Journal of Technology Law & Policy

Volume XV—Fall 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.159

http://tlp.law.pitt.edu

Behavioral Recognition: Computer Algorithms Alerting Law Enforcement to Suspicious Activity

J Darwin King, Jr.

Behavioral Recognition: Computer Algorithms Alerting Law Enforcement to Suspicious Activity

J Darwin King, Jr.*

INTRODUCTION

Surveillance through the use of closed-circuit television ("CCTV") is becoming more widespread in the daily lives of Americans—a movement fueled by the recent war on terrorism. The decreasing cost of this technology has made it more available than ever before. High technology surveillance, once reserved for only the most secure locations, now appears in public common spaces. Urban centers faced with budgetary concerns see automation in surveillance as a way to cut costs while still protecting the greatest number of citizens.

Despite its benefits, we must consider the costs to our individual freedoms that the use of these increasingly sophisticated systems may entail. Most troubling is the deployment of a new technology called behavioral recognition.[1] This system couples traditional CCTV systems with a monitoring station that uses a computer algorithm to detect events that may be suspicious.[2] Conducted completely free of human monitoring, behavioral recognition shares commonalities with the more widely known technology of facial recognition.[3] However, this new type of technology identifies certain behaviors of an individual as a whole instead of facial features.[4]

The City of Pittsburgh has tall buildings, many bridges and tunnels, sports and entertainment venues, and a convention center that all demand, in today's world, protection from potential terrorist attacks. In 2013, the City reported 46 homicides,

* J.D. candidate, University of Pittsburgh School of Law, May 2016. The author would like to thank Professor David Harris for insightful discussion and reference suggestions. And thanks to Tulsa, Isabel, and Elisabeth for their love and support.

[1] BRS LABS (Dec. 18, 2014, 9:15 AM), http://www.brslabs.com.

[2] *Id.*

[3] *Id.*

[4] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

90 rapes, 967 robberies, and 1,259 aggravated assaults.[5] Pittsburgh, like most American cities, has an interest in improving public safety. In 2007, Pittsburgh created a plan to provide traditional CCTV coverage of the downtown area, along bridges, and Point State Park.[6] The City set aside $3.4 million in port security money, which included $2.6 million in federal funds and $862,000 in city money.[7] The proposal called for the linking of cameras owned by the city, county, state, and private companies, allowing for a central monitoring system for crime deterrence and public safety.[8] In a later decision, Pittsburgh City Council approved the installation of cameras in high crime neighborhoods.[9] Former Councilman and current Mayor of Pittsburgh William Peduto asked that the administration add language outlining a privacy policy within the legislation before the final vote.[10] Since Pittsburgh currently uses traditional CCTV systems, the use of behavioral recognition could be a logical next step. Behavioral recognition would allow a city to safeguard large areas without the need for personnel, thus maximizing safety and minimizing employee costs.

Before the implementation of a behavioral recognition system in Pittsburgh, new rules would have to be put into place to address Fourth Amendment and general privacy concerns inherent in its use. The public should be made aware of the use of this technology in public places, behavioral data collected by third-parties such as private businesses should be released only upon a valid warrant by law enforcement, individuals should not be tracked over large geographic areas without a warrant, and law enforcement should have procedural guidelines of when and how it may use the information gathered.

I. HISTORY OF BEHAVIORAL RECOGNITION IN SURVEILLANCE

We have seen the introduction of police operated CCTV systems in large cities; both the number of cities and the size of the coverage are expanding, such as

[5] City of Pittsburgh Dept. of Public Safety Bureau of Police Annual Report 2013 (Oct. 31, 2014, 12:56 PM), http://apps.pittsburghpa.gov/dps/2013_Annual_Report_draft_(final).pdf.

[6] Rich Lord, *Network of Surveillance Cameras Proposed for Pittsburgh*, PITTSBURGH POST-GAZETTE (Oct. 31, 2014, 11:14 AM), http://www.post-gazette.com/local/city/2007/06/27/Network-of-surveillance-cameras-proposed-for-Pittsburgh/stories/200706270157.

[7] *Id.*

[8] *Id.*

[9] Rich Lord, *Council Oks Surveillance Cameras Around City*, PITTSBURGH POST-GAZETTE (Oct. 31, 2014, 12:10 PM), http://www.post-gazette.com/local/neighborhoods/2007/09/20/Council-OKs-surveillance-cameras-around-city/stories/200709200260.

[10] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

in the subway system of San Francisco which already uses the behavioral recognition technology.[11] However, at the present moment, there are few procedural controls in place for the use of CCTV systems. The technology has advanced very quickly and courts have been slow to respond. Such progress, coupled with a lack of rules, poses a significant danger to our daily lives. High-resolution cameras, the kind that can read papers held in a person's hands, along with facial recognition cameras, have piqued the public's interests and fears.

Ten years ago, *The New York Times* published an article discussing the emergence of artificial intelligence as a way to monitor areas and flag suspicious events.[12] The article spoke of the implementation of this smart system by the year 2006.[13] Richard M. Daley, serving as Mayor of Chicago at the time, claimed that the system would make the streets safer.[14] Mayor Daley said, "They're the next best thing to having police officers stationed at every potential troubling spot."[15] The statement that the system may be "the next best thing" is critical, since a computer algorithm can hardly substitute for a law enforcement officer as witness to an event. The 2004 article described a system that alerts police whenever someone "wander[s] aimlessly in circles," "pulls a car onto the shoulder of a highway, or leaves a package and walks away from it."[16] The surveillance technology described ten years ago is now ready for widespread deployment and is on our streets. In fact, Louisiana's Port Fourchon deployed this technology to safeguard the maritime port from terrorism with the help of the Department of Defense.[17] The system can alert law enforcement in real time to threats of flagged suspicious behavior and allows for the integration of multiple agencies both at the state and federal levels.[18]

---

[11] Liz Klimas, *Will These Next-Gen Surveillance Cameras in Calif. Detect Crime Before It's Even Committed?*, THE BLAZE (Oct. 24, 2014, 10:55 AM), http://www.theblaze.com/stories/2012/06/05/will-these-next-gen-surveillance-cameras-in-calif-detect-crime-before-its-even-committed/.

[12] Stephen Kinzer, *Chicago Moving to 'Smart' Surveillance Cameras*, THE N.Y. TIMES (Oct. 24, 2014, 10:04 AM), http://www.nytimes.com/2004/09/21/national/21cameras.html.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Louisiana's Port Fourchon Installs Next-Generation Video Surveillance System*, CRESCENT GUARDIAN (Oct. 24, 2014, 11:03 AM), http://www.asmag.com/showpost/13142.aspx.

[18] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

II. THE BEHAVIORAL ANALYTIC TECHNOLOGY

The technology behind behavioral recognition involves computer algorithms and implementations well outside the scope of this work. At its core, however, the system uses traditional CCTV cameras that feed to a central monitoring station.[19] In many cases, human surveillance of the video feed is not required. The computer identifies preprogrammed suspicious "events" and alerts humans to a possible security concern.[20] One company, BRS Labs, leads in this area of technology.[21] BRS has spoken on the confusing nature of interpreting video surveillance and on the need to monitor multiple feeds from a large area with little human staffing.[22] The company touts its product as solving these problems by "using behavioral recognition technology to deliver actionable insights in real-time, so that users know how to apply results intuitively, without analytics training."[23] Its product, AISight, "teaches itself to recognize unexpected patterns within massive volumes of data . . . by alerting users to unusual situations."[24] A named benefit of the technology includes AISight's ability to "[adapt] to changing conditions much like a human brain does, but without fatigue, boredom, or distraction."[25]

III. EVIDENCE DERIVED FROM BEHAVIORAL RECOGNITION

The text of the Fourth Amendment of the U.S. Constitution states,

> The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and persons or things to be seized.[26]

[19] BRS LABS (Dec. 18, 2014, 9:15 AM), http://www.brslabs.com.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] U.S. CONST. amend. IV.

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

The use of behavioral recognition requires courts to interpret constitutional safeguards in light of advancements in technology. The Fourth Amendment requires probable cause for the seizure of a person by a law enforcement officer.[27] The U.S. Supreme Court decision in *Terry v. Ohio* carved out an exception to the probable cause standard.[28] In *Terry*, the petitioner sought relief for the seizure of a concealed weapon on his person obtained through an allegedly illegal search.[29] Petitioner claimed there was no probable cause to arrest the petitioner, and that the "stop and frisk" was a warrantless intrusion.[30] The Court held that an exception to the probable cause requirement exists if there is a reasonable suspicion that an individual has or is about to commit a crime.[31] Since the seizure is based on reasonable suspicion, not probable cause, the "scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[32] The seizure must also serve a legitimate government interest.[33]

While the courts have not specifically addressed the technology of behavioral recognition as it relates to the rights provided in the Fourth Amendment, they have addressed such rights in roughly analogous situations. The use of a computer to flag suspicious events can be compared to a law enforcement officer flagging particular people based on behavior and characteristics that are considered suspicious. One such example of law enforcement using a profile to detect possible criminal behavior is the "drug courier profile," the kind used to identify suspicious individuals from a crowd in *United States v. Sokolow* based on such individual behaviors like buying a ticket with case, checking no luggage, travelling to known drug destinations, and acting nervously.[34] The Court held that the Fourth Amendment[35] does not preclude using "probabilistic" facts describing personal

[27] *Id.*

[28] Terry v. Ohio, 392 U.S. 1 (1968).

[29] *Id.*

[30] *Id.* at 9–10.

[31] *Id.* at 30.

[32] *Id.* at 19 (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967)).

[33] *Id.* at 20–21.

[34] United States v. Sokolow, 490 U.S. 1, 3–14 (1989).

[35] U.S. CONST. amend. IV.

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

characteristics of drug couriers[36] as a basis for a finding of "reasonable suspicion," a standard that justifies a brief detention of the suspected individual.[37]

When considering the tactics used by law enforcement officers in the *Sokolow* case, the similarities with behavioral recognition become more apparent.[38] On July 22, 1984, Andrew Sokolow purchased two round-trip airline tickets for a flight from Honolulu to Miami that was to depart later that day.[39] Sokolow paid cash at the ticket counter from a large wad of money, gave an alias, travelled with a companion using her real name, and neither checked any luggage.[40] The ticket agent noted that Sokolow acted nervously and notified the Honolulu Police Department of Sokolow's ticket purchase.[41] Investigation revealed no person listed under Sokolow's alias, Andrew Kray, in Hawaii and the telephone number provided was that of Sokolow's roommate.[42]

On July 25, 1984, Drug Enforcement Administration ("DEA") agents identified Sokolow during a stopover at the Los Angeles Airport and said he, "appeared to be very nervous and was looking all around the waiting area."[43] When Sokolow arrived in Honolulu with his companion, the DEA continued their surveillance noting that Sokolow was still wearing the same clothes from when he purchased the tickets and neither of the individuals had checked any luggage.[44] When the couple exited the terminal and tried to hail a taxi, four DEA agents moved in to stop Sokolow and requested his airline ticket and identification.[45] At this time Sokolow said he did not have either of the documents, admitted his real name, and that he was travelling under his mother's maiden name of Kray.[46]

The agents escorted the couple to the airport's DEA office where their luggage was sniffed by a narcotics detection canine, which ultimately alerted the

---

[36] *Sokolow*, 490 U.S. at 8 (quoting United States v. Sokolow, 831 F.2d 1413, 1420 (9th Cir. 1987)).

[37] United States v. Sokolow, 831 F.2d 1413, 1585–86 (9th Cir. 1987).

[38] *See generally Sokolow*, 490 U.S. 1 (1989).

[39] *Id.* at 4.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.* at 5.

[44] *Id.*

[45] *Id.*

[46] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

DEA agents to Sokolow's brown shoulder bag.[47] After securing a search warrant, a search of the shoulder bag yielded no illicit drugs, but did uncover suspicious items leading to suspicion of Sokolow's participation in drug trafficking.[48] A more thorough search using the canine alerted agents to a second bag for which the agents did not have a search warrant and, since it was late in the day, the agents allowed Sokolow to leave the airport.[49] After obtaining a search warrant for the second bag, the DEA agents found 1.063 kilograms of cocaine.[50]

The Supreme Court reversed the Ninth Circuit's ruling that the cocaine evidence was inadmissible.[51] The Supreme Court noted the standard of "reasonable suspicion supported by articulable facts that criminal activity 'may be afoot.'"[52] In other words, the Supreme Court upheld the use of the "drug courier profile" the Ninth Circuit had previously rejected. Chief Justice Rehnquist went on to state that the Fourth Amendment requires "some minimum level of justification" for making a stop and the officer must be capable of explaining "more than an inchoate and unparticularized suspicion or 'hunch.'"[53] Reasonable suspicion allows for the brief detention of an individual by law enforcement—called a "Terry stop."[54] However, these "Terry" stops may be justified even when the "proof of wrongdoing" is less than "a preponderance of the evidence"[55] and the court must look at the "totality of the circumstances."[56]

There is a direct relationship between the DEA's "drug courier profile" and the use of a computer algorithm to flag suspicious activity. Both sets of criteria rely on preconceived notions of what criminal behavior may look like, which can lead to problems. For example, the behavioral recognition software may flag an individual for passing through the same area multiple times. This individual's behavior could be a sign of nefarious activity, or that person could simply be lost. Nevertheless, once the event is flagged and an officer is dispatched to the

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.* at 11.

[52] *Id.* at 7.

[53] *Id.*

[54] *See* Terry v. Ohio, 392 U.S. 1 (1968).

[55] *Sokolow*, 290 U.S. at 7 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

[56] *Id.* at 8 (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

individual's location, the officer may briefly detain the individual and ask questions such as, "who are you and what are you doing here?" The officer can encourage answers to these questions that raise the level of evidence to probable cause, which may lead to arrest. In this manner, computer algorithms compile a database of actions and identify certain behaviors as suspicious, putting individuals at risk of police detention as they go about their daily lives. Especially striking is the fact that these algorithmic determinations can occur outside the confines of more high-security environments and without intervention by individuals who can actually bear witness to the putatively suspicious behaviors.

IV. WIDESPREAD NETWORKS OF BEHAVIORAL RECOGNITION AND THE MOSAIC THEORY

As the technology of behavioral recognition becomes more available and capable of covering longer spans of a person's daily route, a concern for the degradation of individual rights grows. The technology is adaptive and capable of learning.[57] While much of the computer algorithm is still undisclosed, it is not a stretch to assume that law enforcement could use a widespread network of CCTV coupled with behavioral recognition to cast a wide net and follow an individual for an entire day, or longer, thus creating a "mosaic" of an individual's movements and behavior over time.

The Fourth Amendment prohibits unreasonable searches and seizures.[58] From an analytical perspective, Fourth Amendment searches require the examination of law enforcement's actions in a sequential manner, where one of the actions must trigger the Fourth Amendment. However, the "mosaic" theory states that searches can be analyzed as a single unit, instead of individualized steps, so that although no single step triggers the Fourth Amendment, the search as a whole can fall under Fourth Amendment protection.[59]

The Supreme Court ruled on the issue of the mosaic theory in *United States v. Jones*.[60] Antoine Jones, a nightclub owner, was suspected of selling cocaine and crack, eventually leading to the discovery of large amounts of drugs and cash.[61] Investigators used wiretaps, pen registers, informants, and camera footage of the

[57] BRS LABS (Oct. 24, 2014, 10:23 AM), http://www.brslabs.com.

[58] U.S. CONST. amend. IV.

[59] United States v. Jones, 132 S. Ct. 945 (2012).

[60] *Id.*

[61] *Id.* at 947–49.

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

entrance to the nightclub to place the suspects under visual surveillance, and, using search warrants, obtained text messages and utilized Jones' cell phone and associated cell tower location to triangulate Jones' location.[62]

However, the investigators used a tactic that brought Jones' Fourth Amendment rights in question. The officers obtained a warrant from a D.C. judge to install a global positioning system ("GPS") device on a Jeep Grand Cherokee belonging to Jones' wife.[63] At the time it was unclear if such a warrant was necessary since D.C. courts had not addressed the issue and other federal courts had already decided that a warrant was not necessary for this tactic.[64] The warrant required installation of the GPS device on the vehicle in D.C. within ten days; however, law enforcement installed the device on the eleventh day, outside of the jurisdiction, in Maryland.[65] This GPS device recorded the location of the vehicle for 28 days and was accurate to location within about 100 feet.[66] The GPS recorded thousands of pages of location data logging Jones' movement to show his colocation with conspirators and the stash house containing drugs and money later seized.[67] At trial, Jones moved to suppress the GPS evidence since the location logger recorded when the vehicle was in his personal garage, and was therefore subject to Fourth Amendment protection against unreasonable searches and seizures.[68] The trial court allowed the use of location data obtained from anywhere outside the home.[69] The court cited *United States v. Knotts*, a similar case that allowed the inclusion of evidence from a radio beeper that alerted police to the suspect's whereabouts.[70] *Knotts* concluded that an individual in a vehicle in public has no reasonable expectation of privacy, as that individual conveyed the details of his or her location to the public at that time.[71]

However, when the Supreme Court granted certiorari, it offered a different view. The Court reasoned that the GPS technology was not only very different, but

---

[62] *Id.* at 947.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.* at 947–49.

[68] *Id.* at 948.

[69] *Id.*

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

[71] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

also more advanced compared to a radio beeper and was thus distinguishable from *Knotts*.[72] The GPS technology was found to be more invasive than other sense-enhancing technology because it could plot an individual's movements over a long period of time and over a large geographic area.[73] The Court agreed with Jones that the use of GPS was an invasive search, because although a person's whereabouts are known to both passersby and police alike when out in public, the collection of location data for 28 days is nearly impossible without the GPS technology.[74] Justice Sotomayor summed up the problem in her concurrence by stating, "GPS monitoring generates 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."[75] Justice Sotomayor also added, "[T]he government can store such records and effectively mine them for information years into the future."[76]

With this in mind, the question arises of whether behavioral recognition technology is analogous to GPS tracking. Certainly, installation of a GPS device requires the physical occupation of a part of the individual's vehicle whereas behavioral recognition technology does not. However, the distinction ends there. Both technologies allow the following of a suspect over a large geographical area, possibly for a long period of time. Using this technology, not only can police monitor an individual's movements within the subway network, but expansion of the system can allow observance of an individual's behavior beyond the subway system. Additionally, since the data may be stored for a long time, or even indefinitely, investigators could go back and reconstruct the individual's movements. The reasons for doing so may not even arise from a crime that has actually occurred. Instead the computer could flag a suspicious event, then, using the algorithm, search for that individual in footage from other locations and other points in time to map movements. Justice Ginsburg hinted at this notion, stating, "For no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life."[77] Thus, a balance must be struck between public safety and intrusions into the daily lives of individuals.

---

[72] *Jones*, 132 S. Ct. at 951–52.

[73] *Id.* at 961.

[74] *Id.*

[75] *Id.* at 955 (citing People v. Weaver, 909 N.E.2d 1195, 1199 (2009)).

[76] *Id.* at 956 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (2010)).

[77] United States v. Maynard, 615 F.3d 544, 558 (2012).

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

V. CURRENT TREND OF THE SUPREME COURT: RECOGNIZING A HIGHER LEVEL OF PERSONAL LIBERTY?

A recent Supreme Court decision concerning the search of cell phones collected at the time of arrest bears similarity to behavioral recognition, and may suggest a trend away from the widespread admission of digital evidence.[78] In *Riley v. California*, evidence obtained from arrested individuals' cell phones led to additional charges.[79] The Court allowed for the physical inspection of cell phones to ensure they were not weapons, but it did not allow searches of digital data on the phone without a warrant, even with a valid arrest.[80]

The interpretation of new cases in light of *Riley* have already entered the judicial system. In *United States v. Guerrero*, the defendant argued for protection of cell-site information based on the privacy concerns stated in *Riley*.[81] The court rejected this argument by distinguishing the search in *Riley*, which was a search of personal data incident to arrest, from the search of Guerrero's cell site information. The court held that a cell phone owner does not have a reasonable expectation of privacy in information held by the third-party service provider.[82] The use of behavioral recognition in a public space seems to be a fusion of these two types of search criteria. It appears, given the decisions of *Riley* and *Jones*, that in instances where a search warrant was necessary, the Court hesitates to allow evidence of all electronic data confirming an individual's whereabouts and life. Behavioral recognition may well fall into these categories with respect to Fourth Amendment protections, requiring warrants for the collection of information.

VI. BEHAVIORAL RECOGNITION AS SENSE-ENHANCING TECHNOLOGY

Use of a computer algorithm to detect suspicious behavior is arguably equivalent to law enforcement reviewing all CCTV camera feeds at once and processing that information. However, the ability to monitor so many feeds over such a wide area with little personnel suggests something much more than "monitoring and processing" and is perhaps best examined by comparing these algorithms to sense-enhancing technology. No one officer or even a small group could possibly process that extent of information in real time. Therefore, behavioral

[78] *See* Riley v. California, 134 S. Ct. 2473 (2014).

[79] *Id.*

[80] *Id.*

[81] *See* United States v. Guerrero, No. 13-50376 (5th Cir. Sept. 11, 2014).

[82] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

recognition technology allows for the enhancement of law enforcement's senses. In *Kyllo v. United States*, a thermal imager identified a drug growing operation within a home after the grow lights heated the home to a temperature higher than neighboring homes.[83] The Court stated, "[W]e think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[84] The Court went on to state, "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[85] The Court in *Kyllo* found a violation of Fourth Amendment rights since the technology peered into the home before issuance of a warrant.

Unlike the sense-enhancing technology used in *Kyllo*, the use of behavioral recognition technology takes place mostly in public in areas that carry a diminished expectation of privacy. *Kyllo* dealt with the use of technology to conduct a search on an individual's home, which carries with it the highest expectation of privacy.[86] Therefore, the *Kyllo* decision is not a direct comparison. However, the Supreme Court hinted at the possibility of a broader interpretation of intrusions upon freedoms through the use of technology, especially if such technology is not in widespread use.[87] The Court noted that technology not in general public use might be problematic in search and seizure cases as the technology quickly advances.[88] At this time, behavioral recognition technology remains unknown to many members of the general population. Few individuals would even suspect the use of such a technology to analyze daily movements. The *Kyllo* decision illustrates the difficulty the legal system has in keeping laws in line with ever-developing technology.

VII. BEHAVIORAL RECOGNITION REGARDED AS AN INFORMANT TO LAW ENFORCEMENT

Behavioral recognition allows law enforcement to collect facts relating to possible crime, thus serving a function similar to that of police informants. In *Florida v. J.L.*, an anonymous call alerted police to a young black male carrying a

[83] Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

[84] *Id.* at 34 (citing Silverman v. United States, 365 U.S. 505, 512 (1961)).

[85] *Id.* at 36.

[86] *Id.*

[87] *Id.*

[88] *Id.*

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

gun.[89] The tip described the bus stop location and the clothes of the suspect, but when police arrived at the bus stop, they did not see a gun or notice any unusual movements.[90] A frisk of the suspect revealed that he did in fact have a firearm in his possession and the Court ruled it an unreasonable search, stating, "[U]nlike a tip from a known informant whose reputation can be assessed and who can be held responsible if her allegations turn out to be fabricated, an anonymous tip alone seldom demonstrates the informant's basis of knowledge or veracity."[91]

If a computer algorithm is considered a tipster to police, questions arise regarding which human party can be considered the informant. Potential answers include the officer working the central monitoring station or possibly the computer programmer of the algorithm used in detection. Either of these parties may be the reliable informant. However, the responsibility of who is to blame for incorrectly flagging suspicious yet benign activity is unclear. If the human source of the underlying reason for flagging a suspicious activity cannot be determined, then the informing algorithm becomes much more anonymous, which diminishes the credibility of the information that compels a search or seizure and can lead to exclusion of certain evidence at trial.

CONCLUSION

The removal of human discretion has both advantages and drawbacks. Certainly, behavioral recognition technology allows for the monitoring of expansive areas with very little human staff involved. The public as a whole may be safer for the installation of this technology. However, this safety comes with the price of our own liberties. Not only is the computer watching the actions of citizens, it makes the determination of what constitutes a behavior worthy of investigation by a law officer. For example, what if a person exited their vehicle and walked away for a legitimate reason, such as saving a runaway dog. Or a tourist unfamiliar with the city passes through the same area multiple times with no nefarious plans. Suppose the behavioral analysis algorithm flags these innocent individuals and the police stop and detain them. Suppose they are searched. It is possible they may have contraband on their person wholly unrelated to the reason for the stop. No human witnessed the original act nor did the human make the determination to stop the individual. Courts may be slow to understand or

[89] Florida v. J.L., 529 U.S. 266, 268 (2000).

[90] *Id.*

[91] *Id.* at 270 (citing Alabama v. White, 496 U.S. 325, 329 (1990)).

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu

transform law in light of this new technology. Therefore, technological advances such as behavioral analytics could create constitutional problems in our society.

The new technology raises important Fourth Amendment issues the courts have yet to address. Preprogrammed computer algorithms used to detect possible crime are analogous to law enforcement's use of the "drug courier profile," which is an accepted law enforcement tactic. Behavioral recognition could increase the number of stop and frisk stops in a region. While use of a computer may decrease the targeting of certain demographics, the deployment of behavioral recognition in poor areas could counter balance this effect. It remains to be seen how the courts will view the technology as possible sense-enhancing technology that is not in widespread use. However, these concerns become less troublesome in public areas with diminished expectations of privacy. The widespread use of the technology in a city could track individuals over large spaces and time. Thus, it becomes simple to record and map a mosaic of a person's life, contacts, habits, and preferences. Law enforcement may later use recorded information to aid in charging an individual. Accountability of who really observes the suspicious event is blurred. The computer programmer, the agent at the monitoring station, or the interdicting officer are all possible "witnesses" to the event. However, none of them may have actually observed the flagged event firsthand.

Behavioral recognition will continue to develop. This will lead to more powerful algorithms, cheaper cost, and more widespread use. The court system can be slow to adapt to and understand new technology. By failing to address these issues, our liberties slowly erode. Proper safeguards can stop this. City councils must think through the implications of smart CCTV systems before deployment. By ignoring individual liberty issues, cities face legal challenges and possible exclusion of evidence from criminal cases. Reaching a balance between personal rights and the safety of our cities can insure the interests of both government and individuals.

Volume XV—Fall 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.159 ● http://tlp.law.pitt.edu