Criminal Law Practitioner

Volume 3 | Issue 4 Article 4

2017

Body Worn Cameras With Facial Recognition Technology: When It Constitutes a Search

Kelly Blount

Body Worn Cameras with Facial Recognition Technology: When It Constitutes a Search

Kelly Blount

Hadi Partovi, a board member at Taser recently told *Bloomberg Business Week* that "Taser wants to be the Tesla or Apple of law enforcement."[1] The switch to a more technology-oriented product base was developed in response to public outcry over a series of deaths resulting from the electrical impulses emitted by the 'taser.'[2] Subsequently, Taser released a camera that switched on when a police officer activated his taser. In creating a record of any interaction where the taser is used, officers are accountable for their actions as well as protected against any accusations of misconduct where fallacious. In addition to the practical consequences of camera technology, Taser has reported that in the first quarter of 2016 the company's revenue was higher for camera and cloud services than for weaponry for the first time ever.[3]

Similarly, after a series of fatal police shootings of unarmed African American men across the United States, the Department of Justice funded a program that subsidized body worn police cameras for police officers. A recent survey found that as of 2014, twenty-five percent of the nation's police officers were already wearing the body cameras.[4] The body cameras were being used in addition to squad car-mounted cameras. The purpose of body cameras is to hold police officers accountable for any acts of misconduct. Similarly, the cameras are meant to protect the officer and in theory should encourage both parties to a police-citizen interaction to behave in accordance with the knowledge they will be held accountable.[5] Though little research exists on the subject to date, some studies have suggested that body worn cameras decrease excessive force by police officers and decrease altercations with citizens.[6]

There have been legal arguments both for and against the widespread use of body cameras, including the effect that they may have on First Amendment rights and personal privacy. However, on the whole, they have been considered a positive development in policing by both police departments and the public.[7] As the technology continues to advance and companies continue to compete for top selling iterations of the product, constitutional issues have begun to emerge. This paper will specifically discuss the development of body cameras equipped with facial recognition

1 Karen Weise, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, Bloomberg Business Week (July 12, 2016).

2 *See id.*

3 *See id.* (noting that the company reported that for cameras and cloud services reached $52 million in bookings for future revenue).

4 *See* Michael D. White, *Police Officer Body-Worn Cameras; Assessing the Evidence,* Washington D.C. Office of Community Oriented Policing Services (2014).

5 *See* Jonathan Young, *Local Law Enforcement Plans for Body Cameras*, Stillwater Gazette (Dec. 16, 2016). In addition to causing fallacious complaints against officers to go down, may also encourage more positive interactions generally. One police officer in Oak Park Heights, Minnesota reported that once a citizen learned the officer had recorded their interaction, he subsequently dropped a complaint against him.

6 *See* Scientific Am., *Cities Want Cops to Wear Cameras, but Technology Could Heighten Distrust if Not Carefully Used,* Scientific Am. (Dec. 1, 2014).

7 *See* Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win For All American Civil Liberties Union* (Mar. 2015).

technology. Facial recognition technology is a frequently used and generally accepted technology; however, the implications of applying it to real-time police work by linking the capability to body worn cameras has sparked debate over possible violations of the Fourth Amendment. Because this combined technology is still in its nascent stages, this paper will suggest various ways in which this technology may be constitutionally permissible, as well as applications that may render its use unconstitutional.

The paper will begin with a brief survey of the technological landscape, namely the company players and their progress in developing this combination of technologies. The discussion will broadly explain the function and process of facial recognition technology and how it may be used in conjunction with body worn cameras. This section will also outline the process by which a facial scan is searched against a database.

Next, the paper will investigate policies that are currently in place regarding the use of body worn cameras as well as scant regulations regarding facial recognition technology. The section will suggest that the lack of stand-alone regulation of these two products leaves a large space for abuse and misuse of the technologies if combined. The paper will argue that lack of regulation at the federal level requires the judicial system to set the standard by which constitutional issues that arise with the use of enhanced law enforcement technology will be evaluated. Further, the generally unregulated nature of the products also de-centralizes the means by which processes are developed and gathered information is maintained. The discussion will suggest that the technology will remain governed by local and state policy, which could result in the application of dispersed legal frameworks.

The third section of the paper will suggest ways in which integrating body worn cameras and facial recognition technology might be used under the auspices of a Fourth Amendment legal search. Because the technology is still being developed, the discussion will address different uses of the technology that may affect its legality or may constitute a search. In recent years, the scope of Fourth Amendment analysis has been slowly transitioning from the physical world to the more technologically networked world. This section will argue that such a product will link the physical and theoretical spaces of property, and significantly complicate the way that courts will rule on these issues in the future. This section then applies several standards which courts may use to evaluate the use of the technology.

Lastly, the paper will make recommendations on the potential benefits and drawbacks of linking facial recognition technology to body worn police cameras. While regulation will likely remain fractured by jurisdiction for the foreseeable future, it is still imperative that the constitutional bounds of the technology are established. Not only will this be necessary in crafting policy surrounding its use, it is also likely to be the subject of future litigation and relevant to countless searches and arrests.

TECHNOLOGY

Paris 1887: Social anthropologist Mr. Alphonse Bertillon developed a facial recognition methodology, the same procedure which constitutes the basis for our current technology, now digitized and automated.[8] Mr. Bertillon catalogued arrested criminals by taking precise measurements of a person's standard features such as ears, nose and mouth, and documenting any distinctive features such as scars and birthmarks.[9] Next, the collected data with the arrestee's name and charges was noted on a card with a photo, giving rise to the mug shot.[10] The cards were often circulated among cities where the person may wander, giving police a veritable, albeit physical, database of locally known criminals.[11] Aside from the mug shot of a falsely accused person who was arrested and booked, there is no evidence to suggest that law enforcement was maintaining a record of persons who committed no crime or ever encountered a police officer. In addition, the mug shots were ostensibly used only after a crime had been committed. Courts in the early twentieth century held that it was a responsible police technique to utilize photographic technologies to prevent recidivism and hasten enforcement capabilities.[12]

Fast forward to the current day, in which we keep digital records of arrested individuals.[13] Today law enforcement relies increasingly more on digital databases that include photographs captured by police surveillance cameras monitoring public places.[14] As will be discussed below, the future of this technology is to combine body-worn cameras with facial recognition capability. It has been reported that at least five police departments in the country have the ability to live-stream[15] footage back to a central server where facial recognition technology is used to identify an individual in real time.[16] As stated above, the traditional use of body-worn cameras thus far has been for accountability, so as to settle accusations of misconduct by police after the fact. Facial recognition technology software will enhance the technology by adding the ability to theoretically identify anyone an officer encounters. This capability creates an active use of records or databases that traditional mug shots did not. In its original iteration, the Bertillon measurements were utilized to catalogue charged suspects after the fact. Facial recognition technology gives police officers the ability

[8] *See* U.S. Nat'l Library of Medicine, https://www.nlm.nih.gov/visibleproofs/galleries/biographies/bertillon.html (last accessed Apr. 30, 2017).

[9] *See id.*

[10] *See* Defense of the Bertillon System, *New York Times*, (Jan. 20, 1896); *Maryland v. King*, 133 S.Ct. 1958 (2013) (holding that DNA samples taken incident to arrest is not a violation of the Fourth Amendment.).

[11] *See* Jennifer Tucker, *How Facial Recognition Technology Came To Be; The FBI's Astonishing New Identification System is the Product of 175 years of Innovation and Paranoia. A Visual History*, The Boston Globe (Nov. 23, 2014). Tucker recounts how during a time that some believed criminals could be typified by his characteristics; this type of profiling allowed each person to be represented by a unique record.

[12] *See Hodgeman v. Olsen*, 86 Wash. 615 (1915); *Shaffer v. United States*, 24 App. D.C. 417, 426 (1904).

[13] Inmate Identification Photographs (Mugshots)," N.Y. State Corrections and Community Supervision Directive. No. 4038 (Feb. 26, 2015), http://www.doccs.ny.gov/Directives/4038.pdf.>.

[14] *See* Clare Garvie, Alvaro M. Bedoya, & Jonathan Frankle, *The Perpetual Line-Up; Unregulated Police Face Recognition in America,* Geo. L. Ctr. on Privacy & Tech. (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[15] This paper uses the term live-stream to describe the temporal aspect of the technology in question. Live-stream refers to the real-time transmission of a video as it occurs, allowing identification to happen while the person may still be in the police officer's vicinity.

[16] *See id.*

to capture the photographic images of anyone that passes the screen of their cameras whether they have been accused of a crime or not. In addition, this feature essentially creates a geographical tagging of a person, essentially creating a record of where that image was taken.

In the wake of numerous instances of fatal and egregious police brutality body-worn cameras have been considered an important method to ensure accountability of police officers and restore public trust in local police.[17] In addition to addressing issues of police misconduct, the cameras also help police departments to address systemic issues within their officer corps.[18] Some civil rights groups though have warned that the ability of police to record interactions with private citizens could also have a myriad of negative consequences.[19] Some of the most touted fears of police body cameras include the threat of a chilling effect that recording may have on First Amendment rights, which could compromise any legitimizing effects.[20] For instance, footage could be leaked to stigmatize the subjects of the video.[21] In fact, in a claimed effort to ensure unconditional accountability, some police departments have already made it policy to publish captured video footage, excepting particularly sensitive footage such as sexual assault.[22]

The concerns of body-worn cameras is further complicated by the potentially imminent combined technology of facial recognition.[23] Several companies, including the giant Taser, are actively developing software capability that will link real time footage collected by body cameras to cloud technologies using data analytics.[24] The importance of this technology cannot be understated. From a legal standpoint capturing and analyzing any person's face may imply that probable cause is no longer necessary for a stop and search to occur.[25] More specifically, if a police officer is able to identify you by use of his body-worn camera, now linked to a facial recognition database just by passing you on the street, it may qualify as a search.[26]

It is important to also note that there are benefits to the technology as well. Proponents of this combined technology claim that facial recognition technology in public places may help locate missing persons or to satisfy a warrant.[27] In 2014, the United States Department of State successfully located a suspect who had disappeared after a warrant was issued for his arrest on charges of child abuse and kidnap-

[17] *See* Jessica Tolliver, et al., *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*, Washington, D.C. Office of Community Oriented Policing Services (2014).

[18] *See id.*

[19] *See* Jay Stanley, *Body Cameras Should Not Be Live-*Streamed, Am. Civil Liberties Union (Jan. 29, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/body-cameras-should-not-be-live-streamed.

[20] *See* Larry Greenemeier, *Police Body Camera Use Not a Pretty Picture*, Scientific Am. (Aug. 4, 2016), https://www.scientificamerican.com/article/police-body-camera-use-not-a-pretty-picture/.

[21] *See* Timothy Williams, *Downside of Police Body Cameras: Your Arrest Hits YouTube,* N.Y. Times (Apr. 26, 2015), https://www.nytimes.com/2015/04/27/us/downside-of-police-body-cameras-your-arrest-hits-youtube.html. Seattle now has its own YouTube channel on which they post all of their body camera feeds (it does blur faces).

[22] *See id.*

[23] *See* Press Release, *Leadership Conference on Civil and Human Rights, Civil Rights, Privacy, and Media Rights Groups Release Principles for Law Enforcement Body Worn Cameras* (May 15, 2015), https://civilrights.org/civil-rights-privacy-and-media-rights-groups-release-principles-for-law-enforcement-body-worn-cameras/.

[24] *See* Matt Stroud, *Taser Plans to Livestream Police Body Camera Footage to the Cloud by 2017*, VICE (July 18, 2016), https://motherboard.vice.com/en_us/article/4xa43g/taser-axon-police-body-camera-livestream.

[25] *See id.*

[26] *See id.*

[27] *See* Garvie, *supra* note 14.

ping.[28] By running a facial scan of the suspect through a database used to detect passport fraud, officials located him living in Nepal under an alias.[29] There are also ways in which the technology may potentially resolve issues that have not yet been widely addressed. Not very long ago, the general guidance to law enforcement officers was to remain in place during an active shooter situation until reinforcements arrived.[30] Today, police protocol in the United States is transitioning toward instructions that dictate arriving officers immediately enter the scene of the shooting and work to mitigate casualties and collateral.[31] Using real-time technologies in such situations may open up the ways in which active shooter or hostage scenarios may be handled. In fact, similar guidance is now also given to first responders and emergency medical personnel, possibly hinting at the future expansion of live feed video technology.[32] Tragedies such as the 2016 shooting at an Orlando nightclub offers an insight into which having a remotely accessible view of the field is critical for effective decision making in real time. Though responding officers wore body cameras, the footage has since been released and it is apparent that the inability of the video to be live-streamed at the time of the shooting was a critical missed opportunity.[33] These types of realizations may lead the technology toward more robust and diverse uses.

The remainder of this paper will focus on the legal implications of advances in body camera technology that employs live stream video footage and advanced facial recognition technology. Because the technology is still being developed, the paper will suggest potential uses and outcomes. For instance, such a capability could mean that anyone passing a police officer equipped with the technology may be scanned, identified, and catalogued in the facial recognition database, even without officer interaction and in the absence of an alleged crime.[34] As many civil liberties groups have maintained, this turns walking down the street into a potential police interaction.[35] In fact, it has recently been found that several cities used body cameras to gather information on Black Lives Matter protestors in order to create a "watch-list."[36] Short of the severe implications of the First Amendment, as in the Black Lives Matter allegations, the ability of law enforcement to image and identify an innocent civilian presents the potential for a Fourth Amendment

[28] *See Long-Time Fugitive Captured: Juggler Was on the Run for 14 Years,* Fed. Bureau of Investigation (Aug. 12, 2014), https://fbi.gov/news/stories/2014/august/long-time-fugitive-neil-stammer-captured/./>.

[29] *See id.*

[30] On September 23, 2016 several speakers, including Paige Schilling of the New Jersey Office of Homeland Security and Preparedness, at the Rutgers Institute for Emergency Preparedness and Homeland Security colloquium entitled, "Homeland Security and Intelligence for the Healthcare and Public Health Sector," spoke on this subject in New Brunswick.

[31] *See* Police Executive Research Forum, Critical Issues in Policing Series: The Police Response to Active Shooter Incidents (Mar. 2014), http://www.policeforum.org/assets/docs/Critical_Issues_Series/the%20police%20response%20to%20active%20shooter%20incidents%202014.pdf.

[32] *See supra* note 30.

[33] *See* Christopher Hayers, David Harris & Gal Tziperman Lotan, *Deputies Release Body Cam Footage From Inside Pulse*, Orlando Sentinel (Nov. 10, 2016), http://www.orlandosentinel.com/news/pulse-orlando-nightclub-shooting/os-pulse-ocso-bodycam-20161110-story.html.

[34] *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2014).

[35] *See* Ava Kofman, *Real-time Face Recognition Threatens to Turn Cops' Body Cameras Into Surveillance Machines*, The Intercept, https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ (last accessed on Apr. 30, 2017).

[36] *See* Associated Press, *5 Black Lives Matter Protesters Claim Bias, Sue Memphis, Graceland*, New Haven Register 3 (Jan. 19, 2017), http://www.nhregister.com/nation-world/article/5-Black-Lives-Matter-protesters-claim-bias-sue-11315533.php.

search. Courts have yet to analyze the constitutionality of this nascent technology, largely because it is not yet widely used, but courts have traditionally grappled with how changing technology affects expectations of privacy under the Constitution.[37]

Modern facial recognition technology is an advanced adaptation of the Bertillon model, and uses facial characteristics such as the eyes, chin, cheekbones and nose to correlate what are termed nodal points on a face.[38] Over time the identifying characteristics constituting nodal points are becoming more complex and numerous. For instance, the New York State Department of Motor Vehicles reported that after increasing the number of facial recognition points used in license imaging from 64 to 128 points, the system has assisted in identifying one hundred persons guilty of identification fraud.[39] Mapping out the face in nodal points, called Principle Components Analysis, or aka "Eigenfaces," is one of the more commonly used methods of facial recognition technology.[40] In this analysis, the component extracts are reduced to finite data points that are then put into a template.[41] This template can then be used to search a database for a matching template or face.[42] There are countless databases that may be utilized for this purpose, including those developed by individual police departments and state motor vehicle departments.[43] In March, 2017, the federal government reported that approximately one half of Americans' facial data are stored in some facial recognition database.[44] The FBI has reportedly run facial recognition searches against sixteen state drivers' license databases, building a biometric network that includes a myriad of non-criminal entries.[45] In addition, police officers may request a search of the Federal Bureau of Investigation's Next Generation Identification database, which as of 2014, by itself contained approximately 400 million facial images.[46] At this time, it is unclear whether a profile or record is created for each searched individual (or created template), regardless of whether a match is found. Such a use could essentially create a footprint cataloging an individual's movements and whereabouts over time based on search records.[47] Policy in this area has been slow to follow the technology. Currently, there is no state with comprehensive regulations on how law enforcement can use facial recognition technology and the data that it compiles.[48] For instance, the Maricopa County Sheriff's Office has entered all the drivers licenses and mug shots of locally registered Honduran persons into its database.[49] Similarly, its been recorded that the Pinellas County Sheriff's Office in Florida runs 8,000 monthly searches of the state's drivers' license database, absent any reasonable suspicion.[50] These frightening an-

[37] *See States v. Knotts*, 460 U.S. 276, 285 (1983) (holding that law enforcement tactics must be able to advance with technology in order to prevent circumvention of the law).

[38] *See* Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 George Mason L. Rev. 15 (2014).

[39] *See* David Kravets, *Enhanced DMV Facial Recognition Technology Helps NY Nab 100 ID Thieves*, Ars Technical (Aug. 31, 2016).

[40] *See* John D. Woodward, Jr., *Biometrics: A Look at Facial Recognition*, Va. State Crime Comm'n & Rand Corp., 8-9 (2003).

[41] *See Id.*

[42] *See Id.*

[43] *See* Garvie, *supra* note 14.

[44] *See* U.S. House of Representatives Committee on Oversight and Government Reform, Committee to Review Law Enforcement's Policies on Facial Recognition Technology, 2 (Mar. 22, 2017), https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/.

[45] *See* Clare Garvie, *supra* note. 14.

[46] *See* Kimberly N. Brown, *supra* note 38 at 188.

[47] *See* Jay Stanley, *supra* note 19.

[48] *See* Clare Garvie, *supra* note 14.

[49] *Id.* at 4.

[50] *Id.* at 4.

ecdotes may be a small glimpse into a larger misuse of public records.

Since 9/11, the desire to create and utilize this technology has been growing and has already played a large role in United States military operations abroad. In 2012, the Department of Homeland Security issued an assessment update on a facial recognition technology being developed as a stand-alone recognition system for federal biometric cataloguing.[51] The stated purpose of the research was categorized as "advantageous technology to develop and implement for national security purposes."[52] The operative functioning component of the technology exists in many places already, such as social media platforms including Facebook and Snapchat, which utilize nodal point recognition to recognize faces.[53] The images that may be found in the databases accessed by law enforcement using this technology also includes images obtained of persons at United States border crossings, i.e. by Customs and Border Protection.[54] Ultimately this assessment found that the use of facial recognition technology for large crowds produces a number of flawed readings and matches, such as in a stadium or Times Square.[55] As will be addressed below, this finding means that in order to capture a "useable" image for the purposes of facial recognition scans, it is necessary to strategically pair camera capability with compatible location. This spatial strategizing may also hold clues as to the constitutionality of capturing and logging identities without cause.

Private companies are developing cameras that will allow police to both transmit live feed video and run it through facial recognition software almost instantaneously.[56] In addition, a survey conducted by Johns Hopkins University has found that at least nine of the 38 companies manufacturing body cameras already have the facial recognition technology available in their cameras.[57] One company has begun to work with local police on a pilot basis of its live stream capabilities.[58] Another company based in Arizona, called Iveda, owns a video surveillance platform aptly titled Sentir.[59] The Sentir platform allows almost any network connected technology, as elementary as a smartphone, to stream live feed video to a number of locations at once.[60] Similarly, Taser International has been publicly heralding its plans to manufacture facial imaging technology for nearly a decade, and has previously announced it will have the ability to live-stream body camera footage to the cloud this year.[61] Numerous companies have advertised their work on this technology

[51] *See* U.S. Dep't of Homeland Security, *Privacy Impact Assessment Update for the Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests*, 2 (Dec.17, 2012).

[52] *Id.*

[53] *See id.* at 3.

[54] *See id.*

[55] *See* U.S. House of Representatives Committee on Oversight and Government Reform, *supra* note 44.

[56] *See* Ava Koffman, *Real-time Face Recognition Threatens to Turn Cops' Body Cameras Into Surveillance Machines*, The Intercept (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/.

[57] *See* Vivian Hung, Jacqueline Coberly, & Steven Babin, *A Market Survey on Body Worn Camera Technologies, Nat'l*, Nat'l Institute of Justice. Doc. No. 250381 (Nov. 2016).

[58] *See* Matt Stroud, *The Company That's Livestreaming Police Body Camera Footage Right Now*, VICE Motherboard (July 27, 2016), https://motherboard.vice.com/en_us/article/9a3ddv/visual-labs-police-body-camera-livestream.

[59] *See* Sentir Cloud Video Surveillance Management Platform, Iveda, https://www.iveda.com/sentir/ (last accessed Mar. 15, 2017).

[60] The term virtually indestructible comes from the Iveda website. The website states that once the video is captured it is immediately transferred to the cloud and the loss/destruction of the camera will not compromise the video content.

[61] *See* Stroud, *supra* note 58.

and will likely hasten the entrance of this product to police departments across the country.[62]

There are also many prohibitive factors to this technology spreading too quickly, including financing, connectivity and transmission speeds, body camera battery life, and data storage capability.[63] For instance, the platform "Evidence.com" which houses and manages footage generated by Taser body cameras currently holds an amount of data reported to be comparable to the whole of Netflix's streaming catalog.[64] Further, footage must be maintained to meet the standards for admissible evidence, which further increases the price and need for sizable data storage.[65] In 2015 San Diego paid roughly $500 per camera to outfit its officers with body-worn cameras, but must pay $1,495 per camera per year to simply house the footage.[66] Similarly, Los Angeles pledged $57.6 million dollars to outfit its 7,000 officers with body cameras; however, due to the prohibitive price, they still had not received the cameras as of 2016.[67]

EXISTING POLICY

Body worn cameras, even without the facial recognition add-on, have dismally low levels of regulation.[68] In a Brennan Center for Justice study, researchers found that Baltimore is the only city police department that has a policy on the biometric search of footage collected by body cameras.[69] The same study found that about half of the departments surveyed have no policy on the ability of police to record First Amendment activity, with a handful prohibiting recording for uses of surveillance or identification.[70] Though the technology is widely used, states are only beginning to require that regulations govern body camera use. Interestingly, some states, such as Minnesota, have legislated that local police departments must develop individual policies, rather than legislate a state-wide policy.[71] Similarly, New Jersey has adopted standards which require that police departments using body cameras have a policy in place, but regard more details beyond foundational state guidelines to be the purview of the department itself.[72] In fact, New Jersey awarded police departments across the state with $2.5 million in grants for the purchase of 5,000

[62] Companies which has also recently publicized their research include Digital Ally, www.digitalallyinc.com,> and WatchGuard, www.watchguard.com; *See also* Weisse, *supra* note 12.

[63] *See* Eric Markowitz, *Police Departments Face A Crucial Question: How To Pay For Body Cameras?,* International Business Times (May 12, 2016), http://www.ibtimes.com/police-departments-face-crucial-question-how-pay-body-cameras-2366968. Markowitz reports that police body cameras can range from $300 to $800 per officer (before storage and streaming). It's indicated that Los Angeles negotiated a contract for cameras for 7,000 officers at a price of $57.6 million over five years. The mayor of Philadelphia has enacted a sugary drink tax to defray costs.

[64] *See* Weise, *supra* note 12.

[65] *See id.*

[66] *See* Eric Markowitz, *supra* note 63.

[67] *See id.*

[68] *See* Greenemeier, *supra* note 20.

[69] Brennan Ctr. Center for Justice. *Privacy and First. Amendment Protections* (July 8, 2016), https://www.brennancenter.org/analysis/police-body-camera-policies-privacy-and-first-amendment-protections. In a study of 23 police departments, Brennan Center used a scorecard of four factors to rate the regulations of body worn cameras. The study also then matched policies against model policies.

[70] *Id.*

[71] Jonathan Young, *Local Law Enforcement Plans For Body Cameras*, Stillwater Gazette (Dec. 16, 2016), https://www.hometownsource.com/stillwater_gazette/news/government/local-law-enforcement-plans-for-body-cameras/article_e42ee484-d2c5-5049-b457-4ddb-1de55884.html.

[72] *See* Directive No. 2015-1 from N.J. Office of Atty Gen. (July 28, 2015).

body worn cameras.[73] This brought the number of departments in New Jersey using cameras up from 50 departments to 200 departments.[74] Ostensibly, one may presume that the result is nearly 200 different sets of departmental policies and protocol on the use of body-worn cameras. Where policies exist, they include the amount of time footage can be held, how it is stored, and protocols to obtain footage for legal purposes.[75] As of the end of 2016, no state had passed a law that places comprehensive limits on the use of facial recognition technology by law enforcement.[76] The piecemeal approach has led to loopholes in policy and a lack of clarity on what police officers may and may not do in regards to facial recognition technology. As the next section will address, this may leave the courts as the final arbiter of setting a Fourth Amendment standard over the use of real time facial recognition searches.

In addition to camera technology, it is also important to have policies in place for the use and maintenance of facial recognition databases. The FBI currently has Memorandums of Agreement with eighteen states on the use of their driver registration databases in order to pursue facial recognition searches.[77] The implications of this type of information sharing arrangement are staggering. While it means that data are being used by entities beyond the original receiver of the information, it also means that non-criminal persons are being searched in connection with potential criminal investigations. The databases held by the FBI are constituted by eighty percent of people with non-criminal records, such as incidentally obtained photos that include work identification photos and drivers license photos.[78] The Georgetown Law Center on Privacy & Technology performed a study of thirty states' drivers license records policies.[79] Its results show that of the 245,273,438 adults in the United States, 117,673,662 adult drivers are in a "law enforcement face recognition network."[80]

Regulation is also necessary to protect the integrity of the data being collected.[81] It has been shown that fingerprints, like any other type of personal, identifiable information can be stolen in electronic hacks.[82] This also applies to facial recognition data.[83] Without the proper regulation of this technology it is easy to imag-

[73] *Attorney General Offers Over Half a Million Dollars in New Grant Funds to Help N.J. Police Dep'ts Buy Body Cameras*, Dep't L. Pub. Safety Off. Att'y Gen. (Sept. 20, 2016), http://www.nj.gov/oag/newsreleases16/pr20160920a.html.

[74] *Id.*

[75] "*Police Body Camera Policies: Privacy and First Amendment Protections*, Brennan Ctr. Just (July 8, 2016.) https://www.brennancenter.org/analysis/police-body-camera-policies-privacy-and-first-amendment-protections. In a study of 23 police departments, Brennan Center used a scorecard of four factors to rate the regulations of body worn cameras. The study also then matched policies against model policies.

[76] Clare Garvie et al., *The Perpetual Line-up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 1, 59 (2016).

[77] U.S. House of Representatives Committee on Oversight and Government Reform. *Committee to Review Law Enforcement's Policies on Facial Recognition Technology*, *Before the H. Comm. on Oversight and Gov't Reform*, 115th Cong. 2 (2017) (statement of Jason Chaffetz, Chairman, United States H. Comm. on Oversight and Gov't Reform).

[78] Adrienne Lafrance, *Who Owns Your Face?*, The Atlantic. (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731/.

[79] Garvie, *supra* note 76 at 3.

[80] *Id.*

[81] *See generally* Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, The Atlantic (Apr. 7, 2016).

[82] *See* Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords*, The Atlantic. (Mar. 24, 2017) https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/.

[83] *Id.* Waddell writes that researchers at the University of North Carolina designed a 3D replica of a person's head by inputting their facial recognizable data into a 3D printer. They reported that the model when animated was so accurate that it tricked "four out of five facial recognition tools they tested."

ine that its decentralized storage and usage protocol may make it vulnerable to hacks and theft by foreign agents, criminal enterprises or individual criminals.[84] In addition to the proprietary nature of facial images, it is important that the technology works accurately. In March of 2017, the U.S. Government Accountability Office stated in testimony before congressional committee that the FBI had not taken previous instruction to improve the accuracy of its facial recognition technology.[85] One unheeded recommendation included the need to ensure that external databases used by the FBI were not including the images of innocent persons.[86] Even more troubling, the facial recognition technology available today consistently finds false positives in its searches and matches of African American persons.[87] In 2012 a study in Florida compared several vendors' software and found that the findings were five to ten percent more likely to fail in searches of African American subjects.[88] Though the National Institute of Standards and Technologies has reported that its regular testing every four years has shown rapid advances, any amount of false positives along the lines of a protected group is a problem with massive implications.[89]

FOURTH AMENDMENT USES AND PROHIBITIONS

Existing case law has consistently held that visual surveillance on its face is not a search per the Fourth Amendment.[90] This line of cases builds on the traditional logic that an object easily observed by the naked eye without a physical intrusion into a person's home does not constitute a search. Taken to its logical end this is appropriate. The alternative would be infeasible, for instance banning police officers from observing their surroundings. This was the standard for some time, following Olmstead v. United States.[91] Therefore, if this standard still applied, live streaming alone via a police body camera may not pose any threat of violating the Fourth Amendment. However, the Court later revisited the issue with the advent of more advanced surveillance technology.[92] In Katz v. United States, the court scrapped Olmstead, holding that the Fourth Amendment does not require that a person's property be invaded upon but that the expectation of privacy is connected to the individual.[93] Therefore, the use of a body worn camera able to live-

[84] *Id.*

[85] *Face Recognition Technology, DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy*, U.S. Gov't Accountability Off. (Mar. 22, 2017), https://www.gao.gov/products/GAO-17-489T.

[86] *Id.*

[87] Garvie, *supra* note 81.

[88] *Id.*

[89] *Id.*

[90] *Florida v. Riley*, 488 U.S. 445 (1989); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (holding that it'd be unreasonable to hold out visual observation as a search, which would "require law enforcement officers to shield their eyes when passing by a home on public thoroughfares").

[91] *Olmstead v. United States,* 277 U.S. 438 (1928) (finding that the wiretapping of a man did not violate the Fourth Amendment because no search and seizure occurred, defining a search to have meant his home was entered; instead the information was collected by the listening ear of a police man) (overturned *by Katz v. United States,* 389 U.S. 347 (1967)).

[92] Robert C. Power, *Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. of Crim. L. and Criminology. 1, 12 (1989.).

[93] *Katz v. United States*, 389 U.S. 347, 352 (1967) (holding that the wire-tapping of a public phone booth used by the petitioner constituted a search under the Fourth Amendment).

stream a person's image without consent or person-to-police interaction may constitute a search under Katz. As will be discussed below, the addition of a facial recognition technology further complicates this analysis.

The Supreme Court has held that a visual search of the exterior of a home is not a violation of the Fourth Amendment protection against privacy. However the use of technology for an external search has been addressed differently.[94] An increase in the use of technology for law enforcement searches has forced judges to discern when technology may change what a visual search looks like in Fourth Amendment analysis. Namely, in 2001 the Supreme Court held that the use of thermal imaging technology constituted a search of a person's home, even when used from the outdoors.[95] The distinction made by the Court hinged on the use of a particular technology by police officers, rather than the information that the technology collected or how it was collected.[96] I will refer to this first approach to a simple visual search as "The Kyllo Test."

In this case police officers suspected defendant Kyllo of growing marijuana in his Oregon home.[97] Police officers used a thermal imaging device to monitor the heat emanating from the exterior of his home, assuming that this may indicate growing lamps for the marijuana plants.[98] The Court held that the thermal imaging information gleaned about a house was a violation of Kyllo's reasonable expectation of privacy.[99] The Court makes clear that this technology did not penetrate the walls or windows of Kyllo's home and was not a search in the traditional sense, however through the use of technology the police were able to learn information about the interior of a protected place.[100] The Court found that because the technology is not in general public use, Kyllo had a reasonable expectation that thermal technology would not be used in monitoring the thermal footprint of his home.[101] Therefore, the Court held that a warrantless use of technology unavailable to the public will likely constitute a search as its unavailability makes it an unexpected intrusion. The holding states that, "the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant."[102] This approach rests on the Fourth Amendment standard posited by Justice Harlan in his famous concurrence in Katz. He found that in order for a Fourth Amendment protection to exist, a person must have an actual expectation of privacy, and that expectation must be reasonable as viewed in terms of contemporaneous societal standards.[103] Certainly a person has the right to privacy when in his home. Kyllo takes this standard another step to the use of technology for gleaning information from a home without physical entry.[104] The Court reaches the conclusion that if a form of technology is not widely available, using that technology to penetrate the walls of a protected place constitutes an

[94] *See also Florida v. Riley*, 488 U.S. 445, 452 (1989) (holding that aerial photographs of a house and surrounding area isn't a search.)
[95] *Kyllo v. United States*, 533 U.S. 27, 35 (2001).
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Kyllo*, 533 U.S. at 31-41.
[103] *See also Bond v. United States*, 529 U.S. 334, 338 (2000) (holding that a person must exhibit an "actual expectation of privacy")").
[104] *Kyllo*, 533 U.S. at 31-41.

unconstitutional search even where entry was never physically established. [105]

Applying the Kyllo Test to streaming live video of a private citizen's face on the street, it is unclear how courts may come down on Fourth Amendment searches. Applying the first requirement of the test, that a person can be easily viewed when on a public street is obvious and it is clear they have no general expectation of privacy. Courts have held that some risk to privacy is assumed when persons subjects themselves to public scrutiny. [106] If courts apply only the first part of the test, the live stream feature of body cameras to facial recognition may not be considered a Fourth Amendment violation. However in using the court's logic in Kyllo, one may argue that the addition of facial recognition technology in real time may constitute a search due to the advanced technology inherent in its use. While passing through an airport may negate the expectation of privacy of identity, when walking down the street the average person does not have the expectation that their identity is being registered in real time. As suggested in Kyllo, the average person does not have access to this technology and therefore would not assume that their neighbors and other passers-by do either. Therefore, as long as the technology remains relatively apart from general consumption, the average citizen may make the argument they have an expectation of privacy in their facial identity.

In looking at the airport caveat to privacy, the concept of public spaces has been generally blurred. If we accept a theory of "private spatialization," in which a location may confer a "sphere" or "zone" of privacy, the next step is to evaluate if and how privacy may exist in public.[107] For instance, if a parking garage has 24-hour surveillance, a person utilizing the garage for parking understands they are being filmed, but they do not expect that the tapes serve any purpose other than the real-time monitoring of potential crime. They may further assume that after a reasonable period the tapes are destroyed if no incident requires their extended retention. However if the tapes are used to monitor and identify an individual who is not committing a crime, it is no longer a legal use of surveillance under the Fourth Amendment. The spatialization of privacy requires that the Fourth Amendment analysis compare the use and context of a search, and properly frame the reasonability of an expectation of privacy in public. Though not explored in this paper, the dichotomy of self-exposure and privacy in online public forums requires a similarly specific analysis.[108] This nuance also applies to facial recognition technology's use in public. The Supreme Court has addressed private spatialization tangentially. The Supreme Court held in 2013 that "the scope of a license – express or implied – is limited not only to a particular area but also to a specific purpose."[109] Though

[105] Ian Hardy, *How Thermal Imaging Tech is About to Become Hot Stuff*, BBC Bus. (Dec. 11, 2015) ("As technology becomes more affordable and subsequently more accessible, courts will be required to look at the Kyllo Rule for the reasonableness of its continuation and make distinctions about how accessible negates an expectation of privacy.").

[106] *See United States v. White*, 401 U.S. 745 (1971) (holding that an undercover informant using a concealed wire did not constitute a search, as the person assumes the risk that his conversant will share the information); *see also California v. Greenwood*, 486 U.S. 35, 40 (1988) (holding that the search of a person's trash once discarded is not a search).

[107] Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. Chi. L. Rev. 181, 190-92 (2008).

[108] *Id.* at 197-98. ("using the analogy of online presence and the ability to expose herself to certain forums, but also expect differing levels of privacy depending on the forum to explain "networked space.").

[109] *Florida v. Jardines*, 133 S. Ct. 1409, 1416 (2013) (holding that a police officer's use of a sniffing canine on the porch of a person's house was a trespass of their

relying on the traditional concept of a search as a physical intrusion, the Court is maintaining that there is a societal expectation that there is a limit to how far a search may be extended. This is illustrated in the parking garage example. Rather than address the physical, Kyllo distinguishes known technology from unknown, or unavailable technology, drawing the veil of privacy at the borders of public awareness and accessibility. The idea that a person may expose herself to public scrutiny, but not to unknown forms of surveillance, is an important distinction. The Court has held that physical features or characteristics that a person knowingly exposes to the public, including facial and vocal features, are not protected under the Fourth Amendment.[110] Therefore, in combining these standards, courts may hold that body-worn cameras are not a search, but that transmitting images for unexpected facial identification is unconstitutional.

Kyllo distinguishes public visual surveillance from the added use of technology. Academics further suggest that a particular public context may govern whether the use of known technology violates a reasonable expectation of privacy. For instance, the use of a legal facial recognition apparatus often relies on what is termed a "face trap."[111] Practitioners and experts of the technology consider a face trap to be the circumvention of a recognized inability of cameras to align with lighting and the angle of a person's face in certain instances. Therefore, by controlling the conditions of the 'face trap' and manipulating the camera, the ability of the camera to capture an accurate image increases.[112] An example of this is surveillance cameras placed at the top of escalators where people are statistically most likely to be looking while riding. By aligning the camera with the escalator's angle and overhead lighting, it is statistically more likely a usable image will be captured. Applying the above contextualization argument of public settings to technology per Kyllo standards, live streaming of images into a facial recognition software may at times constitute a search. It should be noted, the constant advances in technological innovations require that the Kyllo standard be fluid. Public places are increasingly more "wired" with security technology and this causes the argument for an expectation of privacy to fade proportionately.[113]

The Mosaic Theory

In recent years courts have begun to apply the "Mosaic Theory" to Fourth Amendment challenges of technology and surveillance. This section will describe the underlying reasoning behind the Mosaic Theory and apply it to the use of live-stream facial recognition technology in the context of policing. Distinguished from the Kyllo Test, the Mosaic Theory posits that it is not the context and technology of the search, but the aggregation of its findings that may constitute an unconstitutional search. While the use of a body-worn camera itself may be legal, and possibly even the identification feature of facial

property, though external to the dwelling, as it exceed the reasonable expectations of what a search entails).

[110] *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (holding that a person does not have a reasonable expectation of privacy in those physical characteristics that are constantly exposed to the public, such as one's facial characteristics, voice, and handwriting.); *see also United States v. Miller*, 425 U.S. 435 (1976).

[111] Woodward, *supra* note 40, at 14. (describing inadequacies of facial recognition technology such as poor lighting or a face being held at an angle that don't allow for an accurate scan).

[112] *Id.*

[113] Lauren Young, *The Hidden Security Bugs in Architecture That You Never Noticed*, Atlas Obscura (June 24, 2016), https://www.atlasobscura.com/articles/the-hidden-security-bugs-in-architecture-that-you-never-knew-about details (detailing the way in which many public places are built to be advantageous for security and surveillance collection).

recognition technology under the Mosaic Theory, it is the use and storage of the data that creates an illegal search. As previously discussed, if body-worn cameras may transmit images that are searched in real time, the storage of that data is capturing distinct individual movements that aggregate into a broader record of movements. For instance, if a person passes a police officer every Thursday on her way to the doctor, and we are assuming that the officer is scanning her image in a facial recognition database causing a record to be made of each search, there is then too a record of her Thursday trips to the doctor. This type of tracking may constitute a search. Because actual protocol is not available, it is conceivable that if no record is created, and perhaps she is not surveilled in the way the Mosaic Theory posits. This section will ultimately argue that while facial recognition technology as applied to police body-worn cameras even if itself constitutional under the Fourth Amendment, the effect of the data collected may constitute a search under the Mosaic Theory.

The Mosaic Theory was initially posited by the D.C. District Court in U.S. v. Maynard. The Maynard Court held that searches may be analyzed "as a collective sequence of steps rather than as individual steps."[114] This would apply to the accumulation of data, such as making a record of a person's weekly trip to the doctor. The Supreme Court subsequently addressed the issue of aggregate data as a trespass. In Justice Sotomayor's concurrence to Justice Alito's majority opinion in U.S. v. Jones, she coins the aggregation of data a mosaic of data aggregation.[115] The Court's holding in Jones declined to follow an earlier decision that held the use of a radio tracking devices attached to a car was not a search if transmissions were only utilized by police while the car was on public thoroughfares.[116] Instead, Justice Sotomayor argued that the use of a GPS device affixed to Jones' car for the tracking of his movements amounts to a search specifically due to the length of time and sophistication of the data, versus the more remedial technology as was used in Knotts.[117]

Justice Sotomayor further elaborated that the ability of a police officer to observe the movement of a car at any given isolated point is different than the police monitoring where the person travels at all times, potentially in real time.[118] In the lower court, D.C. Circuit Judge Ginsburg held that while a single movement within the period of the car's tracking may be observable to the public, it is unlikely that any individual observing the car in public will observe the entirety of its travels for an extended period, creating a reasonable expectation of privacy in consecutive travels.[119] Therefore, while traveling on public roads is not private information per se, the accumulation of data on an individual gathered by a constant monitor violates the expectation of privacy of that person.[120] The Court went so far as to call the four week tracking of Jones' car as a "dragnet."[121] In dicta, Justice Alito stated that even without the act of trespass, the sum of the data collection may amount to an intrusion on a person's privacy even if the constituent aspects of the search

[114] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 313 (2012) (quoting *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010)).

[115] *United States v. Jones*, 132 S. Ct. 945, 953 (2012) (holding that people have an expectation that their public movements on a street remain private).

[116] *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) (holding that while use of a [GPS] by police was valid when the car was on public roads still made transmissions from within the plaintiff's home a search).

[117] *See United States v. Maynard*, 615 F.3d 544, 568 (D.C. Cir. 2010).

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

[119] *Maynard*, 615 F.3d at 560.

[120] *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (citation omitted).

[121] *Id.* at 412, 409 (citations omitted).

itself do not.[122] Justice Sotomayor's concurrence stated that the accumulation of private information about a person, such as tracking a person for an extended amount of time, will inherently reveal personal and private information such as "familial, political, professional, religious and sexual associations."[123]

In 2014 the Supreme Court seemingly adopted and applied the Mosaic Theory in Riley v. California.[124] Though the theory was not invoked by name, the Court used a similar analysis to come to a conclusion on the aggregation of private data and found that the accumulation determines what will constitute a search. The Court held that the general tenets of the theory apply based on the specific items to be searched incident to an arrest, specifically a cell phone on which large quantities of data are deposited. Justice Roberts stated that police may search a cigarette box in an arrested individual's pocket,[125] however it would be a violation of the Fourth Amendment to search that person's cell phone.[126] The Court's argument rests on the distinction that the amount of private data that a phone may hold about a person will nearly always be incriminating in some way.[127] The opinion states that the "privacies" of a person's life are carried around with him on his cell phone but that makes them no less private or deserving of protection than physical records.[128] Though the Court takes the approach that a case-by-case analysis is necessary when determining whether a cell phone search is proper, it is clear that the Court's approach toward the protection of aggregated material is shifting toward a more mosaic-like understanding. If this approach continues to near the spatialization theory, the Court may bridge the gap from private aspects of the physical world to private nontangible items within the Fourth Amendment context.

Analogizing the data accumulated by facial recognition technology to the use of a GPS device on a car reaches the same conclusion. Though a person may expect to be seen when walking down the street and potentially recognized, his expectation is likely that law enforcement will not identify and record his image. Further, if the technology is applied in this manner, it is wholly unlikely a person expects the cumulative collection of data captured by facial recognition to create a record of his movements. Therefore, courts applying the Mosaic Theory will likely find the use of facial recognition technology of persons in public who are not interacting with the police, to constitute a search.[129] The use of facial recognition technology is further complicated by the fact that under the Mosaic Theory we must distinguish between matters of depth and matters of breadth. The distinction is between large amounts of information on an individual or a small amount of information on many people. With such advanced technology it is feasible that both forms of data collection are

[122] Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in United States v. Jones*, 123 Yale L.J. F. 393, 394 95 (Mar. 24, 2014).
[123] *Jones*, 565 U.S. at 415.
[124] *Riley v. California*, 134 S. Ct. 2473, 2493 94 (2014).
[125] *Id.* at 2483 (citing *United States v. Robinson*, 414 U.S. 218, 234-35 (1973) (distinguishing the Court's holding that the context for a search weighed against the police officer's safety is a case by case analysis and is less compatible with cell phone searches).
[126] *Riley*, 134 S. Ct. at 2493.
[127] *Id.* at 2492.
[128] *Id.* at 2494 95.
[129] *United States v. Skinner*, 690 F.3d 772, 780 (2012) (holding that "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes").

present in this type of surveillance.[130] Scholars have described this phenomenon as an "aggregation effect," which relies on a massive amount of information about a person or persons to piece together a larger and more broad set of information.[131] Though the public understands law enforcement's ability to conduct limited searches under reasonable conditions, the accumulation of personal data that in essence forms a record of a person's movements outside a criminal investigation would be unreasonable by current standards.[132] Despite developing technology, the public trend has been moving toward an expectation that a person's movements over time are private and considered highly personal.[133]

Because facial recognition technology is still in its infancy it is hard to know how exactly a facial scan and search will be obtained, used, stored and handled. In addition and as previously discussed, regulation of this technology is based on scant law and policy, which exists entirely at the state and municipality level. Therefore, it is not known whether a camera will constantly be filming and identifying or whether it will be used for specific persons or searches. Likely this will vary across departments. As argued above, for police officers to actively scan anyone they encounter on the street without reasonable suspicion or initiating a conversation, will likely be held as a violation of privacy under the Fourth Amendment. However under the Mosaic Theory, such a finding requires broad generalizations about the processing of data and assumes that it will be compiled into a record and accessed at will. It is feasible that the proper use and regulation of facial recognition databases may protect the use of live-stream technology against violations of privacy.

The most obvious counterargument to a violation of the Fourth Amendment found under the Mosaic Theory relies on the Third Party Doctrine. The Third Party Doctrine posits that when a third party maintains information as a result of a business transaction, it can keep the information as long as it is private and not used for another purpose.[134] In order to apply this argument to the discussion of facial recognition technologies, we must assume that the databases are managed by third parties and that the public is put on notice that their images are being collected.[135] At this point in the development of pairing live-stream body cameras with facial recognition technology, there is a two-step process. The first step requires that the video be live-streamed to *somewhere*.[136] As of right now, the

[130] *Id.* at 787. Baer posits that there are two types of data collection: one in which a huge amount of data is collected on one person (such as Jones), and the other in which a lesser amount of data is collected on a large number of people; Baer, *supra* note 122, at 396.

[131] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 44 (2004). In this piece Solove compares the finite pieces of data collected by technology to the pointillism style of a Seurat painting contributing to a larger picture.

[132] *See Oliver v. United States*, 466 U.S. 170, 177 78 (1984) (citation omitted) (holding that the limit to searches under the Fourth Amendment must be linked to what society "understand[s]" to be the bounds of its privacy).

[133] Hanni Fakhoury, Hanni and & Jennifer Lynch, *EFF Fights Government's Effort to Get Cell Location Records Without a Warrant*, Elec. Frontier Found Deeplinks (Nov. 18, 2014), https://www.eff.org/deeplinks/2014/11/new-eff-brief-explains-why-cell-phone-location-records-are-private-and-government (citing a Pew Research Center study published in 2014 that stated "82% of Americans consider the details of their physical location over time to be sensitive information more sensitive than their relationship history, religious or political views, or the content of their text messages.").

[134] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009).

[135] *Id.*

[136] Brennan Center for Justice. "*Police Body Camera Policies: Retention and Release*, N.Y. Univ. Sch. of L. (Aug. 3, 2016), https://www.brennancenter.org/analysis/police-body-camera-policies-retention-and-release> (last visited on Apr. 30, 2017).

majority of technologies are developing streaming capabilities to the cloud.[137] Assuming this is the case, the images captured are transmitted in real time to a location that may be maintained by the software company.[138] The second step requires that the image be run through the facial recognition database of choice against existing records for a match.[139] Law enforcement maintains their own databases but also pulls in records from external databases.[140] As discussed above, some databases, such as that maintained by the FBI and state departments of motor vehicles, are external parties that require a request by the police department.[141] Matches in the external database will trigger notification to the police department.[142] It is possible protective measures such as warrant requirements may be implemented to further bolster the constitutionality of this type of information sharing.

For the Third Party Doctrine to apply, this would require that the database of images is not held by the police department and requires formal requests for access to records. Though not yet decided in connection with live-stream, facial recognition searches, there is analogous precedent in the courts. According to a Fifth Circuit Court of Appeals case decided in 2013, the Third Party Doctrine allows for extended record keeping when a third party retains the information for a business purposes and does not share it with other parties.[143] Specifically, the court held that cell phone records retained by the cellular provider are akin to business records, and as such the cell provider is the possessor of the records with the blessing of the cell phone user.[144] Therefore, the court concluded that it was not a violation of the Fourth Amendment for agents to obtain court orders for records under the Stored Communications Act.[145] Though the case was later overturned on procedural grounds, it laid the groundwork for issues of cellular data under the Fourth Amendment, and for applications of the Third Party Doctrine.[146]

The Third Party Doctrine nearly saves the constitutionality of this type of surveillance. However the court goes on to specify that the Third Party Doctrine does not apply when a

[137] Weise, Karen, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, Bloomberg Business Week (July 12, 2016) https://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so.

[138] Also possible that it could be the police department, but as previously stated the expense of maintaining footage is exorbitant

[139] Garvie, *supra* note 76.

[140] *Id.*

[141] Karen Weise, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, Bloomberg Business Week (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so (currently some third parties provide storage platforms, albeit with a hefty price tag. For instance, vendors such as Taser utilize a platform called Evidence.com, to store the information collected by body worn cameras).

[142] This paper does not consider the circumstances by which a warrant would be necessary for these records, and assumes that based on agreements with the database holder and the level of probable cause necessary, it will vary by circumstance. For instance, the *New York Times* reported in "Downside of Police Body Cameras: Your Arrest Hits YouTube," previously cited, that one of the bigger issues with footage retention is the cost and availability of subpoenaed records the ACLU tried to get footage from the Sarasota PD and they claimed it'd cost $18,000 for 84 hours of film

[143] *See In Re: Application of the United States of America for Historical Cell Site Data*, No.724 F.3d 600 at 15 (5th Cir. 2013) (overturned on procedural grounds) (holding that "where a third party collects information in the first instance for its own purposes," the government can later obtain that information for law enforcement purposes if a subpoena or appropriate order is used); *See also Oregon Prescription Drug Monitoring Program v. DEA*, 998 F. Supp. 2d 957 (D. Ore. 2014) (holding that a patient's prescription records are stored by the store, a third party, when held in a database).

[144] *Id.*

[145] *Id.*

[146] Somini Sengupta, *Warrantless Cellphone Tracking is Upheld*, N.Y. Times (Jul. 30, 2013), http://www.nytimes.com/2013/07/31/technology/warrantless-cell-phone-tracking-is-upheld.html.

person is not knowingly giving that information to a third party.[147] Therefore the issue remains as to whether a person may be expected to retain privacy of their face against identification and tracking when in public. The Sixth Circuit has held that when a person is engaged with a business, for instance a financial institution, those records are the property of the bank as a party to the transaction and are obtainable by a third party. (CITE) This is distinguished by a situation such as letter carried by the postman; though the post office has temporary possession of the letter, the contents of the letter only concern the sender and the receiver and the post office is not a party to the transaction.[148] Applying this standard, a court may find that an individual having a conversation with a police officer may be subject to legal facial recognition scanning, whereas a person walking down the street alone and never encountering the officer may have a reasonable expectation of privacy.[149] Courts have not addressed whether an interaction with a police officer makes the expectation of privacy against a facial recognition search constitutional. However, facial recognition technology has already been employed in stationary surveillance cameras in some cities.[150] Applying the logic in Kyllo, if the technology becomes ubiquitous in public places and a person's ability to walk down the street anonymously is no longer a reasonable expectation, it is foreseeable that the Third Party Doctrine could save the constitutionality of the live-stream facial recognition and storage of that information. Another approach may be that used by Moscow's law enforcement, which pairs facial recognition technology with the100,000 public CCTV cameras around the city.[151] However Moscow scans only databases that include criminals and missing persons, unlike the civilian records searched by FBI and local law enforcement in the United States.[152] Obviously, it is hard to know whether additional data is mined for the Russian program, but if it does in fact utilize only criminal databases, it may lessen the impact of such a search and provide a model to replicate.

RECOMMENDATIONS

The practical and important uses of facial recognition technology are obvious. The ability to link an officer's position in a high risk situation with a live feed to a secure location would be an incredible benefit to public and officer safety, such as an active shooter or hostage situations. Further, uses such as the ability to locate missing persons and children will bolster the legitimate use of a constant stream-

147 *In Re: Application of the United States of America for Historical Cell Site Data*, 724 F.3d 600 (2013) (citing *Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978)); distinguished by *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (holding that "when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.").

148 *See United States v. Warshak,* 631 F.3d 266, 288 (6th Cir. 2010) (distinguishing an "intermediary" between a party to the transaction).

149 *See also United States v. Forrester,* 512 F.3d 500, 511 (9th Cir. 2008); *United States v. Phibbs*, 999 F.2d 1053 (6th Cir. 1993) (holding that the manner in which information is obtained by law enforcement informs whether or not it was obtained by illegal search).

150 Karen Weise, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, Bloomberg Business Week, (July 12, 2016), https://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so (this report details the program used by the Los Angeles Police Department as the only department actively using this technology. However, the authors further hint to the use of this technology by undisclosed departments, evidenced by contracts made with certain manufacturers of the technology).

151 *Id.*

152 *Id.*

ing feature. However as discussed above there are multiple hurdles to the constitutional use of this technology. This section will briefly list some recommendations for the proper and legal use of live-stream facial recognition technology paired with police body cameras.

First and foremost, policies need to be in place governing the use of this technology. There is a worrying lack of regulation on the use of body cameras alone, before even adding the ability to live-stream the footage. This must be remedied before the technology is advanced any further. The need to protect citizens' rights is as important as keeping officers safe and accountable, and to allow the technology to exceed its value is extremely dangerous. While it appears unlikely that a uniform structure of regulation will occur nationally, state laws will provide ample notice to police departments on rights of citizens captured by the body-worn cameras. Further, while federal regulation may be unlikely, there is little chance that federal courts will not rule on matters of Fourth Amendment rights as they apply to body cameras. Therefore, courts will need to begin work on a legal standard that can help to create a more uniform set of guidelines as a way to inform state and local policies on developing surveillance technology.

Second, law enforcement and technology providers must come together to determine if live-streamed images will be catalogued, where they will be held, and the proper procedure for accessing the data. Similar to the way in which the FBI has Memorandums of Understanding with state and local partners around the sharing of databases, law enforcement should be transparent about the use of shared databases.[153] In addition, private companies developing this technology may be critical in informing the public as to the capabilities of the technology, as well as the contracts it creates with law enforcement entities. As discussed above, the accumulation of data secured by body-worn cameras may in theory begin to construct a digital footprint of anyone whose image is captured by the cameras. To fully protect rights according to the Mosaic Theory, data must be stored in such a way that law enforcement cannot use or access it to violate privacy. Further, it must be protected against unlicensed disclosure.

Lastly, there must be notice to the public that their images may be captured and identified in public. The notice is a requisite to any security against unconstitutionality conferred by the Third Party Doctrine. Further, notice is a necessary requirement to overcoming the reasonable expectation as set out by Katz. This paper has argued the reasons for each of the above recommendations, and now argues further that each of these recommendations provides extra protection for both law enforcement and the public. Through regulation and third party involvement there is added accountability and security for all parties. Further, the notice given to the public not only protects their rights, but adds additional deterrence against potential criminal acts.

CONCLUSION

As discussed above, law enforcement is relying increasingly more on technology. There are clear benefits and needs for policing to keep up with technological developments and to utilize all the tools available. However as with anything, it is necessary to implement regulations and policy on the use of such powerful tools. This is especially true with the unique capabilities of facial recognition technology.

[153] *Id.*

As argued by this paper, facial recognition technology is a critical component of our law enforcement and security apparatus in the United States. But its use by law enforcement in a real time, public setting may also constitute a search. Because public places are less likely to afford an expectation of privacy, courts must look to the technology itself. In looking to the technology, courts must discern the ways in which collecting any private information requires the storage and continued use by law enforcement. It is likely that collecting such myriad information on individual persons will constitute a record of that person and therefore result in a search.

Lastly, law enforcement has the duty to protect this information once collected. As has been recently disclosed by the United States government, most American citizens can be found in at least one of the numerous databases held by government entities. Even further, most of those entries are compiled with non-criminal records. In the context of a criminal search the use of private citizen's information from sources such as drivers license databases highlights the necessity of protecting non-criminal records against incidental searches without proper protective measures.

About the AUTHOR

Kelly Blount is a New Jersey licensed attorney, focusing on national security and criminal law. As a law student, Ms. Blount was a 2016 Rutgers Homeland Security Fellow and Research Assistant to the Rutgers Institute for Emergency Preparedness and Homeland Security from 2016 to 2017. In this capacity, Ms. Blount served as a researcher on an expert team engaged with the Brussels Police Department to adopt progressive strategies in police-community relations. In addition, Ms. Blount was a student intern for the Department of Homeland Security Immigration and Customs Enforcement, as well as the Department of Justice Executive Office for Immigration Review, in New York City. Prior to law school Ms. Blount served in several public policy offices, including in the role of Constituent Liaison for Immigrant and Foreign Affairs in the United States Senate. Ms. Blount is a graduate of Rutgers University School of Law and holds a Masters Degree in Middle East Studies from the City University of New York.