WHEN GANGS GO VIRAL: USING SOCIAL MEDIA AND SURVEILLANCE CAMERAS TO ENHANCE GANG DATABASES

Megan Behrman*

TABLE OF CONTENTS

I. INTRODUCTION.................................................................315
II. AN OVERVIEW OF SOCIAL MEDIA AND VIDEO SURVEILLANCE MONITORING..............................................316
   A. The Fourth Amendment and Initial Police Examination of Public Surveillance Cameras and Social Media........316
   B. Social Media’s Impact on Gang Investigations..........................320
III. HEIGHTENED SURVEILLANCE: DATA AGGREGATION AND FACIAL RECOGNITION SOFTWARE ................................321
   A. Using Social Media as a Tool To Enhance Gang Databases.................................................................321
   B. The Limitations of Social Media Monitoring ..................325
   C. Incorporating Social Media Monitoring and Database Aggregation with Surveillance Cameras ........327
   D. The Constitutionality of Heightened Surveillance Methods.................................................................328
IV. CONSEQUENCES OF TECHNOLOGY-BASED EVIDENCE IN THE COURTROOM AND ON THE STREETS........333

I. INTRODUCTION

When asked to picture a child watching a video, many people might imagine a child sitting close to the television screen, sipping juice and eating popcorn, enthralled by a film, such as Despicable Me or Frozen. However, children in gang-ridden areas now also tend to watch a different type of video, one in which they play the lead character. Children as young as eight\(^1\) can now view online footage of their own gang initiations, which showcases these children being

* Harvard Law School, J.D. 2015; University of Pennsylvania, B.A. 2012. Many thanks to Professor Alex Whiting for his comments and advice concerning the paper that inspired this Note. Thanks also to my family for their encouragement and support. Finally, thanks to Article Editor Molly Mahan and to the entire staff of the Harvard Journal of Law & Technology for their hard work in bringing this Note to print.

physically beaten by older gang members as part of the “jump-in” process necessary to join the gang.2 Posting such videos online not only provides gang members with an immediate audience composed of their peers and rival gang members,3 but it also has the unintended consequence of offering police and prosecutors valuable evidence they can potentially present at trial.4 Law enforcement can further use information found on social media websites to construct gang databases, chronicling every known and suspected gang member in a community.5 By using such databases, along with public surveillance cameras equipped with facial recognition technology to track gang members, the police can investigate and curb gang-related violence.6 However, the use of such technology, by itself, remains unlikely to stop the spread of gang-induced violence plaguing many American communities, for doing so requires a proactive approach that can prevent children from joining gangs in the first place.7 This Note examines the roles that social media monitoring, surveillance cameras, and electronic databases play in both retroactive responses — those that occur after a crime has been committed and are made in anticipation of trial — and proactive initiatives — those meant to prevent crimes from occurring — toward gang violence. It first addresses privacy concerns relating to a police probe of social media sites and surveillance cameras before focusing more specifically on the ways in which electronic surveillance can impact investigations.

II. AN OVERVIEW OF SOCIAL MEDIA AND VIDEO SURVEILLANCE MONITORING

A. The Fourth Amendment and Initial Police Examination of Public Surveillance Cameras and Social Media

Monitoring gang members’ social media accounts and utilizing public surveillance cameras to identify and track gang members allow

4. Id. at 648.
7. See, e.g., Rebecca Rader Brown, The Gang’s All Here: Evaluating the Need for a National Gang Database, 42 COLUM. J.L. & SOC. PROBS. 293, 311 (2009) (noting that we need a “sustained public effort to protect kids from the lure of gangs”).
law enforcement to investigate gang-related crimes without violating the Fourth Amendment,\textsuperscript{8} which protects citizens against unreasonable invasions of privacy.\textsuperscript{9} Traditionally, this privacy right only applied to physical trespasses by government actors.\textsuperscript{10} Because monitoring a social media profile and observing someone’s movements through the public via surveillance cameras do not require physical trespasses, such methods would not constitute prohibited searches under the original understanding of the Fourth Amendment. The Supreme Court, however, expanded the notion of privacy in \textit{Katz v. United States}, and Justice Harlan in concurrence developed a two-part test, which courts now regularly use to determine whether an action violates the Fourth Amendment:\textsuperscript{11} (1) the person must have exhibited an actual (subjective) expectation of privacy, and (2) that expectation must be reasonable.\textsuperscript{12} Under this broadened conception of privacy, police actions that do not amount to physical trespasses can nonetheless represent prohibited searches under the Fourth Amendment if they invade a person’s reasonable expectation of privacy.

In \textit{Katz}, the Supreme Court held that one who makes a private telephone call from the inside of a telephone booth possesses a reasonable expectation “that the words he utters into the mouthpiece will not be broadcast to the world.”\textsuperscript{13} Similarly, in \textit{Kyllo v. United States}, the Supreme Court held that the government’s use of a thermal-imaging device that was not generally available to the public constituted an impermissible search when the police pointed the device at a suspect’s home.\textsuperscript{14} Yet, even under this broadened scope, one has no reasonable expectation of privacy concerning information one fails to keep hidden but instead knowingly exposes to a third party or to the public.\textsuperscript{15} Additionally, “nothing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[s]...
Indeed, in United States v. Knotts, the Supreme Court noted that technology — in this case, an electronic beeper inside of a suspect’s car — merely enhanced the police’s ability to observe a suspect’s movements along a public roadway. \(^{17}\) The Court held that the technology raised no constitutional issues that visual surveillance would not also raise and upheld the surveillance. \(^{18}\)

The police have long relied on surveillance footage to discover additional evidence. \(^{19}\) In fact, the police have used video surveillance from stores, restaurants, and gas stations to learn more about crimes that cameras have captured on tape. \(^{20}\) Similarly, the police frequently comb through video footage on witnesses’ cell phones and cameras. \(^{21}\) While law enforcement generally obtains this sort of evidence from private individuals or entities, \(^{22}\) surveillance cameras set up by the state that only record people in the public sphere also do not infringe on any Fourth Amendment rights. \(^{23}\) Indeed, “[t]he use of video surveillance in public does not appear to face any constitutional obstacles so long as the devices are not used to peer into areas that have traditionally been considered private,” \(^{24}\) for police observation of a person who knowingly exposes him or herself to the public does not constitute a search. \(^{25}\)

Just as the electronic beeper inside of a moving car in Knotts only provided the police with information an officer could have gleaned from observing the car’s public movements, the surveillance cameras mounted in public locations only document activities that one performs publicly. Similarly, since one’s online friends, Internet service providers, and website hosts can view one’s social media posts, a social media user exposes each post to a third party. Indeed, Facebook founder and CEO, Mark Zuckerberg, asserted that “[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people,” a statement that led some commentators to declare that “[t]he rise of social networking


\(^{17}\) Id.

\(^{18}\) Id. at 285.

\(^{19}\) See, e.g., Janet Reno, Fighting Youth Violence, 11 CRIM. JUST., Summer 1996, at 30, 32-33; Suho, supra note 5, at *5.

\(^{20}\) See Suho, supra note 5, at *5.


\(^{24}\) Hansen, supra note 6, at 47.

\(^{25}\) Bruder, supra note 15, at 1704.
online means that people no longer have an expectation of privacy.”

In addition to sharing their information with innumerable third parties in this manner, many people also make a habit of browsing their social media accounts in public places, such as coffee shops or subways. Unlike the caller in Katz, who enclosed himself in a private telephone booth, people who use social media in public today take little to no steps to shield their phones or computers from their neighbors’ wandering eyes. This behavior allows other people around them to view their profiles and further undermines any expectation of privacy. Thus, despite a user’s subjective belief that information on his or her social media profile is limited or private, by exposing such information to any third party — ranging from a website platform’s host to an onlooker on a train — the user erodes any reasonable expectation of privacy. Therefore, neither government monitoring of surveillance cameras nor government inspection of social media profiles implicates Fourth Amendment concerns, even under the reasonable expectation of privacy standard articulated in Katz.

While the Fourth Amendment does not represent a constitutional bar to using these technologies to develop evidence, in any case involving electronic surveillance the government must consider both the need to protect an individual’s privacy with the necessity and importance of keeping people safe. Indeed, courts often balance a practice’s “intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.” When using technology to prosecute members of a gang, the balance often weighs in favor of surveillance. In 2011, the National Gang Intelligence Center (“NGIC”) reported that gang membership across the United States had increased forty percent, from 1 million members in 2009 to 1.4 million members in 2011. In 2013, the NGIC found that “gang membership and gang-related crime in the United States continue to increase steadily.” The gangs’ continued growth allows them to commit various acts of terror throughout their communities. In 2011, for example, the NGIC attributed forty-eight percent of vio-


lent crimes across the country to gang members and noted that in some jurisdictions, gangs committed ninety percent of violent crimes. The amount of violence has not subsided:

January 2013 open source reporting indicate[d] that the murder rate in Chicago, Illinois, surpassed the number of American forces who died in Afghanistan for the corresponding timeframe. The elevated murder rate in Chicago is reportedly attributed to fractionalized gangs battling for turf control and employing retaliatory violence.

In order to prosecute a gang member successfully, the prosecutor must possess information — information that electronic and social media surveillance can provide. Additionally, this technology-based data is more reliable and precise than eyewitness testimony. Thus, the benefits gained by using surveillance to combat the increasing threat posed by gangs outweigh the costs associated with privacy concerns.

B. Social Media’s Impact on Gang Investigations

One type of surveillance the police can employ during a gang investigation is to monitor a suspect’s social media activity. Not only do current gang members fall within the age group most likely to use social media, but studies have found that they also use the Internet and social media websites “as much, if not more, than their nongang counterparts.” In fact, gang members routinely use social media to highlight their criminal endeavors, to intimidate and threaten rival gangs, and to promote their own gang. Much of the gang activity formerly relegated to the streets, such as spray-painting graffiti and taunting other gangs, now takes place in the virtual landscapes of Fa-

---

32. See NAT’L GANG INTELLIGENCE CENTER, supra note 30, at 15.
33. NAT’L GANG INTELLIGENCE CENTER, supra note 31, at 10.
34. See Shieber, supra note 28, at 1335.
35. See John S. Ganz, It’s Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices, 95 J. CRIM. L. & CRIMINOLOGY 1325, 1327 (2005). Of course, investigators should examine this type of evidence closely to ensure its veracity and should differentiate between posts that portray actual events and those that could be the result of exaggeration or posing.
38. Id. at 472.
39. See O’Connor, supra note 3, at 647 (noting that “gangs are increasingly using social media to accomplish gang objectives and commit crimes.”).
When Gangs Go Viral

When gang members do congregate on the streets to participate in crime, they often record themselves in the act, later posting the videos to their social media accounts. The gang members’ prolific use of technology illustrates the need for law enforcement to examine such technology during an investigation.

The police most often use social media monitoring as a retroactive measure designed to supply prosecutors with evidence to use at trials for crimes that have already been committed. While law enforcement may be able to prevent some imminent crimes from occurring by intercepting social media posts detailing a violent plan, they will not be able to prevent all gang-related crimes simply by monitoring social media websites, especially since many gang members’ websites are dedicated to previously committed (and not upcoming) crimes. In addition, although the Supreme Court recently heard a case involving online threats and freedom of speech, it declined to address related First Amendment concerns; it focused instead on the defendant’s requisite mental state, clarifying only that the mens rea in such a case must be more than negligence. Therefore, due to the uncertainty surrounding the required mental state and the interplay between words written on social media platforms and the First Amendment, it remains difficult for the police to arrest a suspected gang member based solely on his or her online behavior.

III. HEIGHTENED SURVEILLANCE: DATA AGGREGATION AND FACIAL RECOGNITION SOFTWARE

A. Using Social Media as a Tool To Enhance Gang Databases

The police constitutionally can and should use social media monitoring as a way not only to provide prosecutors with evidence of crimes already committed but also to enhance their gang databases, which contain lists of known or suspected gang members, their photographs, and other pertinent details about their lives, such as their nicknames, tattoos, schools, addresses, and known associates. By

41. For example, a gang member in St. Louis claimed: “Someone’s always got a phone recording. Anything you record goes on Facebook or YouTube.” Pyrooz et al., supra note 37, at 490.
42. See id. at *3–4; cf. O’Connor, supra note 3, at 658.
43. See Supra note 5, at *3.
including more tailored information in these databases — information that police and prosecutors learn from monitoring gang members’ social media posts — law enforcement will strengthen its ability to punish and prevent gang violence.

The police possess several methods of obtaining the information displayed on a gang member’s social media page. Much of the evidence found on social media sites is public, so the police can simply look up a suspect’s name to find the data.47 Indeed, people today “are voluntarily surrendering their rights of privacy . . . to satisfy their personal desires for pleasure, closeness, convenience, information, and a sense of belonging.”48 Even when the gang members restrict privacy settings on these social sites, such as limiting content only to their “friends,” they still share the information with online service providers and the social network websites themselves.49 While some sites, such as Twitter, openly oppose disclosing information in response to subpoenas in favor of preserving its users’ anonymity, other social media platforms comply with most police requests and turn over incriminating information.50 The police can also obtain information by looking at a cooperating witness’s account if that witness has access to the social media pages.51 Finally, if the police cannot obtain a subpoena or prefer to monitor a suspect’s profile themselves, they can create undercover profiles.52 Although these undercover profiles violate many social networks’ terms of service,53 the Supreme Court has long acknowledged that “in the detection of many types of crime, the Government is entitled to use decoys and to conceal the identity of its agents.”54 Indeed, in upholding the use of an agent’s undercover online profile, the Eastern District of New York noted that to hold otherwise “would completely eviscerate the government’s ability to conduct undercover operations in which its agents adopt fictitious identities.”55 Thus, just as going undercover in the traditional sense — by assuming a fake identity and infiltrating criminal enterprises in person — represents valid police work, so too does creating an under-

48. Id. at 54.
50. See Zegas, supra note 47, at 56.
53. See, e.g., Zegas, supra note 47, at 55.
cover online profile.\textsuperscript{56} Some officers even go undercover posing as young teenage girls or drug dealers in an attempt to craft a persona that gang members may friend.\textsuperscript{57} Once friended, the police can observe anything the gang member posts on his wall, and “[n]o matter how surprised or dismayed the target of such investigative strategies may be . . . he simply has no Fourth Amendment complaint if those with whom he shared information in confidence decide to violate that trust, whether voluntarily, under force of subpoena, or by threat of contempt.”\textsuperscript{58}

Social media provides a wealth of information about individuals — their pictures, their habits, their favorite sports teams, and their friends. Maintaining and updating a database with this information may prove invaluable to police officers and prosecutors in their investigative efforts.\textsuperscript{59} For example, the police and prosecutors can learn gang members’ motivations for participating in violence by reading their views on social networking sites.\textsuperscript{60} As feelings of jealousy or a purported lack of respect precipitate most gang violence, and since these slights often occur via social media, the police can use social media posts as evidence of motive in individual cases.\textsuperscript{61} Additionally, the police and prosecutors can find critical evidence supporting a suspect’s guilt, such as video of a recent crime\textsuperscript{62} or a recorded rap song sung by the suspect detailing his or her role in the crime,\textsuperscript{63} which prosecutors can use to corroborate witness testimonies.\textsuperscript{64}

Examining social media sites also enables the police to discover which gangs are most popular among prospective members, as well as gangs’ habits and customs.\textsuperscript{65} Many gang members use social media sites simply to demonstrate their involvement and membership in a gang, posting pictures of fellow gang members holding guns, flashing hand signs, and showing off tattoos.\textsuperscript{66} By paying attention to these postings, the police can learn which gangs wear what colors and can determine if a gang endorses shooting people wearing its rivals’ col-

\textsuperscript{56} See, e.g., id. at 55–56.
\textsuperscript{57} See, e.g., id.; Gogolak, supra note 40.
\textsuperscript{58} Gray & Citron, supra note 15, at 138–39.
\textsuperscript{59} See Suho, supra note 5, at *3; see also Goggins, supra note 2, at *4–5.
\textsuperscript{60} See Pyrooz et al., supra note 37, at 492; see also O’Connor, supra note 3, at 648–49.
\textsuperscript{61} Cf. Goggins, supra note 2, at *1 (noting that gang members normally commit crimes “to further the interest of the gang (which they think of as family) or to perhaps prove themselves — one way of gaining rank and respect within the gang”).
\textsuperscript{63} See Gogolak, supra note 40.
\textsuperscript{64} See Goggins, supra note 2, at *4.
\textsuperscript{65} See Pyrooz et al., supra note 37, at 477.
ors. This kind of information can greatly aid prosecutors by showing a gang connection between different individuals and by providing important information the police need to include in a gang database.

For example, police in Cincinnati and researchers at the University of Cincinnati’s Institute of Crime Science created a gang database filled with information gleaned from monitoring suspects’ social media accounts.\(^67\) Thanks to this database, the police possessed evidence that not only highlighted a given member’s participation in certain crimes but also enabled them to link suspects together.\(^68\) As a result of these efforts, in 2008, the Cincinnati police arrested seventy-one people and took down the North Side Taliban gang.\(^69\) Similarly, police in New York used a cooperating witness’s account to examine a defendant’s Facebook posts — posts that detailed “prior acts of violence, threatened new violence to rival gang members, and sought to maintain the loyalties of other alleged members of [his] gang.”\(^70\) By using these posts as evidence for a search warrant,\(^71\) prosecutors ultimately convicted multiple defendants of murder and obtained life sentences against them.\(^72\)

The police can also use intelligence gained from continued social media monitoring proactively in order to prevent specific future crimes from occurring. For example, if an officer notices that members of one gang often insult or threaten members of another via social media, that officer could infer that the insulted gang will attempt to seek revenge.\(^73\) Armed with this knowledge, the police could take steps to ensure that the retaliation does not move beyond words and turn violent. Additionally, including information about previous attacks in a database would provide the police with evidence about how and when each specific gang likes to retaliate. Monitoring gang members’ profiles could also lead the police to determine allegiances between gangs based on pictures and messages between two different groups. Even if gang members attempt to evade detection by speaking in code,\(^74\) prolonged monitoring of these accounts could enable officers to decipher the code and thus uncover information about upcoming crimes. Therefore, the police could use social media intelligence in an attempt to uncover and prevent some imminent crimes.

---

\(^67\) See Kelly, supra note 52.


\(^69\) Kelly, supra note 52; Graham, supra note 68.


\(^71\) Id.


\(^73\) See, e.g., Goggins, supra note 2, at *9.

\(^74\) See Pyrooz et al., supra note 37, at 490.
B. The Limitations of Social Media Monitoring

Although the use of these databases may effectively prevent an imminent gang-related crime from occurring, it is unlikely to halt the systemic violence caused by gangs, for such surveillance on its own cannot stop a root cause of gang violence — children joining gangs. Some police departments use their social media intelligence to illustrate a child’s involvement in a gang to parents, however, this tactic only works once the child is already in a gang. It does not prevent children from enlisting, and once a child joins, it is extremely hard for him or her to leave the gang, even if a parent attempts to extricate the child.

Although many children join gangs because they believe that entering a gang will lead to a lifestyle full of clothes, money, women, and protection, many others suffer from fear and intimidation at the hands of current members who force them to join. Monitoring social media sites is unlikely to protect children who join a gang due to pressure and threats from current members, unless the current members communicate these threats to their targets through social media and the police intervene before the child enlists. In addition, although gang members certainly exploit children’s expectations and fascinations with the gang lifestyle by glorifying that lifestyle online, the police cannot shut down gang members’ social media profiles solely due to their affiliation with a gang, for that would violate the First Amendment’s freedom of speech and freedom of association rights. Even if the police could stop the gangs from advertising online, it is

75. See Goggins, supra note 2, at *4.
77. See, e.g., Brown, supra note 7, at 294; Décary-Hétu & Morselli, supra note 66, at 884.
78. See David S. Rutkowski, A Coercion Defense for the Street Gang Criminal: Plugging the Moral Gap in Existing Law, 10 NOTRE DAME J.L. ETHICS & PUB. POL’Y 137, 155–56 (1996) (detailing the story of an ex-gang member from Los Angeles who initially refused to join a gang but enlisted after several members of the gang who wanted him to join beat him over the course of several days).
79. See, e.g., Décary-Hétu & Morselli, supra note 66, at 884.
80. See O’Connor, supra note 3, at 670 (“It is well settled that a person’s First Amendment right to freedom of speech generally extends to speech conducted on the Internet.”). A person’s First Amendment freedom of association also extends to the Internet, and although “[c]ertain laws prohibit membership in certain groups — these narrow situations generally apply only to groups advocating for the toppling of the U.S. government,” not to gangs. See id.
not clear how much good this prohibition would do.81 After all, some
of the children the gangs recruit are too young to even have their own
social media profiles.82 Instead of targeting specific recruits online,
gangs most often use social media to brag about their crimes and spar
with rival gangs.83 Therefore, the difficulties faced by police in im-
peding the gangs’ online promotions and in identifying children online
who appear at risk of joining a gang encumber law enforcement’s at-
ttempts to use social media monitoring as a tool to prevent the younger
generation from enlisting.

Additionally, once gang members know the police gain intelli-
gence by monitoring their social media posts, they will change their
tactics, a response that makes it hard for the police to use social media
monitoring proactively to prevent another generation of children from
joining gangs.84 Indeed, as police and prosecutors learn more about
how gangs operate, gangs also discover more about how police and
prosecutors try their cases, and the gangs change their ways in re-
response.85 For example, many gang members now report a decreased
online presence.86 They no longer conduct gang-related business
online,87 behavior that at best prevents the police from using social
media to determine the gangs’ happenings and at worst enables the
gangs to provide false intelligence to the police. Many websites dedi-
cated to gangs are now riddled with warnings, such as “WATCH WAT
U SAY FEDS ARE READIN.”88 Other gang members report that they
now password protect their websites,89 that they write important mes-
sages in code,90 and that they remove videos detailing their participa-
tion in crimes from their social media pages.91 Additionally, many
websites devoted to gangs use generic images, making it hard for po-
lice to tie these sites to specific groups.92 Gangs that previously
voiced their opinions about rival gangs online now enlist ally-gangs to

81. Pyrooz et al., supra note 37, at 490. Other studies did find a link between recruitment
and social media; however, these studies focused on gangs’ general presences online and
not a gang’s use of social media to recruit specific children. See O’Connor, supra note 3, at
658.
82. Cf. Peters, supra note 1 (noting that some gang members are eight years old).
83. Pyrooz et al., supra note 37, at 492–93; see also Décary-Hétu & Morselli, supra note
66, at 879.
84. See Spencer, supra note 62, at *6.
85. Id.
86. Pyrooz et al., supra note 37, at 478.
87. Id.
88. Gogolak, supra note 40. This message appeared on TheHoodUp.com, a website that
serves as a virtual hangout space for gang members. Id.
89. Pyrooz et al., supra note 37, at 490.
90. Id. (recounting that an interviewed gang member noted that “we got a baseball game”
written on Facebook actually represents a way to call a gang meeting).
91. Id. (noting that many gang members post fights online “but remove them after a cou-
ple of days to prevent law enforcement from securing the incriminating videos”).
When Gangs Go Viral

327

When Gangs Go Viral

When Gangs Go Viral

retaliate against their enemies, hoping that the police will fail to link their gang to the crime, giving them free rein to strike their rivals.93

Therefore, social media monitoring will only enable the police to develop intelligence for as long as gang members continue to use social media in ways that produce inculpating evidence. However, even though gangs are becoming savvier in their use of social media and have started to refrain from making open admissions of their illicit activities online, these websites are still ripe with data that prosecutors can use in court, despite the gang members’ attempts to communicate in code and quickly remove videos portraying them partaking in criminal activities.94 Because today’s gang members have “been using the internet since they can remember,”95 it is unlikely that they will for- sake it completely to avoid detection. Indeed, the Internet and social media sites play crucial roles in allowing gangs to brag about their exploits and establish credibility in their neighborhoods.96 Despite the fact that gang members are “keenly aware that police are monitoring their online activities,” “[s]omeone’s always got a phone recording, [and] anything [a gang member records] goes on Facebook or YouTube.”97 Although some of the teenagers’ posts and videos last only ephemerally since savvy gang members now remove them within a couple of days,98 the information still passes through the gang members’ pages, and diligent monitoring will enable the police to capture the fleeting information. The police can then aggregate this information and place it in databases, which they can use in conjunction with public surveillance cameras to further combat the spread of gang violence.

C. Incorporating Social Media Monitoring and Database Aggregation with Surveillance Cameras

In addition to aggregating the data found on social media and incorporating it into databases, the police can also lawfully use gang databases to track known gang members through public surveillance cameras equipped with facial recognition software.99 This technology uses an algorithm that matches facial features with pre-identified photographs from a database100 — images the police can gain not only from surveillance cameras and mug shots but also from social media.

94. Pyrooz et al., supra note 37, at 490.
95. Gogolak, supra note 40.
96. See, e.g., Pyrooz et al., supra note 37, at 477–78.
97. Id. at 478, 490.
98. See, e.g., Pyrooz et al., supra note 37, at 490 (noting that gang members remove videos from social media sites after a few days to avoid detection).
99. See Fretty, supra note 6, at 431.
100. Id. at 432–33.
Facial recognition technology is only as useful as its photo database, and by limiting the database to people known to be part of a gang or to people the police have probable cause to suspect belong to a gang, the government would not invade the privacy of every citizen through its use of the cameras. Although the cameras would capture every person in the area on film, they would only recognize and track certain pre-identified suspects in the gang database. Thus, cameras equipped with facial recognition software would treat those excluded from the database the same way traditional surveillance cameras treat people in the public. Therefore, innocent people should not fear that the government might delve into their daily lives and track them in real time through the use of these cameras.

D. The Constitutionality of Heightened Surveillance Methods

As stated above, viewing pictures and information gleaned from social media is constitutional. Likewise, monitoring suspects’ public movements via video cameras is constitutional. This Section argues that combining these technologies to track specific people via cameras equipped with facial recognition software is constitutional as well. Limiting the database to known or suspected gang members would allow the facial recognition software to operate much like CODIS, a computer system that compiles suspects’ DNA profiles into a database that law enforcement uses to match suspects’ DNA to known or suspected perpetrators. As such a system does not represent an unreasonable intrusion into privacy, neither should a system detailing suspects’ movements through surveillance cameras. Indeed, one could argue that the collection of DNA is more personal, because it gathers and categorizes inherently private data, whereas the tracking of one’s movements relies on the aggregation of public knowledge and information.

The fact that police officers use the information found on a suspect’s social media profile to create a gang database and then search that database using facial recognition technology does not violate a suspect’s reasonable expectations of privacy. While the Supreme Court has considered subsequent uses of properly discovered information to determine whether someone ultimately possesses a reasona-

101. Id. at 436–37.
102. See id. at 448.
103. Id.
104. See supra Part II.A.
105. See id.
106. Joh, supra note 93, at 50–53; see also Bruder, supra note 15, at 1721–25.
ble expectation of privacy, the Fourth Amendment does not prevent police officers from using technology to overcome their physical shortcomings. For example, the Supreme Court in *California v. Ciraolo* held that a defendant had no reasonable expectation of privacy against police officers who used a plane flown one thousand feet above the defendant’s backyard to observe his illegal marijuana plants, because “[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.” Conversely, in 2010, the District of Columbia Circuit held in *United States v. Maynard* that a man did possess a reasonable expectation of privacy when the police tracked his movements for four weeks. The accumulation of one’s public actions over a four week period, the court noted, is not actually exposed to the public, since “the likelihood a stranger would observe all those movements is not just remote, it is essentially nil.” However, several other circuits have upheld the use of prolonged surveillance. In *United States v. Pineda-Moreno*, for example, the Ninth Circuit held that the government’s continuous monitoring of a suspect’s car via numerous mobile tracking devices for four months did not constitute a search. Indeed, the defendant in this case did not even argue that the prolonged nature of the surveillance endowed him with a reasonable expectation of privacy over the course of his public movements.

Just as the technology the police used in *Ciraolo* was “routine,” modern technology equipped with the ability to recognize faces and track people is commonplace today. Therefore, like the defendant in *Ciraolo*, who had no reasonable expectation of privacy when the police used modern technology to view his marijuana plants, and unlike the defendant in *Kyllo*, against whom the police used technology

---

111. Id. at 215.
112. 615 F.3d 544, 563 (D.C. Cir. 2010).
113. Id. at 560, 563.
114. See United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007). Although the reasoning invoked in Justice Sotomayor’s and Justice Alito’s concurrences in *United States v. Jones*, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring), id. at 957 (Alito, J., concurring), calls the validity of long-term surveillance into question, the holding of *Jones* rests on the fact that the government physically trespassed on an individual’s property, see id. at 950, which is not at issue insofar as the proposition of this Note is concerned.
115. 591 F.3d at 1217.
116. Id.
118. Id.
not available to the general public, a person whom the police track using a database containing information pulled from social media has no reasonable expectation of privacy. Indeed, given the widespread network created by social media, a stranger today could easily recognize someone on the street based on that person’s social media footprint. Thus, an expectation of privacy — indeed, of anonymity — is unreasonable in the public sphere today.

Given the ubiquity of cameras in the public sphere, the expectation of privacy within it becomes even more untenable. Today, cameras line parking lots, banks, shopping malls, schools, and street intersections. Indeed, it could be that the person viewing the recording from a street camera is a Facebook friend of a friend of a friend who could recognize the person on film. Additionally, Facebook routinely uses a tagging algorithm that can identify individuals and match their names with their photos. Consequently, people should very well be aware that technology is capable of automatically recognizing and matching their faces and names. Just as the defendant in Ciraolo could not expect privacy from low-flying airplanes, people who walk in public today cannot reasonably expect privacy from cameras that can automatically recognize their faces, for modern day, ubiquitous technology can perform the same task.

Unlike the defendant in Maynard, who, as the DC Circuit found in 2010, possessed a reasonable expectation of privacy in his movements over the course of a month, a defendant today would not have the same reasonable expectation of privacy. The rapid development, social acceptance, and pervasive use of technology equipped with the ability to identify specific people and track one’s movements created a stark difference in the world in just a few years’ time. For example, in 2011, only thirty-five percent of adults and fifty-two percent of young adults in the United States owned a smartphone; today, sixty-eight percent of all adults and eighty-six percent of young adults in America own one. In 2010, Pew Research reported that only seven percent “of adults who go online with their mobile phone use a

120. See Fretty, supra note 6, at 441.
123. 476 U.S. at 214.
location-based service," whereas another study by the same organization found that seventy-four percent of smartphone users enabled the GPS feature on their phones just a year and a half later. Therefore, the reasonable expectation of privacy surrounding one’s movements over time that the DC Circuit found in 2010 must now be analyzed in light of society’s embrace of modern technology over the past few years.

In 2012, in United States v. Jones, Justice Alito noted in concurrence that “wireless devices now permit wireless carriers to track and record the location of users . . . [the use of which] will continue to shape the average person’s expectations about the privacy of his or her daily movements.” This statement suggests that the Court realizes that the development and mainstream use of new technologies will continue to impact what people consider to be a reasonable expectation of privacy. Although Justice Sotomayor expressed concern that people may not expect the government to aggregate their public data, even if they willingly share it with third parties, people today should expect to be tracked no matter where they go and for as long as they stay out. Our phones have GPS on them; we use social media to “check-in” to places we enter; public transportation and most intersections have cameras; and many people use smart watches and Fitbits to broadcast their exercise routines, all of which diminish their expectations of privacy regarding the aggregation of daily movements. Today, it is possible not only to watch someone from a camera for an extended period of time but also to observe someone’s past and present movements through their own posts and updates on social media. Therefore, people no longer possess a reasonable ex-

126. Kathryn Zickuhr & Aaron Smith, 4% of Online Americans use Location-Based Services, PEW RESEARCH CENTER (Nov. 4, 2010), http://www.pewinternet.org/2010/11/04/4-of-online-americans-use-location-based-services/ [http://perma.cc/GRP5-7VVP].
129. Id. at 957 (Sotomayor, J., concurring).
130. Gray & Citron, supra note 15, at 139.
131. See Michael Calore, How Foursquare is Forcing Social Networks to Check In or Check Out, WIRED (Mar. 12, 2013, 6:30 AM), http://www.wired.com/2013/03/location-apps-social-media/ [http://perma.cc/T68B-2NUR].
134. See Zegas, supra note 47, at 54–55.
pectation of privacy in their locations, even in the aggregation of their locations over the course of several weeks. Just as the constitutional government monitoring of social media websites and traditional surveillance cameras outweighs the privacy concerns associated with those technologies, the use of facial recognition technology would greatly enhance law enforcement’s capacity to protect the public from the growing threat of gang violence. Some cite the fact that investigators may falsely identify an individual as a gang member and incorrectly include that person in the databases as a reason not to implement such technology. However, while the use of this technology is prone to mistakes and depends on human judgment, all of the information contained in the databases would stem from either public documents or information obtained legally and constitutionally by the police. Such databases thus represent merely an organizational method of culling documents and information that individuals themselves make public. Surveillance cameras not only aid the police and prosecutors in developing evidence but also allow innocent people in the community to feel safer. Since many gangs commit crimes on public streets and playgrounds, the use of cameras could capture these crimes and provide prosecutors with valuable evidence to use retroactively to combat gang violence. Additionally, law enforcement can use facial recognition cameras in a more proactive manner by tracking known and suspected gang members. Tracking a gang member using facial recognition technology will allow the police to learn the suspect’s routine, and thus any deviance from that routine could signal an impending crime. Observing a suspect’s routine could also lead the police to areas a suspect regularly visits, and the police and prosecutors could then further investigate these locations. Furthermore, focusing the cameras on gang members can help the police not only find “hot spots” — locations where

135. Bruder, supra note 15, at 1698; see also Bailey, supra note 46, at 1541–42 (describing Alex, a teenager who is currently listed in a gang database because another boy falsely accused Alex’s friend of being involved in a gang).
136. But see Brown, supra note 7, at 315 (noting that Oregon shut down its gang database in the late 1990s out of concern that it violated people’s civil rights). Regardless, this Article only concerns databases based on information legally obtained from a suspect’s social media account or from public surveillance cameras.
137. See Hansen, supra note 6, at 47 (reporting that people in Baltimore are “overwhelmingly in favor” of public surveillance cameras). People in Chicago also report that they feel safer with the cameras nearby. See Ganz, supra note 35, at 1359.
139. Id. at 431 (explaining the use of facial recognition technology in surveillance cameras).
140. See, e.g., Zegas, supra note 47, at 54–55.
141. See, e.g., United States v. Knotts, 460 U.S. 276, 279 (1983) (upholding the use of GPS surveillance to support probable cause for a warrant to search a cabin the police often observed the defendant visiting).
crime is likely to occur\textsuperscript{142} — but also “hot people” — people who are repeatedly involved in violence, whether as victims or perpetrators.\textsuperscript{143} Therefore, tracking could play a proactive role by helping to alert police when someone in the database may be about to commit a crime.

\textbf{IV. CONSEQUENCES OF TECHNOLOGY-BASED EVIDENCE IN THE COURTROOM AND ON THE STREETS}

While precedent suggests that it is constitutional to use facial recognition technology to track known gang members, and while this enhanced surveillance may proactively aid the police in preventing some imminent crimes, this technology eventually will likely come to serve only a retroactive purpose — allowing the police to hone in on suspects when viewing previously recorded footage, rather than track people in real time in an attempt to prevent children from joining gangs or preemptively thwart crimes. Just as gang members have reacted to police and prosecutors following their social media websites, they will inevitably change their tactics in response to law enforcement’s use of surveillance cameras and facial recognition technology to track their movements.\textsuperscript{144} They may, for example, begin to commit more crimes in secluded areas without cameras in order to avoid detection. Or they will don different disguises each time they go outside in an attempt to evade identification. Hence, as gangs alter their behaviors based on police procedures designed to combat criminals, the police too will need to reevaluate their strategies for proactively reducing gang violence.\textsuperscript{145}

Using surveillance cameras, though constitutional, may also inadvertently cause more violence. For example, facial recognition cameras may contribute to gangs’ growth. Electronic monitoring could encourage gang members to remain in the gang longer than they otherwise would have, as gang members who know the police are tracking them possess less incentive to quit, since their crimes remain on camera and their faces appear in a database in perpetuity.\textsuperscript{146} Children and teenagers who have not joined a gang, but who live under a system of surveillance, may feel that the benefits of joining a gang outweigh the risks, since the police follow them remotely anyway\textsuperscript{147} and offer little proactive protection. Indeed, if surveillance cameras can

\textsuperscript{142} Spencer, \textit{supra} note 62, at *3.
\textsuperscript{144} \textit{See} Spencer, \textit{supra} note 62, at *6.
\textsuperscript{145} \textit{See} Suho, \textit{supra} note 5, at *10 (noting that law enforcement, once again, must play catch up with the gangs).
\textsuperscript{146} Brown, \textit{supra} note 7, at 324.
\textsuperscript{147} \textit{Id.}
play any sort of proactive role in the fight against systemic gang violence, police officers must monitor them in real time, an assignment that pulls them from the streets, where their presence could provide a better sense of security. 148 People who are not part of the gang but who associate with gang members may be swept unfairly into the database and grow to resent law enforcement if they learn of their suspected gang member status. 149 However, research shows that even innocent people who were friends or even friends of friends of homicide victims from gang violence were one hundred times more likely to be involved in a future homicide than people who were not. 150 Thus, even if an innocent person is swept into the database and classified as a suspected gang member based on his or her innocent connection to a gang member, that person still possesses a statistically heightened risk of being involved in a homicide, whether as the victim or the perpetrator. Consequently, tracking known or suspected gang members could still help curb — or at least predict — violence.

A readily available database also could lead to investigative biases if the police begin to focus on people already listed in the database, neglect other viable suspects, and build their cases to match those suspects in the database instead of using the database to find a person who matches a suspected profile. 151 When making generalizations about a suspect, there is always a risk of investigative bias. However, the risk becomes amplified when police rely on computer programs, since such programs can speak in absolutes and since people give great weight to information found on computers. Meredith Broussard’s article, When Cops Check Facebook, details the story of Jelani Henry, a likely innocent teenager who was arrested and charged with a double shooting after his name appeared in a database due to his Facebook activity and his older brother’s gang involvement. 152 She notes that because databases are based on binary logic, human judgment is often essential to prevent mistakes. 153 Police officers will thus need to be aware of and actively avoid letting any bias enter their investigations. To combat this risk when investigating a crime, perhaps police and prosecutors should use the database to find a clearly identifiable suspect, to determine a motive, or to look for other inculpating infor-

148. See Suho, supra note 5, at *3.
149. See Chasin, supra note 49, at 37.
150. See Buntin, supra note 143. This study focuses on gangs in Chicago.
153. Id.
mation once other evidence links a suspect to a crime. By emphasizing the need to look at each case individually and not to rely solely on a database to determine a suspect’s guilt, police training would help combat the risks of bias.

Some argue that, in addition to allowing gangs to expand their membership or prejudicing law enforcement against certain known offenders, the use of gang databases may give gang members more power over their communities. Innocent people who feel strongly about their privacy may forego legitimate activities. They may choose to stay indoors, leaving the streets free for gangs to control, despite the surveillance cameras’ looming presence. In Watching Me: The War on Crime, Privacy, and the State, Kimberly D. Bailey claims that implementing surveillance cameras will discourage young African American and Latino males from spending time outside. She argues that the children’s hesitance to spend time outdoors “limits their mobility and the creation of their life plans,” prevents their ability to “create robust social capital and to be part of mainstream political discourse,” and even deprives them of “self-identity and expression,” since they will refrain from wearing clothes that may cause the police to suspect gang involvement. Certainly, everyone should be able to enjoy the outdoors. However, children and young adults already have lost this basic right in areas riddled by gang violence. After all, it is not as though the people in these communities are not already watched; they are being watched by the gangs, as evidenced by the plethora of crimes committed against innocent people and by the gangs’ relentless recruitment of young children. In these infested areas, seven-year-olds are murdered while sitting in a car with their mothers, nine-year-olds are killed for screaming when they see a gang member holding a gun in the middle of the street, and six-month-olds are shot five times in a drive-by while their fathers change their diapers. Contrary to Bailey’s opinion, surveillance

154. See, e.g., Bailey, supra note 46, at 1543–44.
155. See Fretty, supra note 6, at 438–39. But see supra note 137 and accompanying text (noting that people in Chicago and Baltimore generally favor public surveillance cameras).
156. Bailey, supra note 46, at 1570.
157. Id.
techniques might ensure that people with the communities’ best interests at heart are also watching the citizens and could actually free people to enjoy their communities once again.

Little evidence exists “that citizens subjected to invasive surveillance inevitably withdraw from democratic engagement,” as many people either speak out against what they view as improper police tactics or ignore the technology because they feel they have nothing to hide. 162 Bailey asserts that in the absence of “oppressive surveillance” by the police, residents will develop “strong friendships and networks within the community.” 163 However, the fact that communities lacking police support represent the perfect breeding ground for gangs directly contradicts this statement. 164 Bailey also claims that when the state respects people’s privacy, “it sends the implicit message that the individual is ‘worthy’ of and can be trusted with engaging in essential traits of personhood.” 165 These interests are not mutually exclusive, however, and discouraging the police from investigating violent crimes by using technological surveillance seems unlikely to help any community experiencing frequent murders and shootings. Indeed, using every available technology and resource to focus on people in communities plagued by gang violence could lead them to feel that they, too, possess essential traits of personhood, namely, the right to have police protection. In framing her argument in terms of the public versus the police, Bailey obscures the fact that the government must balance an individual’s right to privacy with protecting the community.

An integral part of this protection stems from ensuring the well-being of the future generation. While prosecutors successfully prosecute and imprison many gang members, gangs continue to recruit, and “what’s lacking is a sustained public effort to protect kids from the lure of gangs.” 166 When applied in isolation, this technology is best used retroactively at trials.

However, when combined with police officers who walk the streets, this technology would have a profound impact, even proactively. Stationing officers near areas the database flags as “hot” can

162. Gray & Citron, supra note 15, at 79; see also Berman, supra note 132.
163. Bailey, supra note 46, at 1555.
164. See, e.g., Gangs Infiltrating Pa. Mountains Region to Avoid Police, ASSOCIATED PRESS, (Aug. 7, 2006), http://www.policelone.com/gangs/articles/508948-Gangs-infiltrating-Pa-mountains-region-to-avoid-police/ [http://perma.cc/M77V-JM96] (“Gang members know that gated communities are not patrolled by state troopers or municipal police.”). Stephen Washington, the chief of staff to former Pennsylvania State Representative John Siptroth, has stated that “the limited police presence has made some private communities ‘almost safe havens for gangs.’” Id.
165. Bailey, supra note 46, at 1553.
166. Brown, supra note 7, at 311; see also Buntin, supra note 143 (“[G]angs don’t necessarily know why, generation after generation, they shoot one another.”).
deter gang members from congregating there and committing violence more than a video camera can by itself. Officers’ presence near hot people and hot spots would increase the likelihood that law enforcement could thwart recruitment. In addition to patrolling hot spots, police officers and prosecutors can visit the individuals identified, informing them of the charges they could bring, notifying their families of the person’s potential gang involvement, and making a concerted effort to keep these individuals out of harm’s way.\textsuperscript{167} Studies have shown that such police tactics and programs reduce the spread of violence.\textsuperscript{168} The opposite may hold true as well: for example, after police presence in Baltimore was reduced in the aftermath of Freddie Gray’s death, gangs became oversupplied with illegal drugs and “murders [rose] to levels not seen in four decades” in parts of the city.\textsuperscript{169}

Police officers on the streets can also counter any negative assumptions people hold concerning the video cameras. Police officers could explain to people who live and work near the cameras the purpose of the cameras, how facial recognition technology works, and who they are tracking, alleviating any fears innocent citizens might have concerning government surveillance. Additionally, although informing members of the community about the cameras’ purpose may enable gang members to learn about the police’s interest in them and perhaps cause the suspects to attempt actively to avoid detection, having gang members know the police monitor them — both remotely through surveillance cameras and in person — actually could serve as a deterrent. For example, in the 1990s, a Boston-based task force employed a targeted approach to gang violence in which members of the coalition “personally met with gang members relaying to them that they were under the microscope because of their violent behavior.”\textsuperscript{170} After such a meeting, “law enforcement officials, probation officers, and Department of Youth Services (DYS) caseworkers, flooded the specific gang’s turf to openly show their lingering presence within the

\textsuperscript{167} Cf. Matthew J. Cannata, Achieving Peace in the Streets: How Legislative Efforts Fail in Combating Gang Violence in Comparison to Successful Local Community-Based Initiatives, 35 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 243, 248–51 (2009) (describing the success of Boston’s Ten Point Coalition and its Ceasefire program, a partnership task force which included members from law enforcement, probation officers, Department of Youth Services, the Boston Police Department, and prosecutors).

\textsuperscript{168} See id. at 253; see also Reno, supra note 19, at 33 ("[T]he work of a good community police officer can go far beyond the gun and the badge. They can save young lives . . . by mobilizing neighborhoods, schools, churches, synagogues, and community organizations to strengthen efforts to keep kids in school and out of trouble with the law.").


\textsuperscript{170} Cannata, supra note 167, at 249–50 (internal citations omitted).
gang’s neighborhood.\textsuperscript{171} The fact that the gang members knew they were being closely monitored helped curb the gang-related violence in Boston, with the homicide rate of youths dropping almost in half just in the program’s first year.\textsuperscript{172} Currently, many people who live in gang-ridden communities do not seek police protection, and ironically, their children often turn to gang members for protection instead.\textsuperscript{173} Infusing these areas with a police presence could enable people, and especially children, to develop positive relationships with police officers and to turn to the police — instead of the gangs — when they need help.\textsuperscript{174} Despite the technologies’ limitations complicating their use as proactive measures to address gang violence when used in isolation, incorporating social media monitoring, surveillance cameras equipped with facial recognition software, and electronic databases with officers stationed in person near suspect areas represents a proactive step in stopping gang recruitment and, eventually, gang violence.

Law enforcement’s responsible use of these technologies, coupled with its ability to develop meaningful relationships with citizens, could galvanize people to regain control over their neighborhoods and, consequently, their lives. With the successful implementation of these strategies, children once again could play joyfully in the city streets, no longer afraid that, by being outdoors, they might fall prey to a gang member’s seductive wiles, or, worse, wind up dead from a spray of bullets intended for a local teenager wearing the wrong color shirt.

\textsuperscript{171} Id.
\textsuperscript{172} Id. ("From 1991 to 1995, the average youth homicide rate was forty-four youths per year. By 1996, a year after the implementation of Operation Ceasefire, the homicide rate dropped to twenty-six youths murdered per year."). This downward trend continued in 1997, 1998, and 1999, leading commentators partially to credit the task force with “the Boston Miracle.” Id.
\textsuperscript{173} See Rutkowski, supra note 78, at 152.
\textsuperscript{174} See Reno, supra note 19, at 33; see also Goggins, supra note 2, at *4.