Oklahoma Law Review

Volume 71 | Number 4

2019

Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media

Rachel Levinson-Waldman

OKLAHOMA
LAW REVIEW

VOLUME 71 SUMMER 2019 NUMBER 4

PRIVATE EYES, THEY'RE WATCHING YOU: LAW ENFORCEMENT'S MONITORING OF SOCIAL MEDIA

RACHEL LEVINSON-WALDMAN*

I. Introduction

Social media is a powerful tool that gives people the chance to connect and interact with others from all over the world. Users on platforms like Facebook, Twitter, and Instagram can easily chat or share videos and pictures with friends and connections in their city or across the world. On most social media sites, all that is generally required to connect and interact with another user is becoming "friends" with, or a "follower" of, that user. Many social media profiles are public, allowing anyone else on that platform to view postings, pictures, or videos.

While most social media sites provide privacy settings to protect profiles so only friends or followers can see them, many people still have at least one social media account where they are "friends" with someone else who may not be a direct friend—or someone with whom they did not intentionally choose to connect. Indeed, social media users are frequently bombarded with "friend requests" from strangers or remote acquaintances, and they may sometimes find it easier to accept the request than spend time determining whether or how they know the person.

* Senior Counsel, Liberty and National Security Program, Brennan Center for Justice. Henry Lecture Series, October 15, 2018. The staff of the law review drafted this piece based on my lecture, and I provided revisions. I am grateful to: the University of Oklahoma Law Review and its entire staff, in particular Michael Waters and Collen Steffen; Dean Joseph Harroz of the University of Oklahoma Law School; Stacey Reynolds, Director of Continuing Legal Education and Events; and Judge Robert Henry, to whom I am indebted for his professional and personal generosity of many years.

As a result, many social media profiles may be observed by unwanted viewers, including law enforcement. In fact, social media accounts are now being monitored and surveilled by state and local law enforcement agencies across the country. In this essay, I will discuss what police monitoring of social media means, how police carry out this surveillance, and how social media monitoring and surveillance can disproportionately affect—and be disproportionately used against—activists, communities of color, and youth of color.

II. Background

A. Statistics on Police Use and Costs of Social Media Monitoring

The International Association of Chiefs of Police (IACP) conducts an annual study in which it sends out a questionnaire to police departments asking whether they use social media and for what purpose. In 2015, over 96% of the 553 departments responding reported that they used social media in some capacity.[1] Of the 539 departments responding to the 2016 questionnaire, social media was used by 76% for soliciting tips on crime, by 72% for "monitoring public sentiment," and by 70% of the departments for intelligence gathering.[2] Given these statistics, police are using social media not only to send information out to the public but also to keep track of what people are doing both online and off.

While police social media monitoring is prevalent, individual police departments vary in their use of social media monitoring and in how much they expend on their monitoring capabilities. Until the fall of 2016—when the major social platforms changed their developer policies to prohibit the practice—many departments bought programs from third-party software developers that enabled police to mine the data available on platforms, including the details of social networks, who was using high-profile hashtags, location information, and more. The Brennan Center conducted a study in 2016, based primarily on publicly available procurement documents; based on those findings, we mapped out departments across the country that were spending at least $10,000 on this technology.[3]

---

1. *2015 Social Media Survey Results*, INT'L ASS'N OF CHIEFS OF POLICE (2015), http://www.iacpsocialmedia.org/wp-content/uploads/2017/01/FULL-2015-Social-Media-Survey-Results.compressed.pdf.

2. KiDeuk Kim, Ashlin Oglesby-Neal & Edward Mohr, *2016 Law Enforcement Use of Social Media Survey*, JUSTICE POL'Y CTR (Feb. 2017), https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf.

3. *Map: Social Media Monitoring by Police Departments, Cities, and Counties*,

For example, in Oklahoma, the city of Tulsa spent $3,500 in 2014, the city of Moore spent $13,387 from 2015 to 2016, and the Oklahoma State Bureau of Investigations spent about $35,250 over that same period.[4] Larger jurisdictions spent much more: for instance, the County of Los Angeles spent nearly $200,000 on these technologies.[5]

At the same time, law enforcement agencies are relatively silent about their use of social media monitoring tools. Only eighteen out of the 157 jurisdictions we surveyed—roughly 10%—have publicly available policies explaining how they use social media monitoring to view or gather data,[6] so many civilians are left in the dark about how their police departments are collecting social media information.

B. How Police Use Social Media Information

There are four basic methods that police departments have historically been able to employ to gain information through social media surveillance. First, police search a user's publicly available social media accounts and posts. For example, if a targeted user has a public Twitter account, police can go on the site to check the user's recent posts and interactions with other users without needing any special third-party software. Nearly all police departments that responded to the IACP annual study confirmed that they use this basic tactic in some form.

Second, police departments may set up an undercover account to monitor or interact with a targeted user. This tactic comes into play when the user has more stringent privacy settings on his or her account, such that posts and pictures are not visible without their permission. As long as the user accepts the friend or follow request—perhaps because the undercover

---

BRENNAN CTR. FOR JUST. (Nov. 16, 2016), https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties [hereinafter *Map: Social Media Monitoring*].

4. *Purchase Order No. 0000131991 for Snap Trends*, CITY OF TULSA (Sept. 30, 2014), https://www.brennancenter.org/sites/default/files/analysis/POs%20_%20GovSpend_Tulsa.pdf; *Purchase Order No. 16-41210 for Snap Trends*, CITY OF MOORE (July 28, 2015), https://www.brennancenter.org/sites/default/files/analysis/POs%20_%20GovSpend_Moore2.pdf; *Purchase Order No. 170889 for Snap Trends*, CITY OF MOORE (Aug. 17, 2016), https://www.brennancenter.org/sites/default/files/analysis/POs%20_%20GovSpend_Moore3.pdf; *Purchase Order No. 15-38940 for Snap Trends*, CITY OF MOORE (Apr. 6, 2015), https://www.brennancenter.org/sites/default/files/analysis/POs%20_%20GovSpend_Moore1.pdf; *Map: Social Media Monitoring*, *supra* note 3, at Oklahoma State Bureau of Investigation.

5. *Map: Social Media Monitoring*, *supra* note 3, at County of Los Angeles.

6. *Map: Social Media Monitoring*, *supra* note 3.

account has a compelling profile picture or features interesting posts—the police can then use that account to glean otherwise private information about the targeted user, as well as to view comments from the users' friends and contacts. About two-thirds of police departments surveyed use this method. Note that this would not include the capability to view private messages exchanged through a service like Facebook Messenger or Twitter direct messaging, unless the undercover officer is a party to the messages.

Third, as discussed *infra*, law enforcement offices could until recently purchase and utilize analytical software to conduct much more sophisticated tracking of people, groups, or hashtags.

Finally, police departments can use a search warrant to get information about a specific user, including private messages between two users.

Police can also use social media monitoring to ascertain the location of users—sometimes even if the user has disabled location tracking on her account. Location information may be available through Wi-Fi and cellular data, GPS information, geotagging, network analysis and hashtags, keywords, or other content.

III. The Exposé of Social Media Monitoring and Subsequent Ban on Data Gathering for Surveillance Purposes

One way police departments are utilizing social media is to monitor hashtags, which are frequently used to talk about socially and politically relevant issues. One of the most prominent hashtags is #BlackLivesMatter, which in a space of several years has been used more than 30 million times on Twitter.[7] Indeed, social media has been a critical avenue for political engagement by communities of color; a recent Pew Research Center study found that half of black and Hispanic users identify social media sites as important venues to express political views, while only 32% of white users agreed.[8] In a similar vein, 36% of black users and 27% of Hispanic users said social media is very important for getting elected officials to pay attention to issues, compared to 19% of white users.[9] As the Pew study indicated, a majority of Americans overall agreed that social media can

7. Monica Anderson et al., *Activism in the Social Media Age*, PEW RES. CTR.: INFO. & TECH., at 3, (July 11, 2018), http://www.pewinternet.org/2018/07/11/activism-in-the-social-media-age/.

8. *Id.* at 2.

9. *Id.*

"help give a voice to underrepresented groups" and "make it easier to hold powerful people accountable."[10]

The Pew Research study makes materials unearthed by the ACLU of Northern California (ACLU) especially relevant. The ACLU was interested in how companies were advertising their social media monitoring services to police departments as a way to get insight into how police were using those technologies. The ACLU sent sixty-three requests to police departments throughout California and discovered that providers were marketing their products as a way to monitor lawful protestors. [11]

A company called Geofeedia, for instance, emailed prosecutors and police departments to boast that it could create undercover accounts and follow hashtags to track lawful protests like those in Ferguson, Missouri.[12] The company also noted that it could create an unlimited number of fake accounts to monitor private users.[13] This is in violation of Facebook's terms of service, which requires users to use more or less their real name, to represent themselves truthfully, and to hold only one account.[14]

In a separate follow-up e-mail to a district attorney's office, Geofeedia advised that "[s]ince we last spoke we have started working with several district attorney's offices around the country, [sic] monitoring for protests and investigations are driving this move."[15] In effect, the company was focusing on using social media to monitor largely lawful protestors.

After uncovering these documents, the ACLU of California, Center for Media Justice, and Color of Change took this information to the social media companies to highlight that the platforms were being used to surveil their users for engaging in constitutionally-protected activities.[16]

In response, during the fall and winter of 2016, the three major social media platforms—Facebook, Twitter, and Instagram—banned developers

---

10. *Id.* at 10.

11. Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU: N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

12. *Id.*

13. *Id.*

14. *Terms of Service,* FACEBOOK, https://www.facebook.com/legal/terms, at "3. Your Commitments to Facebook and Our Community" (last visited Mar. 12, 2019).

15. Email from Geofeedia Representative to Sacramento County District Attorney's Office (Jul. 11, 2016, 06:33 AM), https://www.aclunc.org/docs/20161011_geofeedia_das_monitoring_protests.pdf.

16. Cagle, *supra* note 11.

from using their data for surveillance purposes.[17] This ban did not prevent police investigators or anyone else from viewing public profiles individually or searching manually for specific hashtags or location keywords. However, companies that developed software for the purpose of large-scale social media monitoring, which gathered and analyzed much larger quantities of data than an individual user could, were barred from using the platforms' data for that purpose.[18] As a result of the ban, the major monitoring companies either closed down or had to refocus their strategies and services towards other clients.[19]

These changes—and the nature of social media overall—pose a dilemma. Some content posted on social media is likely to be of significant, and legitimate, interest to law enforcement—for instance, an admission of a serious crime. At the same time, there are both practical and philosophical questions about how police can use social media to find that information. Conducting indiscriminate monitoring in hopes of coming across incriminating content makes it likely that communities that have traditionally been the focus of policing—primarily communities of color—will be disproportionately targeted online as well.[20] This practice also magnifies the risk of incidentally surveilling individuals engaged in First Amendment-protected activities, like organizing for political purposes, or using monitoring ostensibly directed at criminal activity as a pretext for collecting data about constitutionally protected pursuits. Moreover, because

17. *See* Elizabeth Dwoskin, *Facebook Says Police Can't Use Its Data for "Surveillance,"* WASH. POST (Mar. 13, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/?utm_term=.9ca7fa5f3eb8; David Gilmour & Dell Cameron, *Twitter Cuts Off Third Surveillance Firm for Encouraging Police to Spy on Activists,* DAILY DOT (Feb. 24, 2017, 11:41 AM), https://www.dailydot.com/layer8/media-sonar-twitter-social-media-monitoring/; April Glaser & Kurt Wagner, *Twitter Reminds Everyone It Won't Cooperate with Government or Police Surveillance*, RECODE (Nov. 22, 2016, 9:24 PM EST), https://www.recode.net/2016/11/22/13719876/twitter-surveillance-policy-dataminr-fbi.

18. Amina Elahi, *Geofeedia Cuts Half of Staff After Losing Access to Twitter, Facebook*, CHI. TRIB. (Nov. 21, 2016, 5:16 PM), https://www.chicagotribune.com/bluesky/originals/ct-geofeedia-cuts-jobs-surveillance-bsi-20161121-story.html.

19. *See, e.g.*, *id.*; Lani Rosales, *Snaptrends Quietly Lays Off Entire Staff, Ceases Operations*, AM. GENIUS (Oct. 31, 2016), https://theamericangenius.com/business-news/snaptrends-quietly-lays-off-entire-staff-ceases-operations/.

20. Kashmir Hill, *The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook*, ROOT (Oct. 23, 2018, 1:30 PM), https://www.theroot.com/the-wildly-unregulated-practice-of-undercover-cops-frie-1828731563.

these tools were so lucrative for the companies involved, it seems unlikely that this field will dry up entirely, though it remains to be seen exactly how the companies will offer their services.

For example, Babel Street, a D.C.-area company that transacts with companies in the defense community, is marketing social media monitoring services with a wrinkle. Babel Street advertises to defense companies that it can gather users' information from public social media, but it does not give the acquired raw data to law enforcement; instead, Babel Street analyzes the data, packages it, and sells to law enforcement in its modified form.[21] Other companies are targeting schools and school districts, playing off fears of school shootings and other potential threats.[22]

IV. Case Studies

The next question worth answering is: does it matter? People post to social media all the time, with varying assumptions about what happens to their data once it's been posted. Some people may be unaware of the ways in which their social media information may be used, while other users may be cautious about what they choose to share or whom they accept as a friend or follower. One could argue that users are knowingly accepting the risk when they share information on public social media sites. But to answer the question of whether social media monitoring matters, it is important to understand first how police departments are using social media, and second, what constitutional concerns arise from the police's use of social media.

A. Memphis Police Department

The first case study involves the Memphis Police Department, which used social media monitoring tactics to monitor protestors and communities of color. Memphis police officers set up a fake Facebook profile, with the name Bob Smith and a generic profile picture, so they could develop online friendships with targeted users.[23] The police officers used this Bob Smith

21. *See* Aaron Gregg, *For This Company, Online Surveillance Leads to Profit in Washington's Suburbs*, WASH. POST (Sept. 10, 2017), https://www.washingtonpost.com/business/economy/for-this-company-online-surveillance-leads-to-profit-in-washingtons-suburbs/2017/09/08/6067c924-9409-11e7-89fa-bb822a46da5b_story.html?utm_term=.113c0f355eb2.

22. Tom Simonite, *Schools Are Mining Students' Social Media Posts for Signs of Trouble*, WIRED (Aug. 20, 2018, 6:00 AM), https://www.wired.com/story/algorithms-monitor-student-social-media-posts/.

23. Antonia Noori Farzan, *Memphis Police Used Fake Facebook Account to Monitor*

profile to send friend requests to people who were active in the organizing community in Memphis, including Black Lives Matters activists; if the targeted user accepted the friend request, the Memphis police would be able to see everything the user had posted, exchange direct messages with the user, and even view and collect information about other users who commented on and "liked" the activist's posts.[24]

The Memphis police used information gleaned from Facebook to create dossiers on activists, which were distributed internally among the Memphis police department.[25] The officers also used the Bob Smith profile to keep track of organizers around the community and flag not only protests and community meetings but also events like block parties or school supply drives.[26] These types of events would then end up on the internal dossier kept by the police. A police department's primary role is to serve and keep people safe; tracking block parties and backpack events wastes time and resources and undermines the relationship between the police and the community.

The ACLU challenged these dossiers, arguing that in the absence of any allegations of criminal activity, the practices violated a late-1970s consent decree prohibiting officers from surveilling non-criminals.[27] After the ACLU initiated its lawsuit against the City of Memphis, the city argued that the consent decree was outdated and was designed without the internet in mind, and therefore only addressed in-person meetings, not online interactions.[28] The judge ruled recently that the case could go forward, which indicates that the ACLU at least has a colorable argument that the police department violated the consent decree.[29]

Black Lives Matter, Trial Reveals, WASH. POST (Aug. 23, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/?noredirect=on&utm_term=.670e5da474be.

24. *Id.*

25. *Id.*

26. *Id.*

27. *ACLU of Tennessee Joins Lawsuit Challenging Memphis Police Spying on Political Groups*, ACLU (Mar. 2, 2017), https://www.aclu.org/news/aclu-tennessee-joins-lawsuit-challenging-memphis-police-spying-political-groups.

28. Yolanda Jones, *Judge Issues Sanctions Against City for Violating Consent Decree,* DAILY MEMPHIAN (Oct. 26, 2018, 9:59 PM CT), https://dailymemphian.com/article/930/Judge-issues-sanctions-against-city-for-violating-consent-decree.

29. Since this talk was delivered, the court ruled that the city had violated the consent decree; the judge ordered the city to implement new policies and training protocols and appointed a monitor to oversee the process. In the interest of full disclosure, I have joined the monitoring team as a subject matter expert on social media monitoring. *See id.*

B. Boston Police Department

The Boston Police Department also engaged in monitoring and surveillance of users on social media. From 2014 to 2016, the Boston Police Department paid Geofeedia, the company discussed in Part II *supra*, to track protestors and hashtags on Facebook, Instagram, YouTube, and Twitter.[30] In 2014, after the shooting of Mike Brown in Ferguson, Missouri, the Boston police used Geofeedia to track hashtags related to Ferguson, protests, and Black Lives Matter.[31] In 2016, the Boston Police Department used Geofeedia to track the Muslim Lives Matter hashtag, as well as terms common within the Muslim community.[32] As in Memphis, the Boston Police Department monitored these users in the absence of any indication of wrongdoing or criminal activity.[33] Instead, the Boston police simply tracked hashtags associated with particular minority groups. As a result of their surveillance efforts, Boston police officers collected nearly two thousand posts from tracked terms.[34]

C. Other Jurisdictions Utilizing Social Media Monitoring

The Baltimore Police Department has arguably been a repeat offender in terms of both the police technology they use and the lack of transparency around that technology.[35] During the Freddie Gray riots, the Baltimore County Police used Geofeedia for real-time, location-based surveillance, including running photos from social media through real-time facial recognition software, so police could identify people with outstanding warrants and arrest them on the spot.[36] The City of Baltimore also

30. Iqra Asghar, *Boston Police Used Social Media Surveillance for Years Without Informing City Council*, ACLU (Feb. 8, 2018, 12:45 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/boston-police-used-social-media-surveillance-years-without.

31. *Id.*

32. *Id.*

33. *Id.*

34. *See* Nasser Eledroos & Kade Crockford, *Social Media Monitoring in Boston: Free Speech in the Crosshairs*, PRIVACY SOS, https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/ (last accessed Mar. 29, 2019).

35. Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017, 7:27 PM ET), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/.

36. *Id.*; *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, GEOFEEDIA (2016), https://www.aclunc.org/docs/20161011_

contracted with Geofeedia to "continuously monitor and record social media," including setting up alert notifications that were "triggered by specific key words, phrases or users."[37]

In Oregon, the Director of Civil Rights at the Oregon Department of Justice discovered that police were monitoring him after he posted tweets that used the phrase "Black Lives Matter"; the Salem, Oregon police were using a monitoring software that was flagging that and similar hashtags.[38] The Director also learned the police were creating a dossier on him for using this term. After he sued,[39] the Attorney General fired the agent overseeing the monitoring and instructed Oregon law enforcement to cease using monitoring software.[40]

Nationally, the federal government also utilizes social media to track people of interest. The Department of Homeland Security has used Facebook and Twitter to monitor protests in Baltimore, Washington, D.C., Ferguson, and New York City.[41] The Department of Homeland Security also monitored Deray McKesson, an activist for racial justice and a leader in the Black Lives Matter community, because the DHS considered him a "professional protestor."[42] The Department even spent money monitoring

---

geofeedia_baltimore_case_study.pdf.

37. Alison Knezevich, *Police in Baltimore, Surrounding Communities Using Geofeedia to Monitor Social Media Posts*, BALT. SUN (Sept. 5, 2016, 5:59 PM), https://www.baltimoresun.com/news/maryland/investigations/bs-md-geofeedia-police-20160902-story.html.

38. *See* Nigel Jaquiss, *Oregon Department of Justice Civil Rights Chief Intends to Sue His Agency over Black Lives Matter Surveillance*, WILLAMETTE WK. (Oct. 3, 2016), https://www.wweek.com/news/2016/04/15/oregon-department-of-justice-civil-rights-chief-intends-to-sue-his-agency-over-black-lives-matter-surveillance/.

39. *See generally* Complaint, Johnson v. Rosenblum, No. EEEMRC160406-40462, (Or. Bureau of Lab. and Indus. Apr. 5, 2016), https://s3.amazonaws.com/wapopartners.com/wweek-wp/wp-content/uploads/2016/04/15172052/Johnson-complaint.pdf.

40. Dana Tims, *Justice Department Investigator Fired over Black Lives Matter Profiling Scandal*, OREGONIAN: OREGONLIVE (Oct. 26, 2016), https://www.oregonlive.com/politics/2016/10/black_lives_matter_profiling.html.

41. George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

42. Jason Leopold, *Emails Show Feds Have Monitored 'Professional Protestor' DeRay Mckesson*, VICE NEWS (Aug. 11, 2015), https://news.vice.com/en_us/article/qv58n3/emails-show-feds-have-monitored-professional-protester-deray-mckesson; *see also* Lee Fang, *Why Was an FBI Joint Terrorism Task Force Tracking a Black Lives Matter Protest?*, INTERCEPT (Mar. 12, 2015, 6:12 PM), https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/.

D.C.'s Funk Parade.[43] These case studies illustrate the use of social media monitoring tools not to track criminal activity, but to target communities of color for taking part in constitutionally protected pursuits.

D. Use of Social Media in Criminal Cases

Of course, social media can contain evidence of criminal intent as well. In 2014, the New York Police Department (NYPD) and the Manhattan District Attorney's Office (Manhattan DA) prosecuted the largest gang case in New York City's history.[44] The indictments in that case relied on hundreds of references in Facebooks posts and messages where gang members bragged about murders and asked about drugs and robberies.[45] The NYPD and Manhattan DA reviewed over a million social media pages during the investigation and indicted over a hundred people.[46] The use of social media in criminal investigations can have a darker side as well, however.

1. Jelani Henry

Jelani Henry was a teen who grew up in New York City. He and his brother Asheem were members of a "crew," which is not a gang but is a sort of affiliation of neighborhood kids who hang out together.[47] While Asheem had committed some crimes as a crew member, Jelani himself had stayed in the background and away from criminal activity.[48] When he was erroneously picked out of a lineup for committing attempted murder, however, he was described in court proceedings as a member of a "violent gang"—on the grounds that he had appeared on social media in pictures with other members of the crew, and had commented on and liked videos of other crew members.[49] In addition, after Asheem was arrested for his crimes, he was also indicted on conspiracy charges, largely on the strength

43. Joseph, *supra* note 41.

44. Victoria Cavaliere, *More than 100 Indicted in Harlem in Largest-Ever NYC Gang Bust*, REUTERS (June 4, 2014, 9:15 AM), https://www.reuters.com/article/us-usa-crime-gangs/more-than-100-indicted-in-harlem-in-largest-ever-nyc-gang-bust-idUSKBN0EF1DQ20140604.

45. *Id.*

46. *Id.*

47. *See generally* Ben Popper, *How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars*, VERGE (Dec. 10, 2014, 1:15 PM), http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

48. *Id.*

49. *Id.*

of online pictures showing him with other crew members.[50] Jelani ultimately spent two years on Rikers Island, including roughly nine months in solitary confinement, before his case was finally dropped and he was let out.[51] As it turns out, there was no case against Jelani; despite that, he spent two formative years in jail, largely on the basis of social media "evidence."

2. Sondra Arquiett

As part of an investigation, the DEA seized a cell phone belonging to Sondra Arquiett, using pictures that were on it of her and her children—to impersonate her on Facebook.[52] Using the pictures of Ms. Arquiett and her children, the DEA set up a fake account and pretended to be her in order to gather information about a drug-trafficking ring.[53] Ms. Arquiett eventually learned of the impersonation and sued the DEA for putting her life and her children's life in danger by implicating her in the undercover scheme.[54] The agency settled with Ms. Arquiett for a little over $100,000.[55]

V. Constitutional Issues Arising from the Use of Social Media Monitoring by Law Enforcement

Knowing how the police use, or misuse, social media begs the question: Are the police violating the Constitution when they gather information in this way? There is no federal law, and as far as I am aware no state or local law, that limits how law enforcement can use social media. Some police departments have internal policies explicating their use of social media, but very few police departments actually publish those policies, as discussed in Part II. Despite these bleak statistics, some police departments may provide their officers guidance and training on how to use social media appropriately, but, again, few agencies do this.

---

50. *Id.*

51. *Id.*

52. Sari Horwitz, *Justice Dept. Will Review Practice of Creating Fake Facebook Profiles*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/world/national-security/justicedept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html.

53. *Id.*

54. *Id.*

55. David Kravets, *DEA Settles Fake Facebook Profile Lawsuit Without Admitting Wrongdoing*, ARS TECHNICA (Jan. 20, 2015), http://arstechnica.com/tech-policy/2015/01/dea-settles-fakefacebook-profile-lawsuit-without-admitting-wrongdoing/.

So, if there are no on-point laws preventing surveillance of social media by the police, what does the constitutional landscape look like? The first possible constitutional avenue for contesting social media monitoring would be the Fourth Amendment's protection against unreasonable searches and seizures. Traditionally, this would be challenging. The public space doctrine has traditionally held that when someone does something in public that can be seen by another individual, they have no reasonable expectation of privacy in that action, and that a police officer can therefore also watch what they are doing without a warrant.[56] So, for example, if someone is driving down the road, any other driver on the road—including a law enforcement officer—can see that person, and the original driver therefore has no reasonable expectation of privacy in his movements on the road. Similarly, if a social media user posts something publicly, anyone with access to that social media site can see it; the public space doctrine as historically interpreted would hold that user has no reasonable expectation of privacy.

Another doctrine that could pose difficulties in the Fourth Amendment context is the third-party doctrine. Essentially, the third-party doctrine presumes that anytime someone hands information over to someone else, or speaks to someone else, the speaker takes the risk that the receiver is a government agent or may give that information to a government agent. Courts are unsympathetic to the defense that the speaker was communicating in confidence.[57] In general, when the third-party doctrine is applied to instances involving social media—for instance, if a user befriends an undercover cop on social media and divulges important information to the seemingly innocuous fake profile—courts have held that accepting a friend request from another user is akin to connecting with someone in real life, and that the user therefore takes the risk that the other profile could be a government agent.[58]

---

56. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 276 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.").

57. The modern third-party doctrine traces its roots to a series of cases from the 1960s and 1970s. The principle was clearly articulated in *United States v. Miller*, where the Court "held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

58. *See, e.g.*, United States. v. Gatson, No. 13-705, 2014 U.S. Dist. LEXIS 173588, at

Following on these doctrines, courts so far have held that the use of online undercover accounts by police is not a violation of the Fourth Amendment. But that may be starting to change. The U.S. Supreme Court is beginning to see that technology has so significantly expanded what the government and law enforcement can do with such little effort that the constitution may require a more robust response.[59]

For example, one area where the Supreme Court has curtailed police departments' use of monitoring technology is with GPS trackers. Typically, if a police department wants to tail a vehicle to track its movements, it would assign officers to keep surveillance on the vehicle or the individual's whereabouts without the need for a warrant.[60] In order to do so, the police department would have to determine that it was worth expending police resources and manpower to maintain that particular surveillance.[61] With GPS trackers, a police officer can affix a GPS tracker to a specific vehicle and then track its movements, minute-by-minute, remotely via the GPS tracker's signals. This method is much cheaper for police departments to employ and is also very revealing because of its accuracy. Therefore, a plurality of the Court has indicated that even though police officers can follow a vehicle down the street in public spaces, they cannot use a GPS tracker to record an individual's detailed movements without a warrant.[62]

There is an argument that police monitoring of social media is an equally intrusive violation of constitutional rights—certainly through the kinds of third-party tools that are now largely no longer available to law enforcement, and even with the more retail (as opposed to wholesale) monitoring tactics that are still available. Police can gather a lot of information to track what certain users post, which hashtags they use, and with whom they are connected. And they can do all this for multiple users, while sitting at their desks. That is powerful surveillance technology that starts to look a lot like putting a GPS on a car and gleaning all of that information about the driver.

---

*60 (D.N.J. Dec. 16, 2014); United States v. Meregildo, 883 F. Supp. 2d 523 (S.D.N.Y. 2012); *see also* Jordan Crook, *Police Can Create Fake Instagram Accounts to Investigate Suspects*, TECHCRUNCH (Dec. 24, 2014), https://techcrunch.com/2014/12/24/police-can-create-fake-instagram-accounts-to-investigate-suspects/.

59. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014); United States v. Jones, 565 U.S. 400 (2012).

60. *Jones*, 565 U.S. at 429-31 (J. Alito, concurring).

61. *See id.*

62. *See Jones*, 565 U.S. at 404, 413.

What about the third-party doctrine? The Supreme Court recently held in *Carpenter v. United States* that law enforcement must obtain a warrant to get a week or more of historical cell site location information from a cell phone provider, even though the provider is a "third party" in this scenario.[63] The Court reasoned that the data could not truly be said to have been "voluntarily" shared with the provider, since "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[64] This data can reveal whom a person is with, where they go, where they sleep at night or work during the day, and more. Although it is not yet clear how or if this reasoning might apply in the social media context, it is nevertheless a chink in the armor of the third-party doctrine.

Advanced social media monitoring tactics could also complicate the application of the third-party doctrine to social media interactions. The best example is the case of Sondra Arquiett, discussed *supra* in Part IV. There, the DEA confiscated pictures from her phone and used them to create a fake profile impersonating Ms. Arquiett. People who were interacting with the fake Sondra Arquiett account thought they knew with whom they were conversing, but instead there were DEA agents behind the fake account, while the users were deprived of even the opportunity to make the kind of face to face judgments one could do in person. Although this is a largely unexplored area thus far, courts could handle these situations differently because of the heightened difficulty in unmasking an impersonator online.

Another avenue for constitutional challenge is the First Amendment. When police target social activists and political protest groups on social media—as was done in Memphis, Boston, and Oregon—the police are largely monitoring First Amendment-protected actions and, in some cases, taking action based on that monitoring. The Supreme Court has recently said that cyberspace, and especially social media, is now the most important space for the exchange of views, so social media is clearly being viewed as a First Amendment-protected space.[65] Therefore, if the government or law

63. *See Carpenter*, 138 S. Ct. at 2217, 2221.

64. *Id.* at 2219-20.

65. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) ("While in the past there may have been some difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular." (quoting Reno v. Am. Civil Liberties Union, 521 U.S. 844, 868 (1997))); *see also* Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015) (holding that when discriminatory government surveillance dissuades individuals from exercising their rights, they can challenge the surveillance under the First and Fourteenth Amendments).

enforcement were to monitor or surveil an individual on social media in retaliation for his or her First Amendment-protected activity, the user would arguably have a First Amendment claim against the government.

Finally, knowing that police departments around the country are monitoring social media for surveillance purposes, and knowing the fallibility and opportunities for misuse that come with social media surveillance, how should legislators approach this unsettled area of law? While viewing social media profiles may be appropriate and necessary in some cases, there must also be strict limitations on the police's use of social media surveillance tools. Law enforcement agencies engaging in social media monitoring should implement policies governing their use of social media monitoring and publish those guidelines publicly. There should be transparency about the use of social media, procedures for dealing with misuse, and available oversight procedures. Finally, there must be limitations on the use of undercover accounts, the monitoring of First Amendment-protected activity, and surveillance of juveniles. While such steps may not entirely mitigate the risks arising from police surveillance of social media, they would be a step in the right direction.