107] Other objects that could be identified and alerted are bags and backpacks. Besides getting the location of unattended bags or people with bags or backpacks of a certain size, analytics could be run on these bags right away and police officers may get information such as the approximate weight of the bag, approximate sex and age of the person carrying the bag and possibly even the identity of the person carrying the bag if that person is already in the police network because of a previous arrest or as a possible suspect. Similarly, as is the trend in most current legislations, deployment of drones should be authorized without prior judicial approval in emergency situations such as an active shooter or similar situation that would qualify for an emergency exception. Moreover, information obtained during drone use at either public events or emergency situations should be admissible in a prosecution within a state as would be any information obtained by a police officer in the normal patrol operation of such public spaces.

On a broader scale, drone surveillance of public spaces should be allowed subject to specific safeguards that can be achieved with technological capabilities. One big misconception that critics of drones have about them is that drones are innately invasive machines that if

[107] *Id.*

employed for surveillance purposes will be flying around, peeping in people's windows and balconies gathering anything and everything about individuals' private lives that will eventually force people into a state of constant surveillance of every move they make that can rival a totalitarian regime.[108] Interestingly, this creates an image of an evil, autonomous machine, but as drone supporters pointed out at a Drone and Aerial Robotics Conference at New York University, the "drones are merely a technological platform, with a range of possibilities. They don't spy, or kill; the people ordering them around do." [109] In response to privacy concerns, a speaker at the conference replied: "[t]he public lost privacy via 'cellphones, they lost it on GPS, they lost it on the Internet. They can't get that genie back in the bottle.'"[110] Although this harsh statement is partially true, it is important to note that while some privacy is voluntary given up through the use of cellphones, GPS and the Internet, although the use of these technologies for surveillance purposes is limited. Similarly, in the case of peeping Tom technologies, drones are not the only or the first technology that can be used by law enforcement in a similar manner. Long before conversations of drone use have begun, law enforcement implemented privacy eroding tech such as infrared cameras, gps tracking devices, CCTV cameras and manned aerial surveillance. Drones are not significantly different from surveillance methods that came before them, thus determining how they could or should be used is not breaking completely new ground, but rather could be done successfully taking existing legal landscape into account.

Some legislation currently permits the use of drones only with a warrant, while others have less restrictive approaches.[111] At least one police department was considering the use of

[108] Dave Umhoefer, *Bird-sized drones could record you inside your home, Chris Taylor says*, POLITIFACT, April 9, 2014, available at http://www.politifact.com/wisconsin/statements/2014/apr/09/chris-taylor/bird-sized-drones-could-record-you-inside-your-hom/.
[109] Cora Currier, *Drone Makers Gather to Defend Their Much-Maligned Machines*, PROPUBLICA.
[110] *Id.*
[111] *Compare* IND. CODE § 35-33-5-9(a) (2014) (allowing use of drones only with a warrant unless exigent circumstances exist) *with* WIS. STAT. § 175.55(2) (2014) (only requiring a warrant for government drone use

drones in areas with high probabilities of crimes called "hot spots" to monitor a certain geographical area.[112] While many different approaches may be implemented and no one approach can be completely "perfect," to develop the best approach in drone surveillance it is necessary to look at current legal framework of technologies leading up to the emergence of drones, current technological capabilities of emerging technology that is available right now as well as will be available in the next decade, costs to the police departments in implementing the use of these technologies and civil liberty and privacy concerns that arise out of the use of drones for surveillance purposes. One of such technologies is the predictive policing software already in use by some law enforcement agencies.

Predictive policing is a scary term. When people think of predictive policing they tend to think about something akin to the popular science fiction movie "Minority Report" where a pre-crime unit of a police department arrests "would-be murderers" for the crimes they are predicted to commit but have not yet committed.[113] In the movie that's set in 2054, the biggest pitfall of what was thought to be a highly successful method of fighting crime was revealed to be the notion that once people are aware of their future, they are able to change it, so the program is shut down and all of the prisoners are freed.[114] This chilling picture of punishing people based only on the notion of probability is completely counter-intuitive to our society and the criminal justice system. Mathematical probabilities can abstract away from the specific facts of the case and as a substitute, it prods fact finders to derive their decisions from the general frequencies of events. For this reason, our courts apply mathematical probability only to a small number of

when the drones are collecting information from a place where a person has a "reasonable expectation of privacy.").

[112] Nate Berg, *Predicting Crime, LAPD-style*, THE GUARDIAN, June 25, 2014.

[113] Minority Report (Amblin Entertainment 2002).

[114] *Id.*

well-defined categories of cases such as defective products, doctors' liability for patients' lost chances to recover from illness, employers' liability for discriminating against classes of employees, trademark infringers' liability for consumer confusion, and the election law protection against redistricting manipulations.[115] For factual determinations in other types of cases, mathematical probability is simply irrelevant, although it may play a role as part of an expert witness's testimony that fact finders merge with the specifics of the case, as they often do with DNA evidence.[116]

It follows then, that accusing a person of a crime based on a probability is fallacious and should always be forbidden. People are rightfully wary and outraged at the notion of accusing others of crimes they have not committed. However, this type of reference to law enforcement's analytical techniques is very inaccurate and misunderstood. Unlike the characters of the movie, Minority Report, who are seers that can see into the future, machine learning technologies employed in data analytics are a purely scientific phenomenon based on existing facts.[117] Even the word "predictive" is not an accurate description of what the analytics actually do, but rather the correct term to describe these scientific findings would be probabilistic.

In today's technologically evolving age we are no longer limited to the traditional sciences such as mathematics, biology and physics. Although originally born out of statistics,

[115] *See* Thornburg v. Gingles, 478 U.S. 30, 52–61 (1986) (approving use of statistics for determining racially polarized voting and minority vote dilution); Schechner v. KPIX–TV, 686 F.3d 1018, 1022–25 (9th Cir. 2012) (using statistics to determine age and gender discrimination in employment); J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION §§ 23:1–18 (4th ed. 2008) (attesting that courts rely on consumer survey statistics to determine likelihood of consumer confusion in trademark infringement suits); ARIEL PORAT & ALEX STEIN, TORT LIABILITY UNDER UNCERTAINTY 61–67, 116–29 (2001) (analyzing court decisions that used mathematical probability to determine manufacturers' market-share liability and doctors' liability for patients' lost chances to recover).

[116] *See* Andrea Roth, Safety in Numbers? Deciding When DNA Alone is Enough to Convict, 85 N.Y.U. L. REV. 1130 (2010) (explaining how DNA evidence integrates with other evidence presented in criminal trials and when it warrants a finding "beyond a reasonable doubt" upon which jurors should convict the defendant).

[117] Minority Report (Amblin Entertainment 2002).

data science has emerged as a separate area of study in the wake of modern day data mining technology. Vasant Dhar, a professor at the Stern School of Business and the Center for Data Science at New York University and the Editor-in-Chief of the journal Big Data, defines data science as the study of the generalizable extraction of knowledge from data. [118]

The significance of data science being categorized as an actual science is the general notion that science is accepted to be a reliable and precise body of knowledge. So why then is the biggest criticism of data science is its reliability? First, the problem lies in the use of probabilities as evidence. As discussed earlier, probabilities should be looked at with great caution. [119] Probabilistic evidence is generally disfavored because probability is just that, a likelihood, it does not and should never be used to prove causation. However, knowledge of a high probability of an event happening is a powerful tool. Thus, when creating drone legislation probabilistic model can come as an extremely useful and powerful tool, but should not itself be used as evidence if it led to the apprehension of an offender if the crime does happen.

The best and most efficient method of using a predictive analytical model is to use a certain degree of probability, for example an 80% likelihood that an individual will commit a crime as probable cause for the surveillance of that individual. After obtaining a warrant, based on these analytical finding drones can then be employed for surveillance purposes. It is important to keep in mind that the software that is run to develop these probabilities is a scientific tool and should be regarded in that manner. To guarantee a certain degree of accuracy of the analytical model itself, the algorithms chosen in the predictive software to determine those probabilities should be validated, tested and submitted for outside study as is required for other forensic law

[118] Vasant Dhar, Data Science and Prediction, COMMUNICATIONS OF THE ACM, Vol. 56 No. 12, Pages 64-73, (Dec. 2013).
[119] *See supra* notes 115-116.

enforcement tools.[120] Furthermore, as would be expected from any other scientific tool, the software should be tested by not only law enforcement personnel but primarily by academics and scholars who are experts in the field of data science.[121] Although this approach to development of predictive software may be met with criticism from law enforcement agents who will want to maintain the secrecy of the software in order to ensure that it does not get into the hands of the wrong people and that its vulnerabilities will not be exploited, it is a necessary measure to ensure a basic level of transparency from the methods used by law enforcement and a necessary safeguard in ensuring the legitimacy of the software and its use.

Some police departments have already developed predictive policing models of identifying and fighting crimes and have even planned to adopt that technology in identifying areas for drone surveillance.[122] "PredPol is now being used in a third of the LA Police Department's 21 geographical policing divisions… [and] dozens of other cities across the US and beyond are using the PredPol software" including police departments in Atlanta, Seattle and Kent, England.[123] Every police department uses this software differently, mostly targeting areas and times where crime may be committed as opposed to identifying individuals who may commit it and the software is mostly concentrated on specific types of crimes such as property, robberies, drug crimes or gun violence.[124] Captian of the Los Angeles Police Department, John Romero, pointed out that identifying geographical areas where crime is most likely to be committed based on previous statistics is a practice that has been widely used by police departments world-wide since the 1990s, but "the [predictive] algorithm is doing much more

[120] See NIST. (Nov 2001). General Test Methodology for Computer Forensic Tools. www.cftt.nist.gov/Test Methodology.doc pp. 1-8, 2001.

[121] *Id.*

[122] Nate Berg, *Predicting Crime, LAPD-style*, THE GUARDIAN, June 25, 2014.

[123] *Id.*

[124] *Id.*

than just telling cops what they already know, 'it's using much larger collections of data, and processing it in a much more sophisticated mathematical way that allows you to produce significant boosts over just hotspot mapping alone,' explained Jeffrey Brantingham, professor of anthropology at UCLA who helped develop LAPD's predictive software.[125] Interestingly, the article is silence regarding whether this software has been tested and if so how and by whom and what types of data other than previous crimes is used by the algorithms.

Another example where analytical software aided law enforcement is in a study of computer pattern analysis in one of the unsolved homicide cases in Louisiana.[126] In a collaborative effort, researchers in neural network analysis with the Jennings Police Task force combined text mining with point-pattern analysis to a high-profile homicide series case that was attributed to a serial killer.[127] Information that was analyzed was taken from Orion, a web-based database that can be accessed by local, state, and federal law enforcement officials, made up of "Information Packages" that contain email correspondence, transcribed face-to-face interviews and phone calls.[128] The text mining and point pattern analysis specifically focused on the eighth and last victim of the homicide series analyzing 172 individual information packages that were connected or associated with the victim.[129] This data-mining approach is useful because it is done faster then an analysis by a person and the algorithm is able to draw connections between various factors in evidence that may be missed by investigators because they are not readily

[125] *Id.*

[126] Marco Helbich , Julian Hagenauer , Michael Leitner , Ricky Edwards, Exploration of unstructured narrative crime reports: an unsupervised neural network and point pattern analysis approach, CARTOGRAPHY AND GEOGRAPHIC INFORMATION SCIENCE, Vol. 40, Iss. 4, 2013.

[127] *Id.*

[128] *Id.*; *Catching Criminals with the World Wide Web,* WASHINGTON TECHNOLOGY, Oct. 10, 1996, available at https://washingtontechnology.com/Articles/1996/10/10/Catching-Criminals-With-the-World-Wide-Web.aspx?Page=2.

[129] Marco Helbich , Julian Hagenauer , Michael Leitner , Ricky Edwards, Exploration of unstructured narrative crime reports: an unsupervised neural network and point pattern analysis approach, CARTOGRAPHY AND GEOGRAPHIC INFORMATION SCIENCE, Vol. 40, Iss. 4, 2013.

apparent to a human and because the sheer volume of the data makes it hard to effectively piece together the details and draw the connections.[130] The study stated that "[t]he results from this data mining exercise have already been presented to and shared with the Jennings Task Force, which confirmed that this information was previously unknown and may provide new and important clues in this criminal investigation. However, due to confidentiality reasons and this being still an open criminal investigation, the authors of this research cannot go into more detail as far as the specifics of this 'previously unknown information' and 'new and important clues' are concerned."[131]

Both the LAPD PredPol software and the Jennings pattern analysis study demonstrate the value and assistance data analytics provide to law enforcement agencies. With the information overload that police forces are faced with as a result of American social networking culture, it is next to impossible for law enforcement officials to sift through the data that they have access to and make sense of it on their own. Data mining and analytics software is evolving at an insurmountable speed and will likely be widely employed by law enforcement in the near future regardless of individual's feelings towards this technology. Already, one of the Big Data leaders, Information Builders is offering law enforcement agencies a software service, Law Enforcement Analytics (LEA), a cross-platform data-mining and analytics technology with geographical reporting and mapping and predictive analysis capabilities.[132] Michigan State Police Department and Charlotte-Mecklenburg Police Department are at least two police departments that are already using LEA.[133]

[130] *Id.*
[131] *Id.*
[132] *Law Enforcement Analytics: Intelligence-Led and Predictive Policing*, INFORMATION BUILDERS; available at http://www.informationbuilders.com/solutions/gov-lea.
[133] *Id.*; Suzanne Kattau, *Using Predictive Policing to Prevent Crime*, RT INSIGHTS, available at http://www.rtinsights.com/using-predictive-policing-to-prevent-crime/.

Although, allowing analytical software to identifying geographical areas is a good way to allocate what areas are most in need of surveillance and to determine where to allocate drones for surveillance purposes, it may create some undesirable consequences. From the standpoint of allocation of resources, it makes sense that surveillance should be done where it's most needed. Resources are not unlimited, thus an effective way to allocate them is key in efficient and effective policing. However, albeit being an obvious and common sense choice directing drones to crime hot spots for surveillance purposes may not be the most desirable way to allocate those resources. One possible issue with continuous surveillance of a specific geographical area is that it may result in continuous surveillance in a specific individual or group of individuals without a probable cause warrant. To address questions of pervasive surveillance courts have previously decided cases related to GPS surveillance practices.

United States v. Knotts was one of the first cases to apply the Fourth Amendment to the use of a tracking device.[134] *Knotts* upheld the use of a tracking beeper device that had been placed in a container of choloroform that was sold to the defendant with the suspicion that was bought for use in drug manufacturing.[135] The police followed the cars in which the container was placed with a monitor receiving the beeper signals, lost contact once, and found the beeper signal again, stationary at a cabin in Wisconsin.[136] The officers used that information to secure a search warrant for the cabin.[137] They found a drug laboratory in the cabin and the container of chloroform outside.[138] The Court decided there was no intrusion into the defendants' reasonable expectation of privacy because the location of the car containing the container had been

[134] United States v. Knotts, 460 U.S. 276 (1983)

[135] *Id.* at 278.

[136] *Id.*

[137] *Id.* at 279.

[138] *Id.*

voluntarily conveyed to the public – the car was driven on public roads and the container was placed in open fields clearly visible from public spaces.[139]

One year after *Knotts*, the Court decided a second "beeper" case, *United States v. Karo* that distinguished the heightened privacy interests in a private residence.[140] In *Karo*, the item tracked with a beeper was brought into a private residence.[141] DEA agents had learned that the defendants ordered fifty gallons of ether from a government informant, who told the agents that the ether was to be used to extract cocaine from clothing that was imported to the United States.[142] The agents obtained an order authorizing the installation of a beeper in one of the houses.[143] Determining the can of ether was inside one of the houses, the agents obtained a search warrant, found the cocaine, and arrested the defendants.[144] The Court held that the transfer of a can containing an unmonitored beeper conveyed no information the recipient wished to keep private, so it conveyed no information at all.[145] It also did not interfere with a possessory interest in a meaningful way so no Fourth Amendment interest was infringed.[146]

It also concluded that it would be a search to surreptitiously enter a residence without a warrant to verify that a container was there, but that is not what was done here because the chain of custody could have been observed by merely watching the ether travel on the public highways to the house from the outside of the curtilage. [147]

In 2001, the Court applied some of these principles to heat-sensing technology used to detect the heat signature of marijuana-growing lights emanating from the walls and roof of a

[139]*Id.*
[140] United States v Karo, 468 U.S. 705 (1984)
[141] *Id.* at 708.
[142] *Id.*
[143] *Id.* at 709.
[144] *Id.* at 710.
[145] *Id.* at 712.
[146] *Id.* at 713.
[147] United Sates v. Karo, 468 U.S. 705 (1984)

suspect's house.[148] The Court held that the use of sense-enhancing technology to gather information about the interior of a home that could not otherwise be obtained absent physical intrusion into the home requires a warrant "at least where the technology in question is not in general public use.[149]

This was the jurisprudential contest in which the Supreme Court decided its first GPS case, *United States v. Jones*.[150] The question in *Jones* was whether police had violated the Fourth Amendment in placing a GPS tracker on a suspect's car and tracking the car for twenty-eight days without a warrant.[151] Writing for the majority, Justice Scalia chose not to follow the "reasonable expectation of privacy" inquiry and instead applied the physical trespass test, holding that placing the GPS device on the car constituted a physical trespass, so the warrantless search violated the Fourth Amendment.[152] Justice Scalia reasoned that under the common-law trespassory test, the government physically occupied private property for the purpose of obtaining information.[153] Such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.[154] Defendant possessed the vehicle at the time the Government trespassorily inserted the information-gathering device.[155]

The Government forfeited its alternative argument that officers had reasonable suspicion and probable cause.[156] Justice Scalia declined to decide the reasonable expectation of privacy question.[157] However, in Justice Alito's four-justice concurrence and Justice Sotomayor's

[148] Kyllo v. United States, 553 U.S. 27 (2001)
[149] Kyllo, 553 U.S. at 34.
[150] Unites States v. Jones, 132 S. Ct. 945, mandamus denied, 670 F.3d 26 (2012)
[151] *Id.* at 948.
[152] *Id.* at 952.
[153] *Id.* at 949.
[154] *Id.*
[155] *Id.* at 948.
[156] *Id.* at 954.
[157] *Id.* at 947.

separate concurrence, five justices applied the reasonable expectation of privacy test.[158] Justice Alito argued that the four-week tracking in Jones violated society's reasonable expectation of privacy, but that a shorter-term tracking might not.[159] Justice Sotomayor went further and noted the privacy implications of location tracking: it could capture "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[160] Such information can create "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[161]

Unlike a camera on a public street near someone's house or apartment building that may capture repeated footage of the same person passing on the street at particular times, drones will not be stationary. There would be no benefit to employ a drone over using a camera if law enforcement intended to use the drone itself as a CCTV camera. Drones will move over a specific geographical area. If one or more drones move over the same urban geographical area over a prolonged period of time, that drone may capture footage of an individual leaving their house to go to work which may or may not be nearby, then meeting with their friend at a bar down the street, coming home late at night, visiting the neighbor's house the next night, associating with friends who live in the same neighborhood on the weekend. This type of profile that is built over time is beyond what a stationery camera can capture and depending on the person's lifestyle can be very similar to GPS surveillance. What would be more disturbing is that the only thing separating a person under constant, continuous surveillance from a person who is

[158] *Id.* at 957-958.
[159] *Id.* at 964.
[160] *Id*. at 955.
[161] *Id.*

not would be their geographical presence – where they happen to live, work and socialize. Thus, a housewife and a stay at home mother who spend most of their time at home, at the park down the street and the grocery stores a few blocks away would be under continuous surveillance because they are in a target neighborhood where the drone is deployed but a criminal who lives, engages in criminal activities and works at different geographical areas of substantial distance from each other would not. This surveillance technique could adversely impact individuals in a way that Justice Sotomayor has cautioned of in *Jones*.[162]

Although drone surveillance by geographical locations does not fall squarely into the ambit of *Jones*, *Kyllo* or *Karo* because under this surveillance approach a drone would not consistently follow a specific person within the geographical area, nothing would get attached to a person's property and with the help of geofencing, private spaces would be safe from surveillance, those cases demonstrate that use of technologies to conduct pervasive surveillance of individuals is disfavored by the Supreme Court. Furthermore, in 2010, in yet another GPS surveillance case in the Superior Court of Delaware, Judge Jurden expressed concerns created by pervasive surveillance through modern technology such as the GPS that eerily reflect continuous drone surveillance of specific areas. [163] In *United States vs. Holden*, the court concluded that, absent exigent circumstances, the warrantless placement of a GPS device to track a suspect 24 hours a day constituted an unlawful search.[164] While individual have a diminished expectation of privacy in their vehicles, prolonged GPS surveillance provides more information that one reasonable expects to expose to the public.[165] In addition, the court concluded "even if there is no reasonable expectation to be free from casual encounters by others in the public sphere, society

[162] *Supra* notes 81-82.
[163] State v. Holden, 54 A.3d 1123, 1124, 2010 Del. Super. LEXIS 493, *1 (Del. Super. Ct. 2010)
[164] *Id.* at 1134.
[165] *Id.*

reasonably expects to be free from constant police scrutiny."[166] In analyzing GPS surveillance's violation of a person's reasonable expectation of privacy, Judge Jurden stated:

> Prolonged GPS surveillance provides more information than one reasonably expects to "expose to the public." The whole of one's movement over a prolonged period of time tells a vastly different story than movement over a day as may be completed by manned surveillance. GPS "facilitates a new technological perception of the world in which the [location] of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period." It takes little to imagine what constant and prolonged surveillance could expose about someone's life even if they are not participating in any criminal activity.
> GPS surveillance does not simply enhance an officer's sensory capabilities and represents more than a mere alternative to conventional physical surveillance. GPS has the capacity for obtaining and recording information which greatly exceeds the ability of conventional surveillance such that "[t]he potential for a similar capture of information or 'seeing' by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp." The possibility is remote that law enforcement could maintain 24-hour surveillance of a suspect for a prolonged period of time. There is a "difference between [] uninterrupted, [constant] surveillance possible through use of a GPS device, which does not depend upon whether an officer could in fact have maintained visual contact over the tracking period, and an officer's use of binoculars or a flashlight to augment his or her senses." GPS completely replaces conventional surveillance such that one officer with a single computer could record and monitor the travels of hundreds into perpetuity.[167]

Although the court seems to be concerned with pervasive surveillance of individuals, this concern can be cured with restrictions on duration of surveillance of a particular area and restrictions against targeting of individuals focusing instead on surveillance of an area rather than a person or group of people. Moreover, with geofencing, drones can be limited only to the plain view of public places analogous to investigative surveillance.

Another possible civil liberty concern that can arise with the geographical allocation of drones is a disproportional effect on certain neighborhoods and racial profiling. Racial profiling

[166] *Id.* at 1133.
[167] *Id.* quoting United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) and People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009).

has been an issue of public debate for decades and can be traced back as a practice to the 1700s.[168] Racial profiling can be defined as "the use of race, ethnicity, gender, religion, or national origin by law enforcement agents as a factor in deciding whom to investigate, arrest or detain absent evidence of a specific crime or criminal behavior."[169] Racial profiling impacts people of African American and Hispanic descents and Muslim religions in their day-to-day lives.[170]

In publicized police brutality cases police violence and use of deadly force has also been often attributed to racial profiling or at the very least the individuals' bias created due to racial profiling.[171] Police Departments do not deny this practice, in an interview with the Newark-Star Ledger, a New Jersey State Police Superintendent admitted that his department targets minorities in narcotics investigations because they are usually the ones involved in those crimes.[172] New York Police Department has also admitted to targeting minorities in stop and frisk searches because minority neighborhoods are the places where most of the crime occurs and minority groups are statistically responsible for the majority of violent crimes.[173] "This type of thinking means that anyone who is African American is automatically suspect during every drive to work, the store, or a friend's house. Suspicion is not focused on individuals who have committed crimes, but on a whole racial group. Skin color becomes evidence, and race becomes a proxy for general criminal propensity."[174]

[168] Keith Rushing, *Dissecting the Long, Deep Roots of Racial Profiling in America*, HUFFPOST BLACK VOICES, May 1, 2013, available at http://www.huffingtonpost.com/keith-rushing/dissecting-racial-profiling_b_2740246.html.

[169] *Id.*

[170] *Id.*; Stephen K. Rice, Race, Ethnicity and Policing: New and Essential Readings, 2010, p. 37.

[171] Obeydah Chavez, *Police Brutality: Excessive Force and Racial Profiling*, LIBERTY VOICE, Aug. 13, 2014, available at http://guardianlv.com/2014/08/police-brutality-excessive-force-and-racial-profiling/.

[172] Stephen K. Rice and Michael D. White, Race, Ethnicity and Policing: New and Essential Readings, p. 37.

[173] Heather McDonald, *Fighting Crime Where the Criminals Are*, THE NEW YORK TIMES, June 25, 2010, available at http://www.nytimes.com/2010/06/26/opinion/26macdonald.html?_r=0.

[174] Stephen K. Rice, Race, Ethnicity and Policing: New and Essential Readings, p. 37.

One of the insurmountable advantages of analytics software is that they are colorblind. Analytics are done based on a variety of facts, but machines simply make objective connections between those facts, they are not influenced by any innate bias and factors such as race, ethnicity, gender, religion and national origin can and should be left out of the analytics equation altogether. Thus, when making a profile of suspects and areas of probable crimes, the findings will be based on the factual investigative factors such as criminal history, witness interviews, information obtained by confidential informants, public information obtained through public social media sources and the like. However, if geographical drone surveillance is employed, this will not eliminate a disproportionate impact on minority communities and underprivileged communities. Statistically, crime happens to a greater degree in impoverished and minority neighborhoods, thus that population will be targeted the most. However, that means that for example, sprawling estates of Alpine, New Jersey will have no surveillance of residents, while equally law abiding residents of impoverished areas of Newark, New Jersey will inevitably be subjects to continuous, pervasive surveillance.[175] In considering whether such practices should be allowed legislators might consider two approaches: the security trumps approach or the probable cause approach.

Legislators may choose to allow this disproportionate impact on certain neighborhoods, because arguably safety trumps a disproportionate impact of inconvenience and privacy encroachments of a few people. This approach is defended by one of the leading scholars in the area of privacy and security, Kenneth Himma, in a chapter of the book *Privacy, Security and*

[175] *Compare* crime rates in Alpine, NJ where 5 violent crimes per 100,000 capita occurred over a 13 year time period *with* crime rates in Newark, NJ where 18,410 violent crimes per 100,000 capita occurred over a 13 year time period. City-Data.com, “Crime rate in Newark, New Jersey (NJ): murders, rapes, robberies, assaults, burglaries, thefts, auto thefts, arson, law enforcement employees, police officers, crime map,” available at http://www.city-data.com/crime/crime-Newark-New-Jersey.html; City-Data.com, “Crime rate in Alpine, New Jersey (NJ): murders, rapes, robberies, assaults, burglaries, thefts, auto thefts, arson, law enforcement employees, police officers, crime map,” available at http://www.city-data.com/crime/crime-Alpine-New-Jersey.html.

Accountability.[176] Himma argues that security trumps privacy and thus legitimizes certain privacy encroachments because being protected from violent acts of assault and theft is ranked more importantly then any privacy interest possessed by any given individual and because the government has a duty to protect its country and citizens from violence.[177] In essence, Himma says that physical security is always more important than privacy and should trump privacy interests when security and privacy are in conflict.[178] When looking at especially dangerous neighborhoods in the U.S. such as the L.A. street nubbed the Death Valley because of its violence and homicide rates or the physical threat and fear faced by people of Baltimore after the protests that caused reduction in police patrol, Himma's reasoning is demonstrated at its core.[179] In those situations and neighborhoods where violence is prevalent and residents are confronted with fear of physical harm on an everyday basis, it is hard to argue that residents' need for security and state officials' moral obligation and legal duty to provide it doesn't outweigh the need for privacy. Himma argues that there's an hierarchy of collective and individual rights and although security and privacy are both important, security interest "construed to include freedom from grievous threats to well-being, which include death, grievous bodily injury, and financial damage sufficiently extensive to threaten the satisfaction of basic needs, and hence survival, of a person — are at the top of the moral hierarchy, encompassing as they do the rights to life and physical preservation."[180] In Himma's view because security is essential to survival, and privacy is not, security interests will always trump the need for privacy where protecting individuals' privacy threatens physical security of others.[181]

[176] Privacy, Security and Accountability: Ethics, Law and Policy (Kindle Location 279). Rowman & Littlefield International. Kindle Edition.
[177] *Id.*
[178] *Id.*
[179] *See supra* note 91.
[180] Privacy, Security and Accountability: Ethics, Law and Policy (Kindle Locations 3501-3503).
[181] *Id.*

It is of no doubt that the physical security of life and limb is one of the most important moral and legal interests of all people, but whether physical security is always easily trumped by privacy is a heavily contested notion by many scholars. For example, Bruce Schneier pointed to the psychological impacts of surveillance on individuals stating that empirical data supports that surveillance makes people feel like prey.[182] Thus, although a lack of privacy may theoretically provide greater physical security, it may also have very detrimental psychological impacts that are not justified by physical security interests surveillance purports to protect.[183] Another scholar, Annabelle Lever, argued that surveillance might not even provide the benefit of physical security. In her view, impersonal surveillance conflicts with principals of democracy and is an arbitrary application of power that may actually diminish security for people on the margins of society.[184]

The security trumps approach justifies prolonged drone surveillance in neighborhoods with high rates of violent crimes. However, the best way to protect privacy interests and discourage the possibility of profiling is to tailor the use of drone surveillance to limit the effects of pervasive surveillance. One way to do this is to limit the duration of surveillance in any one geographical area when using the hotspot model of surveillance. If drones are deployed only for a limited time, possibility of pervasive surveillance of specific residents of the neighborhood is then limited. However, it is unclear how this approach will be beneficial since it would be highly improbable to predict the time and location of a violent crime, therefore if drones are deployed to any given place for a short time, it is unclear if it would ever be deployed to the right place at the

[182] *Id.*
[183] *Id.*
[184] *Id.*

time of a crime, but further research may be conducted to check the effectiveness of this approach.

The second approach to drone surveillance, using machine-learning analytics is the probable cause approach. This approach would allow law enforcement to use drones for individual surveillance upon finding probable cause for such surveillance. Although this essentially requires a search warrant similar to many existing legislations, the use of analytical software can aid law enforcement in identifying suspects and meeting the probable cause standard. Machine learning software can create suspect profiles based on information in public online spheres and police databases such as Orion and LEA, similar to what the Chicago Police is already doing with their predictive policing software.[185] Chicago Police Department uses an algorithm to compile a "heat list," a report that ranks high probability suspects at risk of committing violent crimes.[186] This approach is highly criticized, because Chicago Police Department has not disclosed a comprehensive description of the algorithm's input.[187] "Chicago's experiment is one of several of a new type, in which police departments move beyond traditional geographic "crime mapping" to instead map the relationships among city residents. Specifically, identifying individuals for tailored intervention is the trend most likely to expand in the future of predictive policing…"[188]

As discussed earlier, this type of machine learning software could be extremely helpful in allowing police to use drones in the most efficient and effective way.[189] If an algorithm goes through hundreds or thousands of different pieces of documents, evidence and information and

[185] *See infra* note 98, 100-101 and 104; Civil Rights, Big Data, and Our Algorithmic Future, Chapter 3: Criminal Justice, "Predictive Policing: From Neighborhoods to Individuals," Sept. 2014, available at https://bigdata.fairness.io/predictive-policing/.
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *See supra* note 127.

maps the relationships between people and crime, then pointing to the existence of probable cause of an individual committing a crime, then that evidence should in fact be treated as probable cause evidence allowing surveillance of that individual.[190] It is important to keep in mind that the police would not be arresting people on the probability that they will commit a crime; instead they would obtain evidence in the more efficient way of piecing evidence together through use of an algorithm rather than manpower.

Furthermore, the technology can be designed with certain standards and limits in place to ensure safeguards against its misuse and inaccuracy. Caracterizing predictive policing software as a forensic tool will ensure that it is properly tested and in the most effective manner.[191] Moreover, as with any data that is handled by law enforcement - transparency, auditing and due diligence procedures are imperative to ensure government accountability and oversight over its use of the data.

V. CONCERNS

One limitation that should be put on the use of drones in any circumstance is equipping the drone with lethal or non-lethal weapons. Currently, a North Dakota House Bill permitting drone use by law enforcement with certain limitations prohibits the equipment of drones with only lethal weapons, which means that drones can be equipped with non-lethal weapons such as tasers, rubber bullets or tear gas.[192] It is easy to see the benefit of arming a drone for the purpose of preventing a crime. A suspect can be quickly neutralized by a drone that is likely to have a higher precision and accuracy rate than a human wielding the same weapon, but the one thing a machine will always lack over humans is the ability to make judgment calls, thus weaponized

[190] *See supra* note 127.

[191] *See* NIST. (Nov 2001). General Test Methodology for Computer Forensic Tools. www.cftt.nist.gov/Test Methodology.doc pp. 1-8, 2001.

[192] HB 1328

drones should never be employed to use weapons autonomously based on neural network analytics. Another issue with weaponizing a drone is the fact that machines may sometimes malfunction. Imagine a law-abiding person minding their own business at a parade or a convention being shot with a taser or something along the lines of a tranquilizer due to a malfunction of the drone. Even if the margin of a possible malfunction is so small that there is only a 1% chance of that happening, that is a chance that a completely innocent person may be harmed by the technology. That chance is almost completely eliminated if the drone is not weaponized. With current technology drones can be so light and small in size that even if a malfunction will cause it to fall and crash into a person, the person will be unlikely to sustain any real injuries.[193]

In an article criticizing North Dakota's bill for failure to ban non-lethal weaponization of drones, ACLU outlined some other reasons why weaponization should not be allowed.[194] Among them is the ease with which non-lethal force is used and the potential to overuse such force when operating a robotic device without the officer's physical presence at the scene; the fact that nonlethal weapons do routinely kill people, for example, there has been at least 39 deaths in 2015 as a result of using tasers where about 90% of the victims were unarmed; the officers will more likely to experience flawed judgments if their perception of the situation is over a greater distance and where they are not physically present; weaponization of drones with non-lethal weapons is a slipper slope to weaponizaton of drones with fully lethal weapons; and weaponization of drones will increase the militarization of police which may shift law

[193] Nidhi Subbaraman, *MIT's entry in Dubai's 'Drones For Good' contest is a drone swarm that can land on water*, THE BOSTON GLOBE, Feb. 2, 2015, available at http://www.betaboston.com/news/2015/02/02/mits-entry-in-dubais-drones-for-good-contest-is-a-drone-swarm-that-can-land-on-water/. The article provides examples of tiny swarming drones that are developed by robotics teams at MIT and Harvard.

[194] Jay Stanley, *Five Reasons Armed Domestic Drones Are a Terrible Idea*, American Civil Liberties Union, Aug. 27, 2015, available at https://www.aclu.org/blog/free-future/five-reasons-armed-domestic-drones-are-terrible-idea.

enforcement approach from a community policing model into a greater militarized “us versus them” mentality.[195] Of these, a particularly important factor to consider in weaponization of drones is the potential to overuse weapons because while drones are extremely useful tools for surveillance purposes, they are also extremely impersonal. This impersonal nature of drones does not create any physical harm when it is employed for observational and identification purposes, but when used in a tactical nature there is more concern with the use of the drones since the distance and lack of physical presence of an officer may lead to dehumanization of his or her actions making it easier to use force in a much more liberal fashion then during a face to face interaction.[196] As in the case of use of robotic lethal force in military operations “[t]he greater the distance between the killer and the victim, the less emotional restraint that will be shown on the part of the former,” the same outcome would likely result in the implementation of robotic non-lethal force.[197]

Legislators may be swayed towards weaponization of drones in highly dangerous environments involving active shootings and hostage situations where weaponized drones could have the potential to save civilian and officers’ lives. To mitigate security risks with concerns regarding use of robotic weaponization, a very narrow exception to weaponized drones may be carved out. Law enforcement may have a separate type of weaponized drone that may be deployed only when faced with an active shooter or a hostage situation that poses a risk to human life. The drone should not be autonomous, it should be operated by a trained officer, who identifies and confirms the target and gives the drone a command to use the appropriate force on that target. In making the judgment call to use the force, the officer may take into considerations

[195] *Id.*

[196] Symposium: The Global Impact and Implementation of Human Rights Norm: Targeted Killing at a Distance: Robotics and Self-Defense, 25 Pac. MCGEORGE GLOBAL BUS. & DEV. L.J. 361

[197] *Id.*

neural network analytics that are presented through use of drones such as the probability that the suspect is in fact in possession of a gun or a grenade or similar lethal weapon only as an aid to help his own observation (such analytics could be helpful in assessing the situation but the use of force should be a carefully made judgment call by the officer), the officer should be able to see the weapon and asses the suspect's danger through the footage transmitted by the drone and should only use the weapon if he sees no safer alternative to neutralize the suspect. The drone should also be equipped with communication technology to make possible negotiations with the suspect. The most important aspect to this exception is that a drone used in this situation should be a specialized drone employed in a known, ongoing, extremely dangerous situation. Drones used for surveillance purposes of places or individuals should never be equipped with either lethal or non-lethal weapons.

Another very worrying considerations in the use of any modern day technology is that it can be hacked. Drones that are operated to survey a certain area or a certain person can be hacked and operated by criminal parties to redirect it to another area or another person during the commission of the crime. A police department may be hacked in an attempt to erase footage of criminal activity that is captured by a drone or predictive policing software can be hacked to manipulate the data that is used by algorithms. In extreme cases, data or video footage may even be manipulated to "frame" another person for a crime that someone else has committed. Although these types of vulnerabilities should be examined and considered very carefully when designing and security the technology; they should not serve to prevent the use of the technology altogether. Typically, this sort of hacking is fairly sophisticated and cannot be done by someone who is only marginally versed in this type of technology. Also, if drones are implemented to target primarily suspects of violent crimes as opposed to white-collar crime, then the amount of people with enough knowledge that would enable them to hack into a police framework would be limited since it is usually white collar criminals who are more sophisticated and educated in fields such as computer science. Of course, this does not mean that violent criminals are absolutely not capable or are not intelligent enough to eliminate them as potential threats and the subjects of surveillance are not necessarily the only ones who can attempt hacking a law enforcement drone or computer system, but any technologically based system could theoretically be hacked and yet we do not propose that businesses and individuals should never use internet or that credit card transactions should be absolute in light of data breach threats, instead we expect better designed and more secure systems. Data used by police department is highly sensitive, but so is data used by banks and medical providers, yet it is not a popular argument that we shouldn't provide them with that data altogether. People take it as a granted that providing sensitive personal information to banks and medical providers is necessary for them to do their job, but do not give the same considerations to police. Similarly, studies should be conducted regarding the security measures and vulnerabilities of technologies involved in drone policing and legislation allowing drone surveillance should mandate that police departments take reasonable measures to protect it systems and data from third party breaches.

Another possible threat to drones could be physical damage. If spotted, drones could be taken down with a gun or other similar measure. Current technologies also make it easier to determine if there are any drones nearby. For example, a company called DroneShield provides acoustic sensors to identify drones in the area based on the unique noises that their motors make.[198] Another company, Drone Labs has drone detection technology that uses radio waves that can alert users through text messages, app notifications or email about a detected drone in

[198] Chris Baraniuk, No Drone Zone, NEW SCIENTIST, Vol. 226 Issue 3019, p. 22, May 2nd 2015.

their area, while a France-based company MALOU Tech developed a manually operated drone that could capture other drones by firing a net.[199] Though currently these companies' clients are lawful entities that consist mostly of government agencies, airports, sports stadia, and celebrities who are concerned about uses of drones for unlawful purposes, it is easy to predict that the roles can be easily reversed and the same technology could be used against police drones by the criminals they are employed to survey.[200]

It is unclear what measures if any can be taken to prevent police drones from being detected as technologies on both sides of the spectrum will continue to evolve, but if a drone is captured there are different factors that that are both comforting and disturbing in determining the repercussions. First, if a drone is captured, that does not mean that any data can or will be recovered from the drone. Drones shouldn't store any data on the hard drive of the drone itself, rather drones should stream whatever footage they capture to a secure server where the data is encrypted and can be accessed by authorized police personnel only. Next, despite an offender's inability to access data captured by the drone, loss of the drone itself can cause a great cost to the department. Although drones are becoming increasingly cheap, it is unclear how much police drones would cost to the department, what capabilities they will ultimately be equipped with and how much its network configurations that will communicate with the police command centers and servers will contribute to the overall cost of an individual drone. Also, to accurately analyze costs we of course would have to know the extent of the damage to a drone and the frequency of such damage and the types of drones employed. These costs may either be very significant or largely insignificant. For example, if swarming is used, then each drone is relatively inexpensive and concerns over one drone being taken down are curtailed by the fact that there are several

[199] *Id.*
[200] *Id.*

others in the same location and depending on different factors it may be extremely difficult to capture or detect all of them because of the size of these drones.

Legislators should keep in mind that while damage of drones may be addressed by existing legislations dealing with damage of police property, capturing or interfering with police drone operations may have to be addressed as a separate infraction to deter such instances.

CONCLUSION

Drones are a truly transformative technology that is growing, evolving and being utilized with an unbelievable speed comparable to the Internet and the evolution of computer technology in the late 1980s. As opposed to computers and the Internet in that era, however, we are better equipped and able to predict the issues we are likely to face with utilization of drones on a day-to-day basis. Although not so long ago, privacy violations by computers were very hard to visualize because people could not even imagine that somewhere, somehow, by the use of malware, phishing or bot nets bits of information may be correlated to consumers and regular internet users' detriment, the evolution of drone technology does not have to pose the same risk. Drones are not completely novel, so people understand them on a deeper level. We realize the potential of drones and can predict the type of technology that is expected to emerge in the next ten years, such as swarming drones, and craft our legislation to address the issues that it may create. Mere lack of education about the technology should not serve as an obstacle to better and more effective use of that technology. Legislators should not be afraid to do what they have been doing for centuries prior to the emergence of robotics – balance the law enforcements' use of the latest technology for enhanced investigative techniques, officer security and protection of citizens with individual personal liberties and come up with a reasonable solution for all parties.

In creating drone legislation, legislators should focus on what rights they want to protect and what surveillance capabilities they want to enable law enforcement with and tailor the legislation to allow the type of technology that will enable law enforcement to do their job in the most effective way while preventing any predictable abuses of the technology. The key point in creating legislation is that any potential abuses can be cured with technological restrictions rather then a restriction on the use of the technology itself as a whole. Geofencing can limit surveillance to only the plain view in public spaces, time limitations can restrict the use of pervasive surveillance, encryption can protect arbitrary access of data, while analytics can help with identifying suspects and suspicious activities. Strict restrictions on the use of technology in law enforcement investigative and policing duties will result in restrictions on police capabilities to secure the safety of its citizens. Thus, to ensure that drone technology benefits law enforcement and serves to ensure the safety of civilians without jeopardizing their civil liberties, legislators should work closely with engineers, not lawyers to understand the best way to achieve their goal.