Government Access to and Manipulation of Social Media: Legal and Policy Challenges

RACHEL LEVINSON-WALDMAN*

INTRODUCTION

Technology is transforming the practice of policing and intelligence. In addition to the proliferation of overt surveillance technologies, such as body cameras and license plate readers, there is a revolution playing out online where domestic law enforcement agencies are using social media to monitor individual targets and build profiles of networks of connected individuals. Social media is fertile

* Senior Counsel to the Liberty and National Security Program at New York University School of Law's Brennan Center for Justice.

2018 Vol. 61 No. 3

ground for information collection and analysis. Facebook boasts over two billion active users per month; its subsidiary Instagram has 800 million monthly users; and Twitter weighs in at 330 million monthly active users, including nearly a quarter of all U.S. citizens.[1] It is thus no surprise that in a 2016 survey of over 500 domestic law enforcement agencies, three-quarters reported that they use social media to solicit tips on crime, and nearly the same number use it to monitor public sentiment and gather intelligence for investigations.[2] Another sixty percent have contacted social media companies to obtain evidence to use in a criminal case.[3]

While these new capabilities may have value for law enforcement, they also pose novel legal and policy dilemmas.[4] On the privacy front, government surveillance was once limited by practical considerations like the time and financial cost associated with monitoring people.[5] As surveillance technology grows ever more sophisticated, however, the quantity of data and ease of accessibility grows as well, lowering the bureaucratic barriers to privacy intrusions and creating opportunities for near-frictionless surveillance that the Founders could not have envisioned. And in an era when people use social media sites "to engage in a wide array of protected First Amendment activity on topics 'as diverse as human thought,'"[6] studies indicating that online surveillance produces a chilling effect and thus may suppress protected speech, association, and religious and political activity are of particular concern.[7]

1. Dan Noyes, *The Top 20 Valuable Facebook Statistics — Updated February 2018*, Zephoria Dig. Mktg., https://zephoria.com/top-15-valuable-facebook-statistics/ (last visited Mar. 9, 2018); Rob Mathison, *23+ Useful Instagram Statistics for Social Media Marketers*, Hootsuite Blog (Jan. 24, 2018), https://blog.hootsuite.com/instagram-statistics/; Salman Aslam, *Twitter by the Numbers: Stats, Demographics & Fun Facts*, Omnicore (Jan. 1, 2018), https://www.omnicoreagency.com/twitter-statistics/; Kit Smith, *44 Incredible and Interesting Twitter Statistics*, Brandwatch Blog (Dec. 17, 2017), https://www.brandwatch.com/blog/44-twitter-stats-2016/.

2. KiDeuk Kim, et al., Urban Inst., 2016 Law Enforcement Use of Social Media Survey 3 (2017), http://www.theiacp.org/Portals/0/documents/pdfs/2016-law-enforcement-use-of-social-media-survey.pdf.

3. *Id.* at 5.

4. *See generally* Alexandra Mateescu et al., *Social Media Surveillance and Law Enforcement*, Data & Soc'y (Oct. 27, 2015), http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf.

5. *See generally* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605 (2007), http://ssrn.com/abstract=1004675.

6. Packingham v. North Carolina, No. 15-1194, slip op. at 5 (U.S. June 19, 2017) (quoting Reno v. American Civil Liberties Union, 521 U.S. 844, 870 (1997) (internal quotation marks omitted)).

7. *See generally* Nafeez Ahmed, *"Chilling Effect" of Mass Surveillance Is Silencing Dissent Online, Study Says*, Vice: Motherboard (Mar. 17, 2016, 6:00 AM), http://motherboard.vice.com/read/chilling-effect-of-mass-surveillance-is-silencing-dissent-online-study-says; Jason Leo-

Moreover, much as with other types of surveillance technologies, social media monitoring appears likely to disproportionately affect communities of color. Youth of color are particular targets, with the most high-profile examples arising in the context of gang surveillance, raising concerns that already over-policed communities will bear the brunt of its intrusion.[8] These tools are likely to pose even more difficult questions in an era of live video streaming, a popular tool that police have used to gather information and also manipulated to control users' access to their friends and contacts.[9]

This essay highlights issues arising from law enforcement's use of social media for a range of purposes; analyzes the legal framework that governs its use; and proposes basic principles to govern law enforcement's access to social media in order to ensure transparency and safeguard individuals' rights to privacy, freedom of expression, and freedom of association.

I. LAW ENFORCEMENT MONITORING OF PUBLICLY AVAILABLE SOCIAL MEDIA

As social media plays an increasingly prominent role in individuals' social interactions, political involvement, and economic transactions, it becomes an increasingly attractive target for law enforcement scrutiny as well. While tools for social media analysis run the gamut from straightforward to sophisticated, and with companies developing ever more creative ways to mine the data embedded in social media communications, law enforcement surveillance of social media can be

---

pold, *How the Government Monitored Twitter During Baltimore's Freddie Gray Protests*, VICE (May 18, 2016, 8:00 PM), https://www.vice.com/read/riot-police-v23n3.

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

9. *See* Lehigh University, *Live-Streaming Crime: How Will Facebook Live and Periscope Challenge US Privacy Law?*, SCI. DAILY (Aug. 3, 2016), http://www.sciencedaily.com/releases/2016/08/160803140150.htm. In August 2016, police requested that Facebook cut off the account of a woman who was live-streaming her hostage negotiations; they subsequently killed her during a shoot-out. *See Baltimore County Woman Killed in Police Standoff Tried to Live Stream Incident*, KTLA5 (Aug. 3, 2016, 12:25 PM), http://ktla.com/2016/08/03/baltimore-county-woman-killed-in-police-standoff-tried-to-live-stream-incident/. The police said they made the request because her friends were encouraging her to resist law enforcement and were making it difficult to negotiate; her friends say the police requested the account takedown simply to cut her off from family and community support. *Id.*; Rachel Weiner & Lynh Bui, *Korryn Gaines, Killed By Police in Standoff, Posted Parts of Encounter On Social Media*, WASH. POST (Aug. 2, 2016), https://www.washingtonpost.com/local/public-safety/maryland-woman-shot-by-police-in-stand-off-posted-part-of-encounter-on-social-media/2016/08/02/d4650ee6-58cc-11e6-831d-0324760ca856_story.html?utm_term=.552347d39c78.

divided into three broad categories: (1) following or watching online an identified individual, group of individuals, or affiliation (e.g., an online hashtag); (2) using an informant, a friend of the target, or an undercover account to obtain information; and (3) using analytical software to generate data about individuals, groups, associations, or locations. In addition, law enforcement officers can go directly to the social media platforms themselves to request information, from basic subscriber information to metadata to the content of messages. Each platform has various mechanisms to handle these direct requests and levels of legal process that are required; the more private the data, the more robust the legal protections.[10]

A. Following Individuals, Groups, or Affiliations

1. Technology and Case Studies

Perhaps the simplest way of learning more about a target or group of individuals online is to follow them on public social media platforms, either individually or by hashtag. On both Twitter and Instagram, for instance, even without an account, it is possible to view any information about a person with a public account via a direct profile link or a search engine.[11] It is feasible to find someone in a similar way on Facebook, although Facebook's privacy settings tend to be somewhat more restrictive than Twitter's, meaning that viewing an individual's public profile is likely to yield less information (though still a significant amount).[12] Messaging and social media services such as

10. *See generally Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Jan. 16, 2018); *Information for Law Enforcement*, INSTAGRAM, https://help.instagram.com/494561080557017 (last visited Jan. 16, 2018); *Guidelines for Law Enforcement*, TWITTER, https://support.twitter.com/articles/41949#7 (last visited Jan. 16, 2018); *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy?lang=en (last visited Jan. 16, 2018); *Snapchat Law Enforcement Guide*, SNAPCHAT (Oct. 11, 2016), https://www.snapchat.com/static_files/lawenforcement.pdf (last visited Jan. 16, 2018).

11. A February 2015 survey about Instagram found that forty-three percent of Instagram users have their accounts set to private, meaning that even someone with an account will be unable to view those users' photos unless they accept a friend request. *See* Melchior Schöller, *10 Surprising Instagram Stats*, LINKEDIN SLIDESHARE (Mar. 31, 2015), https://www.slideshare.net/melkischoller/10-surprising-instagram-facts. While up-to-date numbers on Twitter are not available, studies suggest that a substantial majority of Twitter postings are public. One study estimated that only about ten to fifteen percent of tweets made in 2009 and 2010 were unavailable because the accounts were private. *See* Alexis Madrigal, *How Twitter Has Changed Over the Years in 12 Charts*, THE ATLANTIC (Mar. 30, 2014), https://www.theatlantic.com/technology/archive/2014/03/how-twitter-has-changed-over-the-years-in-12-charts/359869/.

12. *See What is Public Information?*, FACEBOOK, https://www.facebook.com/help/203805466323736 (last visited Feb. 18, 2017) (detailing what information is always publicly available on Facebook); *How Can I Adjust My Privacy Settings?*, FACEBOOK, https://www.facebook.com/help/

Snapchat are more restrictive; only individuals with accounts can see most information about others using the service.[13]

The easy availability of detailed information about individuals' activities has turned social media into a wellspring of information for law enforcement, efforts that inevitably put greater scrutiny on communities of color and particularly youth of color. The New York City Police Department (NYPD) and New York District Attorney's office have been particularly heavy users of social media information.[14] The NYPD's Intelligence Division, which includes a team of detectives and officers described as having "knowledge of current technologies and street jargon," has used social media to monitor and anticipate "large-scale events and criminal activity," as well as to assist other units with criminal investigations.[15] The department's Juvenile Justice Division focuses on "analyzing social networking by local youth gangs and neighborhood crews," groups whose members watch each other's backs but do not have the hierarchy or organizational structure of gangs.[16] In addition, a special social networking unit inside the Division maps out territories covered by crews, block by block, to facilitate the monitoring of crew members on Facebook.[17] Posts on social net-

---

193677450678703?helpref=uf_permalink (last visited Feb. 19, 2017) (describing how to use Facebook's privacy settings).

13. *How to View Snapchat Profile*, WikiHow, https://www.wikihow.com/View-Snapchat-Profile (last visited Mar. 12, 2018); Sean Keach, *Happy Snapper: How to Use Snap Maps Without Having the Snapchat App,* Sun (Feb. 12, 2018, 1:11 PM), https://www.thesun.co.uk/tech/5558154/how-to-use-snap-maps-without-snapchat-app/.

14. *See* Office of Community Oriented Policing Servs., U.S. Dep't Justice and Police Exec. Research Forum, Social Media and Tactical Considerations 13 (2013) [hereinafter *COPS*] (identifying the Department's Intelligence Division and Juvenile Justice Division as being at the forefront of social media analysis within the NYPD). The NYPD's 2012 policy on using social networks for investigative purposes permits officers to access social network sites, and states that "[n]o prior authorization [is] required to review publicly accessible information . . . ." Tim Cushing, *NYPD Social Media Monitoring Policy Allows For Use of Aliases, Has Exceptions for Terrorist Activity*, TechDirt (Feb. 11, 2015, 4:10 AM), https://www.techdirt.com/articles/20150206/17211929943/nypd-social-media-monitoring-policy-allows-use-aliases-has-exceptions-terrorist-activity.shtml; *see also* Handschu v. Police Dep't of N.Y., 241 F. Supp. 3d 433, 460 (S.D.N.Y. 2017) ("For the purpose of developing intelligence information to detect or prevent terrorism or other unlawful activities, the NYPD is authorized to conduct online search activity and to access online sites and forums on the same terms and conditions as members of the public generally."). A separate policy governs the general use of social media by members of the service, focusing more on officers' public-facing use. *See, e.g.*, Shawn Musgrave, *NYPD Social Media Policy*, MuckRock, https://www.muckrock.com/foi/new-york-city-17/nypd-social-media-policy-11570/# (last visited May 12, 2017).

15. *COPS*, *supra* note 14, at 13–14.

16. *Id.* at 13.

17. *Id.* at 15. As of 2013, 250 crews had been identified and mapped. *Id.*; *see also JECS Provides Crew Maps by Borough*, Juvenile Justice Division 2 (Fall 2013), http://www.nyc.gov/html/nypd/downloads/pdf/community_affairs/jjdnewsletter.pdf.

works have also been provided to probation and parole officers, and conditions of parole or probation sometimes include a prohibition on engaging in social networking interactions with other crew members, which could mean a virtual freeze on any online activity for the affected youth, in light of the near impossibility of building an impervious digital wall.[18]

Like many teenagers, young people who join crews communicate on social media, posting pictures of parties and tagging videos with their crews' name. Unlike suburban kids, however, their boasts and brags are often watched in real time by law enforcement, starting — by at least one account — when the youth are as young as ten years old.[19] And because criminal conspiracy laws allow even a picture of friends together at a party to be used as evidence of a criminal act, social media postings can have significant real-world consequences.[20]

In one well-reported case, a young man named Asheem Henry was arrested based largely on social media postings he put up as a juvenile.[21] His younger brother Jelani was subsequently arrested after being wrongly identified as a suspect in an attempted murder; at his arraignment, the district attorney used evidence that Jelani, then a teenager, had "liked" posts about his brother's crew to persuade the judge to deny him bail and send him to Rikers Island.[22] Jelani served two years at Rikers awaiting trial — including nine months in solitary confinement — until his case was finally dismissed.[23] In the words of CryptoHarlem security researcher Matt Mitchell, "if you're black or brown, your social media content comes with a cost — it's a virtual prison pipeline."[24]

18. *COPS*, *supra* note 14, at 16.

19. *See* Rose Hackman, *Is the Online Surveillance of Black Teenagers the New Stop-And-Frisk?*, THE GUARDIAN (Apr. 23, 2015, 8:00 AM), http://www.theguardian.com/us-news/2015/apr/23/online-surveillance-black-teenagers-new-stop-and-frisk.

20. *See* Popper, *supra* note 8. Notably, some scholars agree that online activity can provide a valuable window into real-life feuds and can even provide the spark that turns those feuds into potentially deadly encounters. *See* Ben Schamisso, *How Social Media Can be Used to Stop Gang Violence*, NEWSY (Dec. 2, 2016), http://www.newsy.com/videos/social-media-contributes-to-gang-violence-nationwide/#.WFbTBCjJpZE.twitter. They have advocated for "violence interrupters," social workers, and other community advocates — not law enforcement — to play a role in watching, interpreting, and defusing online exchanges before they translate into real-life violence. *Id.*

21. Popper, *supra* note 8.

22. *Id.*

23. *Id.*

24. George Joseph, *How Police Spy on Social Media*, CITYLAB (Dec. 14, 2016), https://www.citylab.com/equity/2016/12/how-police-are-watching-on-social-media/508991/; *see also* Debra Cassens Weiss, *Suit Claims Arrests Over Social Media Posts and Rap Lyrics Violated First Amendment Rights*, ABA J. (Jan. 13, 2017, 4:30 AM), http://www.abajournal.com/news/article/

Of course, actions that could draw scrutiny on social media — from hitting a "like" or "favorite" button to commenting on a post or sharing a video — are deeply contextual and can be almost impossible to interpret.[25] A "like," for instance, could mean that the user approves of the post, or simply that she wants to acknowledge it; an outside observer cannot reasonably infer a concrete meaning from a brief interaction online, and research suggests that automated tools are poor judges of social media as well.[26] There is also no guarantee that the person who appears to have communicated online is actually the person whose name is displayed; it is not uncommon for people to share computers and to accidentally (or intentionally) use another's account. One individual could even set up an account for another person, whether with malicious purpose or not.

Social media monitoring can also put individuals, groups, and affiliations (for instance, all persons using a particular hashtag) under scrutiny in ways that implicate constitutional rights. The NYPD's Intelligence Division, for instance, explicitly monitors mass demonstrations and protests.[27] According to Department of Justice materials, the Division obtains information about upcoming protests and monitors events in real-time, including "minute-by-minute information about the size and demeanor of crowds of protestors."[28] This online activity is usually supplemented by intelligence officers on the ground, and is also fed in real time to the NYPD's operations center during "any large event."[29] Fusion centers — multi-stakeholder centers created in the wake of 9/11 to facilitate information-sharing under the auspices of DOJ and DHS — have also flagged alerts on social media about upcoming protests for local police departments, an un-

suit_claims_arrests_over_social_media_posts_and_rap_lyrics_violated_first_a (describing arrest and detention of two men for posting rap lyrics and social media posts on the grounds that they promoted gang violence). Declarations filed by police officers in support of arrest warrants stated that the defendants were friends with gang members on Facebook, and that one had posted a message on Facebook about the arrest of two gang members). *See id.*

25. *See, e.g.*, Meredith Broussard, *When Cops Check Facebook*, The Atlantic (Apr. 19, 2015), http://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/ (observing that "liking" a post on Facebook could mean approval or could mean something vastly different, depending on the context).

26. *See generally* Natasha Duarte, et al., *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Ctr. for Democracy & Tech. (Nov. 2017), https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf.

27. *COPS*, *supra* note 14, at 15, 33.

28. *Id.* at 15.

29. *Id*. It is not clear whether this monitoring occurs by following people publicly, utilizing undercover accounts, or using one of the social media monitoring tools described later, but the most likely option is a combination of the three.

dertaking that is a dubious fit with the centers' original focus on counterterrorism.[30]

Of course, social media is bound to yield legitimate leads as well. One Kentucky defendant was arrested after posting a Facebook picture of himself siphoning fuel from a patrol car, while a burglar in Washington, D.C., took a picture of himself "wearing the victim's coat and holding up the victim's cash," and posted the picture on the victim's Facebook page, using the victim's computer.[31] Notably, when 103 people were arrested in New York City in June 2014 for participating in a criminal conspiracy, Facebook was cited over 300 times in the indictment.[32] People may also post pictures of themselves holding illegal firearms or drugs, or "'brag[ ]' about committing serious violent crimes."[33] Once an individual comes under law enforcement scrutiny, social media can offer a wealth of contextual information unconnected to criminal behavior as well: "travel, hobbies, places visited, appointments, circle of friends, family members, relationships, actions," and more.[34]

Police departments have also credited social media for enabling them to anticipate repeat offenses, although there is little transparency about how the process works. In 2010 and 2011, for instance, people involved in a spate of violent flash mobs in Philadelphia stole merchandise, knocked over bystanders, and obstructed traffic.[35] According to the city's police chief, the department learned that plans were being posted on social media several days before each flash mob, and officers began reviewing publicly available posts on Facebook, Twitter, and other platforms to learn about "potentially dangerous incidents."[36] Notably, it is not clear how the police decided whom to follow, what they did with information that was not relevant to this

30. *See generally So-Called "Counterterror" Fusion Center in Massachusetts Monitored Black Lives Matter Protestors*, PRIVACY SOS BLOG (Nov. 27, 2015), https://privacysos.org/blog/so-called-counterterror-fusion-center-in-massachusetts-monitored-black-lives-matter-protesters/; *COPS*, *supra* note 14, at 15 (noting New York fusion center's collaboration with the NYPD during "very large events").

31. Adrian Fontecilla, *The Ascendance of Social Media as Evidence*, CRIM. JUST., Spring, 2013, at 55.

32. Popper, *supra* note 8; Press Release, Manhattan District Attorney's Office, District Attorney Vance and Police Commissioner Bratton Announce Largest Indicted Gang Case in NYC History (June 25, 2015), http://manhattanda.org/press-release/district-attorney-vance-and-police-commissioner-bratton-announce-indictments-two-major.

33. *COPS*, *supra* note 14, at 12.

34. *Id.*

35. *Id.* at 18.

36. *Id.*

task, or how long they retained any information they collected, leaving the public to rely on the department's description of events.[37] In other circumstances, allegations that social media helped facilitate large-scale violent events have proven false. In the case of the 2011 Vancouver riot after the loss of the Canucks to the Boston Bruins, for instance, social media was used primarily for post-riot investigation and outreach, not to plan the riot.[38]

2. Constitutional and Policy Considerations

Law enforcement's use of technological tools to monitor and collect information about American citizens and residents raises First, Fourth, and Fourteenth Amendment issues, as well as important policy questions. This section addresses each of those in turn.

---

37. *See* PHILADELPHIA POLICE DEP'T, DIRECTIVE 6.10 SOCIAL MEDIA AND NETWORKING 2 (2012), https://www.phillypolice.com/accountability/index.html (stating that "[t]here is no reasonable expectation of privacy when engaging in social networking online. As such, the content of social networking websites may be obtained for use in criminal trials, civil proceedings, and departmental investigations."). Even more alarmingly, the police department directed downtown Philadelphia businesses to call 911 "if you see a large group of youngsters or others who appear to be moving very quickly or running from or to something" or saw "any large groups gathering." *COPS*, *supra* note 14, at 19–20. Notwithstanding the genuine risk posed by these flash mobs — one of the most recent in Center City Philadelphia allegedly resulted in violent attacks on several bystanders — these policies seem guaranteed to be enforced disproportionately against youth of color, whose gatherings in large groups will inevitably be viewed as more suspicious than equivalent assemblies of white youths or others. *See* Dan Wing et al., *30 Arrested After Flash Mob Strikes Center City Philadelphia*, CBS PHILLY (Mar. 6, 2017, 1:55 PM), philadelphia.cbslocal.com/2017/03/06/philly-police-more-than-100-kids-participated-in-flash-mob-some-arrested/ (describing flash mob attack at Center City Philadelphia); *COPS*, *supra* note 14, at 20 (noting that after a series of mobbing events involving assaults on bystanders, Minneapolis police began to monitor social media to pick up clues in advance; the report does not disclose details about which sites or accounts were monitored or how they were chosen).

38. *COPS*, *supra* note 14, at 26, 32 (noting that the riots were primarily fueled by high levels of alcohol consumption, not by social media). Social media can be a valuable source of information during a natural disaster or other public safety crisis as well. During 2017's Hurricane Harvey, for instance, when many phone lines in Houston, Texas, were down or inaccessible and the city's 911 system was overwhelmed, residents turned to social media to tweet pleas for help to first responders and to the public at large. *See* Peter Holley, *"Water is swallowing us up": In Houston, Desperate Flood Victims Turn to Social Media for Survival*, WASH. POST (Aug. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/08/28/water-is-swallowing-us-up-in-houston-desperate-flood-victims-turn-to-social-media-for-survival/?utm_term=.f9fdc49e62f2. Many of the victims explicitly tagged the Houston police or other law enforcement agencies, but government officials may have also been monitoring social media channels; one article depicted the Houston police chief responding to a tweet that did not tag or refer to the police department. *See* Rachel Chason, *"Urgent Please Send Help": Desperate Houston Residents Plead on Social Media for Rescue*, WASH. POST (Aug. 28, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/08/28/urgent-please-send-help-houston-residents-turn-to-social-media-for-help-sunday-night/?tid=a_inl&utm_term=.1695be905381.

a. Fourth, First, and Fourteenth Amendment

The Fourth Amendment guarantees the right of the people to be free from unreasonable searches and seizures.[39] Where the police enter an individual's home or detain an individual, the Fourth Amendment is implicated as a straightforward matter. In the information age, however, where the state's action involves the collection of information about an individual, rather than an intrusion into her home or body, the inquiry generally focuses on whether the individual challenging the action had a "reasonable expectation of privacy" in the information collected: that is, whether she expected that a particular behavior would be private, and if so, whether society – as an objective matter – recognizes that expectation as reasonable.[40] When it comes to social media, it is something of an uphill battle to argue that there is an expectation of privacy in information that is shared online; for that to change, courts will need to begin to reconsider the dogma that privacy requires secrecy.

The reasonable expectation of privacy test was articulated in Justice Harlan's concurrence in the seminal 1967 Supreme Court case *U.S. v. Katz*. In *Katz*, the police used a wiretap, for which they did not obtain a warrant, to listen in on conversations that bookie Charles Katz conducted from a public phone booth.[41] The government argued that because the wiretap did not physically invade the phone booth, it was not constitutionally proscribed and did not require a warrant.[42] Rejecting this argument, the Court observed that Mr. Katz intended to preserve his privacy when he closed the doors to the phone booth and placed his call; although observers could still *see* that he was making a call, "what he sought to exclude when he entered the booth was not the intruding eye – it was the uninvited ear."[43] In the Court's words, "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[44] In concurrence, Justice Harlan set out the reasonable expectation of privacy test that has become a touchstone of Fourth Amendment jurisprudence.[45]

39. U.S. Const. amend. IV.
40. Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).
41. *Id.* at 349–52.
42. *Id.* at 349–53.
43. *Id.* at 352.
44. *Id.* at 359.
45. *Id.* at 360–61 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an

Since its issuance, *Katz* has served as the starting point in challenges to law enforcement's collection of information about individuals in ostensibly public areas, whether they be phone booths, public roads, or pedestrian gathering areas. Thus, in *United States v. Knotts*, the Supreme Court held several decades after *Katz* that the police were justified in using a hidden beeper to track a suspect's car in public without a warrant: because anyone on the roads could see the driver, the Court held, the police could as well.[46]

When police have gone further, however, eliciting information that is not obviously available to the average member of the viewing public, the courts have drawn a constitutional line. Thus, in *United States v. Karo*, the police not only tracked a suspect to a private house but also confirmed that he was inside the house, courtesy of a beeper they had surreptitiously planted in the can of ether he was transporting.[47] Because the officers would normally have needed to obtain a probable cause warrant to enter the house and confirm his presence, using a beeper to do the job was outside the bounds of the Fourth Amendment.[48] Similarly, the Supreme Court held in *Kyllo v. United States* that using a heat sensor that detected the use of marijuana grow lights inside a house – again, a discovery that would have otherwise required an officer to enter the house armed with a warrant issued by a neutral magistrate – had to comply with the mandates of the Fourth Amendment.[49]

What, then, do these cases tell us about the social media context? Monitoring individuals (or even groups) directly on public social media (that is, without the use of undercover accounts or sophisticated analytical tools) may look analogous to the kind of one-on-one real-world tracking the Court endorsed in *Knotts*, making courts reluctant to halt such monitoring on Fourth Amendment grounds.[50] Particularly since post-*Katz* Fourth Amendment doctrine rests in large part on concepts of "privacy," courts are likely to find the notion that

actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

46. United States v. Knotts, 460 U.S. 276, 284–85 (1983).

47. United States v. Karo, 468 U.S. 705, 708 (1984).

48. *Id.* at 715–18.

49. Kyllo v. United States, 533 U.S. 27, 29, 40 (2001).

50. Notably, the *Knotts* Court warned that "dragnet-type law enforcement practices" might implicate the Fourth Amendment – practices that more closely resemble the algorithmic analyses described below. *Knotts*, 460 U.S. at 284.

materials voluntarily posted on public social media sites cannot be considered "private" to be persuasive, if not dispositive.[51]

On the other hand, the two situations are not as analogous as they appear on initial inspection. In *Knotts*, the police officers had to physically tail the vehicle in order to remain within range of the tracking device, requiring a significant commitment of time and personnel and heightening the risk that the officers could be detected by the target.[52] By contrast, following targets on social media is nearly undetectable, particularly on platforms (such as Twitter) that do not require police to connect directly with a target in order to monitor them. It is also far less resource-intensive than physically tailing a person, even without using the kind of specialized analytical software described in Section C. As described in that section, a majority of the Supreme Court is embracing the idea that where technological advances enable law enforcement to undertake surveillance of civilians with far greater ease, and with far less expenditure of time and money than in the nation's early days, constitutional obligations may be triggered. While no court has yet considered the application of this recent approach in the social media context, these factors could shift the analysis when the issue gets litigated.

At the moment, the First and Fourteenth Amendments may have far more to say than the Fourth Amendment about monitoring individuals on social media when the surveillance is based on religious affiliations, associations, political leanings, or other protected categories or activities. Notably, the Supreme Court recently affirmed social media's First Amendment pedigree, holding that "the most important place[ ] . . . for the exchange of views . . . is cyberspace – the 'vast democratic forums of the Internet' in general, and social media in particular."[53] Thus, to "foreclose access to social media altogether" would be to "prevent the user from engaging in the legitimate exercise of First Amendment rights."[54] In a similar vein, the Fourth Circuit has affirmatively held that both "likes" and comments on Facebook con-

51. *See, e.g.*, People v. Harris, 949 N.Y.S.2d 590, 595 (City Crim. Ct. 2012) *appeal dismissed*, 2013 WL 2097575 (N.Y. App. Term 2013) ("If you post a tweet, just like you scream it out the window, there is no reasonable expectation of privacy.").

52. *Knotts*, 460 U.S. at 278.

53. Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (quoting Reno v. American Civil Liberties Union, 521 U. S. 844, 868 (1997)).

54. *Packingham*, 137 S. Ct. at 1737.

stitute First Amendment-protected speech.[55] Could monitoring social media users in cyberspace thus trigger a viable First Amendment challenge? A circuit court case from 2015 suggests the answer could be yes. But to understand its significance, we first have to rewind nearly five decades.

Some forty-five years ago, in *Laird v. Tatum*, the Supreme Court considered a challenge to a large-scale data-gathering program in the U.S.[56] The Army had established this program in the late 1960s, in response to civil rights protests.[57] The Army collected "information about public activities that were thought to have at least some potential for civil disorder," reported it back to Army intelligence headquarters, and stored the data in a military data bank.[58] The information came from Army intelligence agents who attended public meetings, as well as from media sources and police departments.[59] By the early 1970s, facing Congressional pushback and stepped-up oversight of the Army's domestic surveillance programs, the Army reduced its efforts, including purging the records stored in the computer data bank.[60] The Under Secretary of the Army also represented to Senator Sam Ervin that the Army would be collecting information on a more limited category of events, would not be storing the reports in a computer, and would destroy the reports "60 days after publication or 60 days after the end of the disturbance."[61] This new regimen was intended to prevent the Army from "'watching' the lawful activities of civilians."[62]

The *Laird* majority concluded (over multiple strong dissents) that "the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose" does not unconstitutionally chill the lawful exercise of an individual's First Amendment rights.[63] The Court characterized the plaintiffs' challenge to the Army's program as a "disagree[ment] with the judgments made by the Executive Branch with respect to the type

55. Bland v. Roberts, 730 F.3d 368, 385, 388 (4th Cir. 2013) (holding that both "likes" and comments on Facebook constitute protected First Amendment speech).
56. Laird v. Tatum, 408 U.S. 1, 2 (1972).
57. *Id.* at 2.
58. *Id.* at 6.
59. *Id.*
60. *Id.* at 7.
61. *Id.* at 7–8.
62. *Id.* at 8.
63. *Id.* at 10.

and amount of information the Army needs" and an objection to "the very existence of the Army's data-gathering system."[64] With only "allegations of a subjective chill," and no showing of a "specific present objective harm or a threat of specific future harm"[65] – no denial of a professional affiliation, no loss of employment, no obligation to request government permission to send certain communications – there was no injury specific and direct enough to give the plaintiffs standing.[66]

Since *Laird v. Tatum* was handed down, it has generally been understood to stand for the proposition that a chilling effect isn't enough to get standing. But in *Hassan v. City of New York*, the U.S. Court of Appeals for the Third Circuit put an important gloss on *Laird*, holding that when *discriminatory* government surveillance dissuades individuals from exercising their rights, they can challenge the surveillance.[67]

Hassan involved the NYPD's surveillance of Muslim communities in New York and New Jersey after the 9/11 terrorist attacks.[68] The surveillance took a variety of forms, including the use of photography, video, license plate readers, surveillance cameras, and undercover officers; attendance at student group meetings and outings; and the monitoring and surveillance of mosques, bookstores, bars, cafes, and nightclubs.[69] The NYPD division conducting the surveillance produced documents reporting on mosques and the "ethnic composition of the Muslim community" in Newark, N.J.; lists of "businesses owned or frequented by Muslims;" information about flyers advertising tutoring in the Quran; and much more.[70] A group of individuals, organizations, and members of mosques or other associations named in the NYPD reports sued the NYPD after an Associated Press article revealed the existence and breadth of the program.[71]

The plaintiffs argued that the NYPD's surveillance program intentionally targeted Muslims, using visible indicia of religion (mosques, businesses with prayer mats) as well as "ethnicity as a proxy for faith."[72] Because of the stigma and the harm to their repu-

64. *Id.* at 13.
65. *Id.* at 13–14.
66. *Id.* at 11–12 (listing examples of concrete harms).
67. Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015).
68. *Id.* at 285.
69. *Id.*
70. *Id.* at 286–87.
71. *Id.* at 287, 292.
72. *Id.* at 286.

tations that followed the disclosure of the program and revelations that they were being surveilled by law enforcement, all of the plaintiffs suffered injury: the individual plaintiffs curtailed their worship and religious activities, including decreasing their mosque attendance and avoiding discussing their faith in public places, while organizational plaintiffs lost members and potential members, lost opportunities to collaborate with other organizations, and changed their programming to avoid attracting further NYPD attention.[73] Some also suffered financial harm, by losing customers or financial support.[74]

The Third Circuit swiftly dispatched the city's arguments that the plaintiffs lacked standing.[75] In response to the city's assertion that the plaintiffs hadn't suffered a real injury because the city had not "overtly condemned the Muslim religion," the panel pointed to *Brown v. Board of Education*, observing that the "'badge of inferiority' inflicted by unequal treatment itself" is a cognizable harm."[76] The fact that the surveillance affected a "broad class" – perhaps on the order of hundreds or even thousands of other people – did not dilute their injury; because the plaintiffs were "the very targets of the allegedly unconstitutional surveillance," they were "unquestionably 'affect[ed] . . . in a personal and individual way.'"[77] The court distinguished *Laird* on the grounds that the plaintiffs' objection here was not to the "*mere existence*" of *non*-discriminatory surveillance activity; instead, the NYPD's surveillance program was carried out in a "discriminatory manner" and caused "direct, ongoing, and immediate harm": namely, the very real impact on the plaintiffs' abilities to undertake their religious and other activities.[78] Because "*Laird* doesn't stand for the proposition that public surveillance is . . . *per se* immune from constitutional attack or subject to a heightened requirement of injury," those harms were sufficient to confer standing.[79] Indeed, a showing that surveillance is racially based, or is undertaken in retaliation for the exercise of First Amendment rights, is itself enough to bestow standing.[80]

73. *Id.* at 287–88.
74. *Id.* at 288.
75. *Id.* at 289.
76. *Id.* at 291 (citing Brown v. Bd. of Educ., 347 U.S. 483, 494 (1954)).
77. *Id.* (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 n.1 (1992)).
78. *Id.* at 292.
79. *Id.*
80. *Id.* (citing Hall v. Pa. State Police, 570 F.2d 86 (3d Cir. 1978) (holding that the state could not rely on racially based criteria in photographing "suspicious persons" entering a bank,

Because the plaintiffs cleared the standing hurdle, the panel conducted an initial assessment of their claims that the surveillance program had infringed their rights to equal protection under the Fourteenth Amendment and to freedom of religion under the First Amendment, to determine whether they had stated a sufficient claim to survive the city's motion to dismiss.[81]

On the equal protection claim, the plaintiffs had to allege (and eventually prove) not only that the NYPD surveilled more Muslims than members of any other religious faith, but that their religious affiliation was "a substantial factor" in the differential treatment.[82] To meet that standard, the plaintiffs could (1) identify a facially discriminatory policy; (2) identify a policy that was applied to Muslims "with a greater degree of severity than other religious groups;" or (3) identify a "facially neutral policy that the city purposefully designed to impose different burdens on Muslims and that has that detrimental effect (even if it is applied evenhandedly)."[83] The plaintiffs argued here that the NYPD's surveillance program expressly singled out Muslims for "disfavored treatment," and alleged enough specifics to survive.[84]

The court rejected the city's argument that even if the plaintiffs did plausibly allege a facially discriminatory policy, it was irrelevant because the city's more likely purpose was public safety, not religious discrimination.[85] As the court tartly noted, the city "wrongly assume[d] that invidious motive is a necessary element of discriminatory intent. It is not."[86] Discrimination can be intentional without being "motivated by ill will, enmity, or hostility"; critically, if the NYPD surveilled the plaintiffs only because they were Muslim, the fact that they may have been sincerely motivated by a legitimate law enforcement purpose was irrelevant.[87] The court observed that this would remain true "even where national security is at stake," emphasizing:

---

even if it could photograph *all* people entering the bank); Anderson v. Davila, 125 F.3d 148, 162 (3d. Cir. 1997) (observing that government retaliation in response to exercise of the "right to petition the government for grievances," a "protected activity under the First Amendment," is a "specific present harm" that gives rise to a justiciable claim)); *see also* House v. Napolitano, No. 11-10852-DJC, 2012 WL 1038816, at *11 (D. Mass. Mar. 28, 2012) (affirming that simply because a search is otherwise constitutional under the Fourth Amendment does not mean that government agents may "target someone for their political association").

81. Hassan v. City of New York, 804 F.3d 277, 294 (3d Cir. 2015).
82. *Id.*
83. *Id.* (citations and internal quotation marks omitted).
84. *Id.* at 295.
85. *Id.* at 297.
86. *Id.*
87. *Id.* at 298 (citations and internal quotation marks omitted).

"We have learned from experience that it is often where the asserted [governmental] interest appears most compelling that we must be most vigilant in protecting constitutional rights."[88]

This analysis informed the court's (far briefer) analysis of the plaintiffs' First Amendment claims, which survived as well.[89] As with the Equal Protection Clause claims, the court held, "allegations of overt hostility and prejudice are [not] required to make out claims under the First Amendment."[90]

How might this play out in the context of social media monitoring? Even *Laird* has a more sympathetic reading than is often acknowledged. First, while the Court doesn't explicitly rely on it, the fact that the Army's program had been significantly constricted by the time the matter was up for decision seemed to be of some consequence to the Court: the Court may have been particularly inclined to tread lightly on the First Amendment issues where the government's incursion into civilian political matters was in retreat anyway.

Second, the Court in *Laird* characterized the alleged chilling effect as "aris[ing] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individuals' concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual."[91] As Justice Douglas pointed out in dissent, even at the time that was a disingenuous description of the state of affairs:

> The present controversy is not a remote, imaginary conflict. Respondents were targets of the Army's surveillance. First, the surveillance was not casual but massive and comprehensive. Second, the intelligence reports were regularly and widely circulated and were exchanged with reports of the FBI, state and municipal police departments, and the CIA. Third, the Army's surveillance was not collecting material in public records but staking out teams of agents, infiltrating undercover agents, creating command posts inside meetings, posing as press photographers and newsmen, posing as TV newsmen, posing as students, and shadowing public figures. Finally, we know from the hearings conducted by Senator Ervin that the Army has misused or abused its reporting functions.[92]

88. *Id.* at 306–07.
89. *Id.* at 309.
90. *Id.*
91. Laird v. Tatum, 408 U.S. 1, 11 (1972).
92. *Id.* at 26–27 (Douglas, J., dissenting).

But even taking the majority's characterization at face value, the Court acknowledged that where the complainant is objecting to a specific exercise of governmental authority beyond "mere" surveillance, and where she is or will be subject to that governmental power, she may have a constitutional claim.[93] The Court cited to *Baird v. State Bar of Arizona*, in which a lawyer was prevented from joining the bar "solely because of her refusal to answer a question regarding the organizations with which she had been associated in the past."[94] The Supreme Court concluded in *Baird* that the government "may not inquire about a man's views or associations solely for the purpose of withholding a right or benefit because of what he believes."[95] Seen through this lens, if an individual's social media were surveilled on the basis of her associations or political beliefs and she were prosecuted for an unrelated offense as a result, or she were denied a housing or other civil benefit, that exercise of governmental authority would appear to confer constitutional standing.

Hassan and its sister cases sharpen the point even further. Under *Hassan*, a social media monitoring policy that is wielded against, for instance, Muslims or African-Americans "with a greater degree of severity than other . . . groups" may run afoul of the Fourteenth Amendment – and importantly, that holds true even if the surveillance was not motivated by "ill will, enmity, or hostility."[96] This is not a mere hypothetical; the Department of Homeland Security, for instance, was found to have directly monitored activity by Black Lives Matter protestors on Twitter.[97] And as detailed in Section A1, social media surveillance in many cities is likely to be disproportionately targeted at minority youth. Of course, the surveillance still has to inflict a concrete harm to be constitutionally cognizable. But if victims of the surveillance can point to concrete ways that it prevented them from exercising their First Amendment rights – for instance, if they pulled back on political organizing, activism, or communications – then they may have more in common with the potentially successful plaintiffs in *Hassan* than the disappointed ones in *Laird*.

93. *Id.* at 11.
94. *Id.* (citing Baird v. State Bar of Arizona, 401 U.S. 1 (1971)).
95. *Id.* at 11–12.
96. Hassan v. City of New York, 804 F.3d 277, 298 (3d Cir. 2015).
97. Jason Leopold, *Emails Show Feds Have Monitored 'Professional Protestor' DeRay Mckesson*, VICE (Aug. 11, 2015), https://news.vice.com/article/emails-show-feds-have-monitored-professional-protester-deray-mckesson; Lee Fang, *Why Was an FBI Joint Terrorism Task Force Tracking a Black Lives Matter Protest?* THE INTERCEPT (Mar. 12, 2015), https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/.

Anderson v. Davila offers useful guidance as well. In *Anderson*, a former employee of the Virgin Islands Police Department filed an EEOC claim and an employment discrimination lawsuit against his former employer; in response to – and, as Mr. Anderson alleged, in retaliation for – the complaints, the police department began intensively investigating him, including putting him under surveillance.[98] The Third Circuit had little trouble upholding the district court's injunction against the surveillance, observing that government retaliation in response to exercise of the "right to petition the government for grievances" – a "protected activity under the First Amendment" – is a "specific present harm" that gives rise to a justiciable claim.[99] Monitoring individuals on social media in retaliation for their First Amendment speech, including protesting government policies, would appear to fall squarely under the umbrella of *Anderson*.

B. Using an Informant, a Friend of the Target, or an Undercover Account to View Otherwise Private Information

When it comes to information not hosted on a public channel – for instance, a private Twitter account, or a Facebook account with reasonably robust privacy settings[100] – law enforcement officers still have several options for viewing information of interest. Officers or detectives can ask an individual who is virtual friends with the target, including an informant or cooperating witness, to view the target's posts, pictures, and more, and report back about what he or she has seen.[101] One fugitive, for example, was nabbed after posting comments and pictures on his Facebook page boasting about living the

98. Anderson v. Davila, 125 F.3d 148, 152 (3d Cir. 1997).

99. *Id*. at 160.

100. In 2012, Consumer Reports estimated that 13 million U.S. Facebook users did not understand or utilize privacy settings on Facebook. (As of January 2017, there were 214 million Facebook users in the United States.) *See 13 Million U.S. Facebook Users Don't Use Privacy Controls, Risk Sharing Updates Beyond Their "Friends"*, Consumer Reports (May 3, 2012), http://www.consumerreports.org/media-room/press-releases/2012/05/my-entry/.

101. The Department of Justice (DOJ) permits an FBI agent to use this tactic in furtherance of a criminal investigation if the same kind of communication would be authorized over the phone, and the NYPD permits officers to "access social network sites using an online alias" after completing a procedure and receiving approval. *The Department of Justice's Principles for Conducting Online Undercover Operations*, Public Intelligence (Mar. 22, 2012), https://publicintelligence.net/the-department-of-justices-principles-for-conducting-online-undercover-operations/; Operations Order 34: Use Of Social Networks for Investigative Purposes – General Procedure, New York Police Department (Sept. 5, 2012), https://s3.amazonaws.com/s3.documentcloud.org/documents/1657435/nypd-social-media-surveillance.pdf.

good life in Cancun.[102] His Facebook friends – who were publicly viewable on his profile – included a former Justice Department official living in the area.[103] The prosecutor pursuing the case, suspecting that he would be able to trust a Justice Department employee, reached out and asked him to dig up the fugitive's address, leading to the fugitive's arrest several months later.[104]

Law enforcement officers can also create undercover accounts to connect surreptitiously with unknowing civilians; indeed, several social media monitoring companies have advertised their ability to create undercover accounts in bulk.[105] Whether using a service or on their own, a number of jurisdictions are doing just this. For instance, the Cook County (Chicago) Sheriff's Office Intelligence Center encouraged sheriff's office intelligence analysts to set up fake accounts to collect information; presentation slides noted that doing so is prohibited by most of the platforms' policies, though not by law.[106] California Highway Patrol officers created Twitter accounts that did not identify them as law enforcement in order to monitor planned demonstrations.[107] Craftily, the Boston police department has used undercover accounts to try to smoke out underground music shows.[108]

As with use of social media monitoring tools generally, use of these technologies in the undercover context may disproportionately affect communities of color. An NYPD initiative, for example, allows detectives to send friend requests to juveniles who have committed

102. Alexandra Topping, *Fugitive Caught After Updating His Status on Facebook*, THE GUARDIAN (Oct. 14, 2009), https://www.theguardian.com/technology/2009/oct/14/mexico-fugitive-facebook-arrest.

103. *Id*.

104. *Id.*

105. *See*, *e.g.*, Geofeedia, e-mail message to Riverside Police Department (Oct. 20, 2015), http://www.aclunc.org/docs/20161011_geofeedia_twitter_instagram_riverside_pd.pdf (noting that "[t]here is no limit on how many fake accounts can be uploaded into the database [to see private users]").

106. George Joseph, *How Police Are Watching You on Social Media*, CITYLAB (Dec. 14, 2016), https://www.citylab.com/equity/2016/12/how-police-are-watching-on-social-media/508991/, (noting that analysts appeared to be compiling information from social media for "longer term retention, not just for 'situational awareness'"). Another detective reported using a fictitious Facebook profile to connect with a drug suspect; the suspect "checked in" regularly from various locations, enabling the detective to track and capture him. *COPS*, *supra* note 14, at 12.

107. James Queally, *CHP Chief Says Officer Aimed Gun at Protestors After Partner was Attacked*, LOS ANGELES TIMES (Dec. 11, 2014), http://www.latimes.com/local/lanow/la-me-ln-chp-officer-gun-demonstrators-20141211-htmlstory.html.

108. Luke O'Neil, *Boston Punk Zombies are Watching You!,* SLATE (Mar. 29 2013, 5:45 AM), http://www.slate.com/articles/news_and_politics/crime/2013/03/boston_police_catfishing_indie_rockers_cops_pose_as_punks_on_the_internet.html.

robberies.[109] The detectives typically befriend the participants – mostly black and Hispanic males – by using a fake avatar of a female teenager.[110] They are not allowed to interact directly with the teenagers, but they do "spend at least two hours daily monitoring the teenagers' chatter."[111] Notably, while the program is intended to prevent youth from committing additional crimes, it has not been shown to have any effect on reducing robberies, further heightening concerns about its focus on youth of color.[112]

To take another example, security staff at Minneapolis's Mall of America, working in coordination with the local city attorney's office, created undercover accounts on Facebook to build dossiers on activists involved in the Black Lives Matter movement.[113] The dossiers included pictures, timelines showing where to find the activists in various videos from the protest, and "information scraped from their social media accounts."[114] A number of the activists surveilled were organizers for a large protest at the Mall of America; after the protest, eleven of the participants were charged with criminal misdemeanors.[115]

And in a troubling federal incident, the Drug Enforcement Administration arrested a woman named Sondra Arquiett on drug charges, appropriated pictures of her and her minor children without her knowledge, and used them to create a Facebook profile. A DEA agent then used the profile without her permission to make friend requests in her name to wanted fugitives, essentially using her as the

109. Wendy Ruderman, *To Stem Juvenile Robberies, Police Trail Youths Before the Crime*, NEW YORK TIMES (Mar. 3, 2013), http://www.nytimes.com/2013/03/04/nyregion/to-stem-juvenile-robberies-police-trail-youths-before-the-crime.html.

110. *Id.*

111. *Id.*; *see also* Joseph, *supra* note 106 (quoting a retired NYPD detective sergeant explaining that "[r]equesting a friendship, as a policeman you have to be careful of that entrapment issue. But if you just put a half-naked picture of [a] woman in there, you're gonna get in.").

112. J. David Goodman, *Report Finds Juvenile Program Failed to Reduce Robberies, but Police Are Expanding It*, NY TIMES (Jan. 4, 2016), http://www.nytimes.com/2016/01/05/nyregion/report-finds-juvenile-program-failed-to-reduce-robberies-but-police-are-expanding-it.html?_r=0. Nevertheless, some perpetrators are nabbed by the program; *see, e.g.*, Oren Yaniv, *Cop Helps Take Down Brooklyn Crew Accused of Burglary Spree by Friending Them on Facebook*, NY DAILY NEWS (May 30, 2012), http://www.nydailynews.com/new-york/helps-brooklyn-crew-accused-burglary-spree-friending-facebook-article-1.1086892.

113. Lee Fang, *Mall of America Security Catfished Black Lives Matter Activists, Documents Show*, THE INTERCEPT (Mar. 18, 2015), https://theintercept.com/2015/03/18/mall-americas-intelligence-analyst-catfished-black-lives-matter-activists-collect-information/.

114. *Id*.

115. *Id.*

cover for his undercover activities.[116] Ms. Arquiett challenged the DEA's practice, arguing that the use of her personal data implicated her as a cooperator with the criminal investigation and put her in danger.[117] The DEA ultimately paid Ms. Arquiett $134,000 to settle her challenge.[118] While the DOJ pledged to review its tactics after this case came to light, the department has not yet updated its policies on online investigations.[119]

1. Policy and legal considerations

From a Fourth Amendment perspective, courts have generally permitted law enforcement agents to engage in undercover activities, both in real life and online, without getting a warrant or clearing some other judicial hurdle. This approach dates to the same era as *Laird*; the Supreme Court that constricted the grounds for a viable First Amendment claim also blessed the government's ability to solicit intimate information from a third party, be it an individual entrusted with the information based on a personal association or a company in a position to receive it because of a transactional relationship.[120] Emerging interpretations of the Fourth Amendment suggest that could change, though the case law has not yet caught up.

Thus, in *Hoffa v. United States*, union boss Jimmy Hoffa invited someone he believed to be a fellow union member into his hotel room and shared confidences with him.[121] His confidant, Edward Partin, turned out to be a government informant, who regularly shared details of their conversations with a federal agent and whose testimony at trial was a substantial factor in Hoffa's conviction for attempted bribery.[122] Hoffa argued that because Partin failed to disclose his true identity, Hoffa had not truly consented to having him in the hotel suite, and that by listening to Hoffa, Partin conducted an illegal search

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

117. *Id.*

118. 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-fake-facebook-profile-lawsuit-without-admitting-wrongdoing/.

119. Horwitz, *supra* note 116.

120. *See generally* United States v. Miller, 425 U.S. 435 (1976); Laird v. Tatum, 408 U.S. 1, (1972).

121. Hoffa v. United States, 385 U.S. 293, 296 (1966).

122. *Id.*

in violation of the Fourth Amendment.[123] The Court rejected this view, reasoning:

> Partin did not enter the suite by force or by stealth. He was not a surreptitious eavesdropper. Partin was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried on in his presence. [Hoffa], in a word, was not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing.[124]

The Court concluded: "Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[125]

Hoffa paved the way for the case that would help crystallize the modern-day third-party doctrine: the 1976 case *United States v. Miller*.[126] *Miller* involved the federal government's use of defective subpoenas to obtain copies of the bank records of one Mitch Miller, who was suspected of running an illegal whiskey distillery.[127] After Miller was indicted for conspiracy to defraud the government, he moved to suppress the records on the grounds that in the absence of a valid warrant, they had been illegally seized. In a cursory opinion, the Supreme Court held – relying on *Hoffa* – that:

> [T]he 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.[128]

While the opinion emphasized that the records were not "confidential communications" but "negotiable instruments," and that they related to "transactions to which the bank was *itself* a party"[129] – a fairly limited category of documents – the case has taken on the status of canon and now stands for the proposition that nearly any informa-

123. *Id.* at 300.

124. *Id.* at 302.

125. *Id.* Chief Justice Warren dissented, arguing that an "invasion of basic rights made possible by prevailing upon friendship with the victim is no less proscribed than an invasion accomplished by force." *Id.* at 314 (Warren, C.J., dissenting).

126. *See* United States v. Miller, 425 U.S. 435, 435 (1976).

127. *Id.* at 436.

128. *Id*. at 443 (citing United States v. White, 401 U.S. 745 (1971); *Hoffa*, 385 U.S. at 293; Lopez v. United States, 373 U.S. 427 (1963)).

129. *Id.* at 440-41 (emphasis added).

tion released to a third party, under almost any circumstance, is fair game for the government, in the absence of a statute putting it off limits.[130]

Thus, in one of the earliest appellate opinions to consider the police use of an online undercover identity, the Sixth Circuit held in *Guest v. Leis* (2001) that subscribers to an "online bulletin board system" had no legitimate expectation of privacy because they had voluntarily disclosed the information to the bulletin board's system operator.[131] A complaint about online obscenity had led police to investigate the bulletin board, the precursor to services like AOL and modern social-networking sites.[132] Using an undercover persona, officers accessed the system to view the allegedly obscene images; armed with that data, they submitted a request for a warrant to collect subscriber information such as names, email addresses, birthdates, and passwords.[133]

A class of subscribers challenged the collection of data on the ground that it was a search or seizure under the Fourth Amendment, requiring police to get a warrant first.[134] Citing to *Miller* for the proposition that "[i]ndividuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties"[135] – arguably a much broader holding than the Supreme Court actually reached in *Miller* – the court rejected the subscribers' claim concluding that no Fourth Amendment violation had occurred.[136]

---

130. In dissent, Justice Brennan quoted approvingly, and at length, from a unanimous decision by the California Supreme Court in a factually similar 1974 case, *Burrows v. Superior Court*. Burrows v. Superior Court, 529 P.2d 590 (Cal. 1974). Anticipating by many decades the modern-day Supreme Court's decisions in Jones and Riley, Justice Mosk observed: "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography." *Id.* at 596 (quoted in *Miller*, 425 U.S. at 451 (Brennan, J., dissenting)). Justice Mosk added that "judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by . . . new [electronic] devices." *Id.* (quoted in *Miller*, 425 U.S. at 452 (Brennan, J., dissenting)).

131. Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001).

132. *Id.* at 330.

133. *Id*. at 330, 335.

134. *Id.* at 330.

135. *Id.* at 335 (*Miller*, 425 U.S. at 443).

136. *Id.* at 336 (citing United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (holding that computer users do not have legitimate expectation of privacy in subscriber information because they have conveyed it to the system operator); United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000) (rejecting privacy interest in subscriber information communicated to internet service provider)).

Other courts have reached similar conclusions, holding that where a social media user shares photos and other information with "friends," even if those friends are actually government informants, they surrender any expectation that the information will be kept confidential.[137] A New York district court relied on *Guest* and *Katz* to hold in 2012 that sending information over the internet or via email "extinguished" the reasonable expectation of privacy that a user would otherwise have in the contents of his or her computer.[138]

In that case, *U.S. v. Meregildo*, the government used an informant who was Facebook "friends" with the target of their investigation to give the government access to his profile, a move that yielded information that ultimately led to the issuance of a search warrant.[139] The court acknowledged that a user's decision to activate privacy settings reflects his "intent to preserve information as private," and that the information shielded by the privacy settings could therefore be protected under the Fourth Amendment.[140] Nevertheless, the defendant's "legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those friends were free to use the information however they wanted – including sharing it with the Government."[141] Because the defendant "surrendered his expectation of privacy," the government's use of an informant to access his Facebook profile did not violate the Fourth Amendment.[142]

Notwithstanding this history, some cracks are starting to appear in the near-consensus around the breadth of the third party doctrine – most notably in *U.S. v. Jones*, the Supreme Court's 2012 case on location surveillance.[143] In *Jones*, the government attached a GPS tracker to the defendant's car without a warrant, and used it to track his location with granular accuracy for a month.[144] While Justice Scalia's majority opinion for the Court held that the attachment itself violated the

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

138. *Meregildo*, 883 F. Supp. 2d at 525.

139. *Id.*

140. *Id.*

141. *Id.* at 526; *accord* Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) (once Facebook information was voluntarily shared with a "friend," including a known government agent, the account holder had no reasonable expectation of privacy in the data).

142. *Meregildo*, 883 F. Supp. 2d at 526.

143. *See generally* United States v. Jones, 565 U.S. 400 (2012).

144. *Id.* at 403.

Fourth Amendment by virtue of being a trespass, it was the concurring opinions by Justices Sotomayor and Alito that continue to garner attention. In particular, Justice Sotomayor – responding to *Katz* and its progeny in the context of surveillance in public – suggested that it might be time to revisit the scope of the third-party doctrine, opining:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.[145]

Justice Sotomayor's admonition may be less salient in the social media arena, where data is often shared not only with a social media provider but with the world, making it hard to distinguish between lack of secrecy and lack of privacy. And she did not explicitly call into question the Court's informant doctrine, as developed in *Hoffa* and others. Nevertheless, as one brick falls in the third-party wall, more may follow. Notably, the Supreme Court is currently considering a case, *U.S. v. Carpenter*, that could reshape the third party doctrine for the digital age.[146]

Moreover, social media is susceptible to a particular type of deception that is nearly impossible in the real-world context. Partin may have been able to persuade Hoffa that he was a sympathetic fellow union member, to Hoffa's misfortune, but it would have been impossible to persuade Hoffa that he was, for instance, Hoffa's own brother; Hoffa would have the contrary evidence in front of him (which would also call into question Partin's other statements).

On the internet, however, as they say, no one knows you're a dog. An undercover agent could not only befriend an unwitting target but pretend to be someone who is actually known to the target in real life; if the agent is careful to build an authentic-seeming profile and is con-

145. *Id.* at 417–18 (Sotomayor, J., concurring).

146. United States v. Carpenter, 819 F. 3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402); Orin Kerr, *Third Party Rights and the Carpenter Cell-Site Case*, Wash. Post (June 15, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/15/third-party-rights-and-the-carpenter-cell-site-case/?utm_term=.2b3a839789d1.

fident the real person does not have a competing online profile, he could entice the target to share information that never would have been revealed without the intimate relationship the target thought they shared. And while it is certainly the case that even that intimate friend could disclose confidences to the government, carrying out the deception in cyberspace deprives the suspect of an opportunity she would otherwise have to assess the likelihood that her friend might betray her.

The notion that the Fourth Amendment must evolve to keep up with the digital age gained additional force in *Riley v. California*, involving the warrantless search of a cellphone incident to arrest, where Justice Roberts wrote for a unanimous Court:

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.[147]

Finally, on the First and Fourteenth Amendment side, the concerns detailed above apply with equal force when it comes to law enforcement using undercover accounts or other surreptitious monitoring techniques to target marginalized groups or inhibit the exercise of protected activity. As one appeals court has recognized, "the constitutionally protected right, [the] freedom to associate freely and anonymously, will be chilled" by disclosure of a protected association, regardless of whether the information is obtained from an informant or online friend.[148]

In short, while the Fourth Amendment in its current iteration offers police a significant degree of latitude to operate undercover, law enforcement is not entirely free to misbehave online.

147. Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).
148. In re First Nat'l Bank, 701 F.2d 115, 117–18 (10th Cir. 1983).

2. Law Enforcement and Company Policies

Notably, constitutional challenges are not the only mechanism for accountability; restrictions on undercover activity and the use of informants online may be more likely to come from some combination of agency policies and internal oversight mechanisms. In 2012, for instance, the NYPD released a set of guidelines governing the use of social networks for investigative purposes, including engaging in undercover operations online.[149] The policy requires supervisory approval for use of an online alias; where terrorist activity is suspected, the Intelligence Division is notified as well,[150] and where political activity is involved, the Intelligence Division must be involved and the Deputy Commissioner of Intelligence authorize the monitoring.[151]

Of course, policies are only as good as their enforcement. The NYPD's independent Inspector General (IG) found in 2016 that the department's Intelligence Bureau had repeatedly violated its own rules on investigations of political activity.[152] In half the cases the IG sampled, the NYPD had failed to provide a justification for continuing the cases; a quarter of the intelligence investigations continued for at least a month after their authorization had expired; and *no* case file properly explained why an undercover officer or informant was necessary, often simply transposing identical boilerplate language from one application to another.[153] In addition, this intrusive authority was deployed disproportionately against Muslims: more than 95% of the persons under investigation were "associated with Muslims and/or engaged in political activity that those individuals associated with Islam."[154] Strong internal guidelines must be matched by a robust departmental culture of compliance to be effective.

149. *NYPD Operations Order 34: Use of Social Networks for Investigative Purposes*, PUBLIC INTELLIGENCE (Oct. 13, 2013), https://publicintelligence.net/nypd-social-network-investigations/.

150. NEW YORK POLICE DEP'T, OPERATIONS ORDER 34: USE OF SOCIAL NETWORKS FOR INVESTIGATIVE PURPOSES – GENERAL PROCEDURE 1–2 (Sept. 5, 2012), https://s3.amazonaws.com/s3.documentcloud.org/documents/1657435/nypd-social-media-surveillance.pdf.

151. *Id.* at 4. *See generally* Handschu v. Police Dep't of New York, 241 F. Supp. 3d 433, 460 (S.D.N.Y. 2017) (setting out circumstances in which "undercover operations" are permitted).

152. *See* Rocco Parascandola & Greg Smith, *NYPD Repeatedly Broke Rules When Investigating Muslims Groups, Inspector General Report Charges*, NY DAILY NEWS (Aug. 24, 2016), http://www.nydailynews.com/new-york/nypd-broke-rules-probing-muslim-groups-inspector-general-article-1.2762445; OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY 1 (Aug. 23, 2016), http://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf.

153. Parascandola & Smith, *supra* note 152.

154. *Id.*

In the federal law enforcement realm, current DOJ policies on online undercover investigations allow agents to assume someone else's identity and communicate through it with that person's consent, as long as the communication would be otherwise authorized under relevant FBI rules. Using a person's online identity without consent, by contrast, is supposed to be done "infrequently and only in serious criminal cases."[155] These restrictions are somewhat porous: while a set of 2002 DOJ guidelines require a special agent in charge to approve "undercover operations" in advance, the agent may engage in a fairly extensive set of communications with the target before the interaction is treated as an undercover operation, allowing the agent to communicate undercover without approval or significant oversight for some time.[156]

Finally, companies' terms of service can be relevant too. When the Sondra Arquiett case became public, Facebook sent a strongly worded letter to the DEA, noting that impersonating another user online is a violation of its terms of service (though in practice, users appear to be able to choose a wide variety of names).[157] The company

155. *The Department of Justice's Principles for Conducting Online Undercover Operations*, PUB. INTELLIGENCE (Mar. 22, 2012), https://publicintelligence.net/the-department-of-justices-principles-for-conducting-online-undercover-operations/.

156. US DEPARTMENT OF JUSTICE, *Attorney General's Guidelines for FBI Undercover Operations* 1 (2002), http://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf. The guidelines explain that the approval process is not necessarily triggered by the first online communication, because there must be a series of activities over a period of time to rise to the level of an undercover operation, including at least "three substantive contacts" by the agent with the individual being investigated. A series of messages sent through social media could constitute just one discrete contact, "much like a series of verbal exchanges can comprise a single conversation"; higher-level approval therefore may not be required until the subject and the agent have communicated fairly extensively. *See also* ONLINE INVESTIGATIONS WORKING GROUP, ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENT 33 (Nov. 1999), https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf (interagency principles on online undercover operations, indicating that agents can use a fake name online in circumstances where they could do the same thing in "the physical world"). Notably, FBI agents can also establish fake websites to interact with the public, though there are no published reports of the agency having set up fake social media platforms. *See id.* at 42.

157. *Letter from Joe Sullivan to Drug Enforcement Administration Administrator Michele Leonhart*, FACEBOOK INC. (Oct. 17, 2014), https://www.documentcloud.org/documents/1336541-facebook-letter-to-dea.html; *see also Statement of Rights and Responsibilities*, FACEBOOK INC. (May 12, 2017), https://www.facebook.com/legal/terms; *What Names are Allowed on Facebook?*, FACEBOOK INC. (May 12, 2017), https://www.facebook.com/help/112146705538576?helpref=faq_content (noting that a user's Facebook name should be "the name your friends call you every day" and should match the name on his or her form of identification). In response to criticism over its "real name policy," Facebook loosened its requirements somewhat, permitting users to provide more information if they choose a different name under special circumstances (for instance, transgender people, Native Americans, and survivors of domestic violence). *See* Alex Hern, *Facebook Relaxes "Real Name" Policy in Face of Protest*, THE GUARDIAN (Nov. 2, 2015), https://www.theguardian.com/technology/2015/nov/02/facebook-real-name-policy-protest.

emphasized that law enforcement authorities are obligated to comply with these policies as well – though the Cook County Sheriff's Office presentation described above suggests that at least some law enforcement agencies consider adherence to corporate policies to be optional.[158]

C. Utilizing Analytical Software to Analyze Individuals' Locations, Associations, Political Affiliations, and More

The methods described above – while often invasive and potentially constitutionally problematic – largely do not require special expertise or tools. Little more is needed beyond a computer, an Internet connection, and perhaps a social media account. Far more sophisticated tools have been available through a suite of data analysis companies that offer the capability to automatically monitor online activity, conduct social network analysis, organize users by location, run keyword searches on social media postings, and more – most often on Twitter, but on Facebook and other social media platforms as well.[159]

It is worth noting that – as described in more detail below – the major social media platforms severely curtailed access by these services to their data for law enforcement and surveillance purposes in the fall of 2016, causing several of the data analytics companies to reduce in size or shutter entirely.[160] While law enforcement agencies are undoubtedly still using social media for surveillance, it appears that one of the routes to engage in large-scale monitoring and network

158. While there is a growing consensus that terms of service violations are over-used and abused to target average computer users under the Computer Fraud and Abuse Act (CFAA), platforms can use their terms of service to police the police without resort to the coercive tools in the CFAA. *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

159. *See, e.g.*, Victor Li, *Software Helps Assemble Social Media Posts From a Specific Event or Point in Time*, ABA J. (Feb. 1, 2017), http://www.abajournal.com/magazine/article/trial_drone_social_media_data (describing program that uses geolocation technology and data mining to "re-create an event by identifying everyone who posts publicly to social media at a given time and location"). This type of social media monitoring is turning into big business; a recent study by the Brennan Center for Justice, where I am an attorney, showed that police departments, cities, and counties across the country had spent close to $6 million on social media monitoring software, with the big spenders laying out hundreds of thousands of dollars each. *See also Map: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CTR. FOR JUST. (Apr. 5, 2017), https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties. This sum does not take into account the amounts spent by departments to do social media monitoring on their own or to buy a service other than the ones identified in the study; the overall figures are thus likely far larger.

160. *See infra* note 179.

analysis has been narrowed.[161] Regardless of recent developments, however, sophisticated data analysis of social media by law enforcement agencies is unlikely to be gone for good; one recent report, for instance, suggests that law enforcement agencies may still be able to purchase analytical products based on social media data even if they cannot access the data itself.[162]

Some companies also offer geo-tagging or geo-fencing, allowing law enforcement to monitor every post coming from a designated location in close to real-time, or to monitor all such tweets that mention a particular word for which an alert has been set.[163] Along with providing critical information for agencies responding to emergencies, this function could allow for easier monitoring of protests and other public events. The Toronto Police Service, for instance, used a monitoring service to track public sentiment during "large events and mass demonstrations" via publicly available information on Facebook and Twitter, including keywords and hashtags.[164] Instagram also collects a substantial amount of location information and makes it available to third parties; while developers can no longer market it for surveillance purposes, it is still likely to be available to the savvy law enforcement officer who is tracking an individual or group on his or her own.[165]

When a user accesses these apps on a cellphone without disabling the phone's location services function, the app may draw precise loca-

161. *See, e.g., We Have Discontinued Service for the BlueJay Twitter Monitor*, BRIGHTPLANET (May 12, 2017), http://brightplanet.com/bluejay/; *see also Capitalizing on The Power of The Deep Web*, 3I MIND (May 12, 2017), http://www.3i-mind.com/products/openmind/; *LexisNexis Launches New Social Media Investigative Solution for Law Enforcement*, LEXISNEXIS RISK SOLUTIONS (Oct. 15, 2013), http://www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1381851197735305; *see also* DIGITALSTAKEOUT, http://www.digitalstakeout.com/ (last visited May 12, 2017).

162. Aaron Gregg, *For This Company, Online Surveillance Leads to Profit in Washington Suburbs*, WASHINGTON 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=.a39bd2d13032.

163. *See, e.g.*, *Location-Based Intelligence*, DIGITALSTAKEOUT (May 15, 2017), https://www.digitalstakeout.com/use-cases/location-based-intelligence; *see also* G.W. Schulz, *Homeland Security Office OKs Efforts to Monitor Threats Via Social Media*, REVEAL NEWS (Nov. 15, 2012), https://www.revealnews.org/article/homeland-security-office-oks-efforts-to-monitor-threats-via-social-media/; Ali Winston, *Oakland Cops Quietly Acquired Social Media Surveillance Tool*, EAST BAY EXPRESS (Apr. 13, 2016), http://www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526; Phil Harris, *Social Media In the Time of Protest*, OFFICER (Mar. 16, 2016), http://www.officer.com/article/12155701/how-to-use-social-media-amidst-protests.

164. COPS*, supra* note 14, at 8.

165. *See, e.g.*, Jeff Reifman, *Using Social Media to Locate Eyewitnesses to Important Events*, TUTS+ (May 4, 2015), https://code.tutsplus.com/tutorials/using-social-media-to-locate-eyewitnesses-to-important-events—cms-23563.

tion information from the phone as well.[166] Notably, this is likely to disproportionately affect poor consumers, who are far more likely to use their phones rather than a computer or other device to go online.[167]

Finally, social media data can be incorporated into predictive policing programs, an algorithmic approach that purports to predict where crimes are going to happen or who is going to be a perpetrator or victim of a crime.[168] Hitachi, for instance, advertises a "predictive crime analytics" tool that combines social media information with other data, including license plate readers, gunshots sensors, historical crime data, weather, and more.[169] Another company (formerly called Intrado, now West) offers a software product called "Beware" that uses content from social media posts, along with a host of other data, to produce "threat scores" for individuals, a process that is opaque and highly susceptible to errors.[170]

166. When consumers access social media apps on mobile devices, the products collect location information via GPS, Bluetooth, Wifi, nearby cell towers, and even the device's gyroscope or accelerometer. It appears that the monitoring tools cannot extract this information if the user disables the location services function on his or her phone (at least with an iPhone), but they may still be able to derive it from other clues, including the content in the social media postings. *See, e.g.*, *Data Policy*, FACEBOOK INC. (May 12, 2017), https://facebook.com/policy.php (indicating that Facebook collects information about the locations of photos that are posted, and collects specific geographic location of devices using the app through GPS, Bluetooth, or WiFi signals); *see also Twitter Privacy Policy*, TWITTER INC. (May 12, 2017), https://twitter.com/privacy?lang=en (indicating that Twitter collects locations that are posted in profiles, Tweets or hashtags, and collects device location information in the same way as Facebook); *Privacy Policy*, INSTAGRAM, INC. (May 12, 2017), https://www.instagram.com/about/legal/privacy/ (indicating that Instagram collects geographical metadata via location tags or location data obtained through signals when the user has enabled location access); *Privacy Policy*, SNAP INC. (Apr. 12, 2017), https://www.snap.com/en-US/privacy/privacy-policy/ (noting that when location services are enabled by the user, Snapchat may collect precise location information using methods that include GPS, wireless networks, cell towers, Wi-Fi access and other sensors, including gyroscopes, accelerometers, and compasses; in addition, the policy notes without further elaboration that "when you use our services we may collect information about your location"); *About Privacy and Location Services in iOS 8 and Later*, APPLE INC. (Sept. 15, 2016), https://support.apple.com/en-us/HT203033 ("When Location Services are off, apps can't use your location in the foreground or background.").

167. Mary Madden et al., *Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 70 (2017) ("sixty-three percent of smartphones internet users who live in households earning less than $20,000 per year say they mostly go online using their cell phone, compared with just twenty-one percent of those in households earning $100,000 or more per year").

168. *See, e.g.*, Sean Captain, *Hitachi Says It Can Predict Crimes Before They Happen*, FAST COMPANY (Sept. 28, 2015), https://www.fastcompany.com/3051578/elasticity/hitachi-says-it-can-predict-crimes-before-they-happen.

169. *Hitachi Data Systems Unveils New Advancements In Predictive Policing To Support Safer, Smarter Societies*, HITACHI VANTARA (Sept. 28, 2015), https://www.hds.com/corporate/press-analyst-center/press-releases/2015/gl150928.html.

170. Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat "Score"*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-

Predictive policing itself has been the subject of sustained criticism on the grounds that it is opaque, disproportionately affects communities of color, replicates patterns of discriminatory policing, and is of debatable efficacy. Adding social media postings to predictive tools is likely to exacerbate the issue; social media is highly contextual, with likes, retweets, and even content notoriously difficult to interpret.[171] Even where perpetrators of major crimes have made elliptical online references to their intentions before the fact, it is not obvious how they could be accurately picked out of the sea of words in cyberspace, a dilemma that has been grudgingly acknowledged in the counterterrorism context as well.[172]

In recent years, reports of misuse of these monitoring and analytical tools have made headlines. In the spring of 2016, the Civil Rights Director of the Oregon Department of Justice filed a complaint asserting that a colleague at the department had used a social media monitoring tool, Digital Stakeout, to search for Twitter users referencing the #BlackLivesMatter hashtag.[173] Because he had used the hashtag, the director's Twitter account was flagged, and he was

---

new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.ed0553f1ca7b.

171. *See, e.g.*, *Twitter Joke to "Destroy America" Reportedly Gets U.K. Tourist Barred from US,* Fox News (Jan. 30, 2012), http://www.foxnews.com/travel/2012/01/30/twitter-joke-to-destroy-america-gets-tourists-barred-from-us.html (British travelers barred from entering United States after joking about on Twitter "destroying America"– British slang for partying). For a comprehensive critique of automated social media analysis tools, *see Mixed Messages: The Limits of Automated Social Media Content Analysis*, Ctr. for Democracy & Techn. (Nov. 28, 2017), https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.

172. *See, e.g.*, Angela Moon, *Oregon Shooting "Threat" May Have Circulated on Social Media*, Reuters (Oct. 2, 2015), http://www.reuters.com/article/us-usa-shooting-oregon-threats-idUSKCN0RV5W720151002; *Initiative: Social Media Behavior & Real-World Consequences*, Citizens Crime Commission of New York City (May 12, 2017), http://www.nycrimecommission.org/social-media-use-preceding-real-world-violence.php; Rachel Levinson-Waldman, Brennan Ctr. For Justice, What The Gov't Does with Americans' Data 16 (2013), https://www.brennancenter.org/sites/default/files/publications/What%20Govt%20Does%20with%20Data%20100813.pdf (quoting multiple officials' observations that one of the main obstacles to picking out critical national security information has been the overabundance of data); *see also* Faiza Patel & Rachel Levinson-Waldman, *Monitoring Kids' Social Media Accounts Won't Prevent the Next School Shooting,* Wash. Post (Mar. 5, 2018), https://www.washingtonpost.com/news/posteverything/wp/2018/03/05/monitoring-kids-social-media-accounts-wont-prevent-the-next-school-shooting/?utm_term=.92bfd7e2e2d4 (detailing the scant hard evidence on social media of intent to commit a school shooting before the fact).

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

deemed a "threat to public safety."[174] The Oregon Attorney General subsequently fired the investigator involved and demoted another official.[175]

That fall, the ACLU of Northern California revealed through public records requests that several online data analysis companies had marketed themselves to law enforcement agencies by touting their ability to track and follow lawful protestors, including at events in response to the killing of Michael Brown, gatherings using the hashtag #BlackLivesMatter, and more.[176] These capabilities were not merely an intriguing hypothetical: the Baltimore police used Geofeedia to monitor protests in the city after the death of Freddie Gray, and even identified and arrested protestors with outstanding warrants by running their pictures though a facial recognition system.[177] The City of Boston tested out a similar program at a large-scale music festival shortly after the 2013 Boston Marathon bombing; the program, which used facial recognition tools to monitor attendees, allowed "city representatives, Boston Police, and IBM support staff [to] watch in real time, all while simultaneously monitoring social media key words related to the event."[178]

Partially in response to the ACLU's disclosures and the resulting media coverage, several social media platforms took steps to limit the availability of their data to companies that were mining it for sale to law enforcement agencies. Shortly after the ACLU of Northern California disclosed its findings, Twitter and Facebook cut off access by several of the most high-profile companies to the platforms' streaming API, or application programming interface, which had allowed the

174. *See id.*; *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.

175. Dana Tims, *Justice Department Investigator Fired Over Black Lives Matter Profiling Scandal*, OREGON LIVE (Oct. 25, 2016), http://www.oregonlive.com/politics/index.ssf/2016/10/black_lives_matter_profiling.html.

176. Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, AM. C.L. UNION OF NORTHERN CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; *see also* Nicole Ozer, *Police Use of Social Media Surveillance Software is Escalating, and Activists Are in the Digital Crosshairs*, AM. C.L. UNION (Sept. 22, 2016), https://www.aclu.org/blog/free-future/police-use-social-media-surveillance-software-escalating-and-activists-are-digital.

177. Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016), http://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

178. Luke O'Nell, *Beantown's Big Brother: How Boston Police Used Facial Recognition Technology to Spy on Thousands of Music Festival Attendees*, NOISEY (Aug. 13, 2014, 12:00 PM) https://noisey.vice.com/en_us/article/6wm356/beantowns-big-brother.

companies to query social media data in real time.[179] In early 2017, Facebook and Instagram issued a statement "clarifying" that their policy does not permit developers to use their data for surveillance; public records requests regarding Department of Homeland Security access to social media for visa vetting purposes suggest that Facebook has stringently implemented those restrictions.[180]

1. Legal considerations

While courts have not yet ruled whether these kinds of algorithmic programs violate the constitutional rights of those being surveilled, aspects of these tools raise both First Amendment and Fourth Amendment issues. In the Fourth Amendment arena, recall *U.S. v. Knotts*. While the Supreme Court declared in *Knotts* that a police officer might observe someone walk or drive down a public street without getting a warrant, the Court also reasoned that "dragnet-type law enforcement practices" might raise more acute constitutional concerns.[181] Indeed, even in *U.S. v. Katz*, the Court observed that the Fourth Amendment "protects people, not places," and added

179. *Developer Agreement & Policy*, TWITTER, INC. (Sept. 30, 2016), https://dev.twitter.com/overview/terms/agreement-and-policy; *see also* Chris Moody, *Developer Policies to Protect People's Voices on Twitter*, TWITTER, INC. (Nov. 22, 2016), https://blog.twitter.com/2016/developer-policies-to-protect-people-s-voices-on-twitter; Ally Marotti, *Twitter Cuts Off Chicago Startup Geofeedia After ACLU Reports Police Surveillance*, CHICAGO TRIBUNE (Oct. 11, 2016), http://www.chicagotribune.com/bluesky/originals/ct-twitter-suspends-geofeedia-access-bsi-20161011-story.html; Colin Daileda, *Twitter Cuts Ties with Another Social Media Surveillance Company*, MASHABLE (Oct. 20, 2016), http://mashable.com/2016/10/20/twitter-social-media-surveillance-snaptrends/#1n5_wdk9k5qm; Dell Cameron & David Gilmour, *Twitter Cuts Off Third Surveillance Firm for Encouraging Police to Spy on Activists*, DAILY DOT (Dec. 9, 2016), https://www.dailydot.com/layer8/media-sonar-twitter-social-media-monitoring/; Dell Cameron, *Twitter Cuts Ties with Second Firm Police Use to Spy on Social Media*, DAILY DOT (Oct. 20, 2016), https://www.dailydot.com/layer8/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/; Billy Utt, *Snaptrends CEO Responds: No More Govt Surveillance*, AUSTININNO (Nov. 2, 2016), https://www.americaninno.com/austin/snaptrends-ceo-responds-no-more-govt-surveillance/; Jordan Pearson, *Facebook Banned this Canadian Surveillance Company from Accessing Its Data*, MOTHERBOARD VICE (Jan. 19, 2017), https://motherboard.vice.com/en_us/article/instagram-banned-this-canadian-surveillance-company-from-accessing-its-data-media-sonar.

180. *Facebook U.S. Public Policy*, FACEBOOK (Mar. 13, 2017), https://www.facebook.com/uspublicpolicy/posts/1617594498258356; *see also Platform Policy*, INSTAGRAM, INC. (Feb. 22, 2017), https://www.instagram.com/about/legal/terms/api/; Colin Lecher, *Facebook Updates its Platform Policy to Forbid Using Data for Surveillance*, CNBC (Mar. 13, 2017), http://www.cnbc.com/2017/03/13/facebook-bans-developers-from-using-data-for-surveillance.html; Sam Levin, *Facebook and Instagram Ban Developers from Using Data for Surveillance*, THE GUARDIAN (Mar. 13, 2017), https://www.theguardian.com/technology/2017/mar/13/facebook-instagram-surveillance-privacy-data; Aliya Silverstein, *Obama Team Did Some "Extreme Vetting" of Muslims Before Trump, New Documents Show,* DAILY BEAST (Jan. 2, 2018, 5:00 AM), *https://www.thedailybeast.com/obama-team-did-some-extreme-vetting-of-muslims-before-trump-new-documents-show*.

181. United States v. Knotts, 460 U.S. 276, 284 (1983).

that what a person "seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected."[182] Taken together, these and a set of more recent cases stand for the proposition that the accumulation and retention of a large quantity of personal information implicates Fourth Amendment rights – even if that information is technically available to the public.

Take, for example, *U.S. v. Jones*, in which a police officer attached a GPS tracker to a car without a warrant and used it to collect highly detailed information about the driver's location over the course of a month.[183] When the evidence came out in the course of a criminal case against him, he asked the court to throw it out, arguing that its warrantless collection violated his Fourth Amendment rights.[184] While Justice Scalia's 2012 majority opinion relied on the fact that the simple act of attaching the device without a warrant violated the Fourth Amendment's prohibition on trespass, five justices writing separately indicated that the device's collection of a large quantity of sensitive data, at extraordinarily low cost, gave them pause as well.[185] Justice Sotomayor emphasized that GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,"[186] a capability that Justice Alito described as at odds with "society's expectation . . . that law enforcement agents and others would not – and . . . simply could not – secretly monitor and catalogue every single movement of an individual's car for a very long period."[187] It is not hard to imagine that the analysis of a wealth of online data, used to extract information that would not otherwise be visible to the average observer, would raise similar concerns.

Similarly, the Court recently ruled that law enforcement generally must get a warrant before viewing their contents of modern-day cell phones, highlighting the ways in which the quantity and diversity

182. Katz v. United States, 389 U.S. 347, 351 (1967) (emphasis added).

183. United States v. Jones, 565 U.S. 400, 403 (2012).

184. *Id.* at 404.

185. *Id.* at 416.

186. *Id.* at 415–16 (Sotomayor, J., concurring) (adding that "because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices").

187. *Id.* at 430 (Alito, J., concurring) (opining that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

of information they hold could enable an observer to extrapolate any number of details about the user's life:

> Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on . . . . The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.[188]

The Court's sensitivity to the constitutional significance of an accumulation of data, even where discrete pieces may individually be public, suggests that the justices may also be attentive to the transformation of publicly available information such as social media posts into much more detailed insights about location, associations, and more.[189]

Finally, many of the First Amendment issues raised above come into play here as well and are even magnified. Katherine Strandburg, who has written extensively about the First Amendment implications of using data analysis techniques on social networks, has emphasized that this type of data mining, used to infer who is connected and how (rather than to elicit the *content* of their communications), "poses a serious threat to liberty because of its potential to chill unpopular, yet legitimate, association."[190] She thus suggests that the First Amendment right to freedom of association must offer "an additional check, distinct from the Fourth Amendment's protections from unreasonable search and seizure," on surveillance of associations.[191]

---

188. Riley v. California, 134 S. Ct. 2473, 2489 (2014).

189. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World*, 49 B.C. L. Rev. 741, 800 (2008) (noting, in the context of *Kyllo v. United States*, that "[i]n the case of relational surveillance of traffic data, network analysis produces knowledge which, like the thermal image in *Kyllo*, is embedded in the data, yet not available without applying the technology. The Court in *Kyllo* specifically rejected the proposition that an investigating tool that was a means of processing data rather than collecting it could not constitute a search.").

190. *Id.* at 794.

191. *Id.* at 748–49. Strandburg goes on to recommend that any program of "relational surveillance" would need to meet a strict scrutiny standard," meaning that it must "serve a legitimate and compelling government interest and its methodology must be sufficiently accurate and narrowly tailored to that interest in light of the extent to which it is likely to expose protected expressive and intimate associations." *Id.* at 748–49. The focus of the inquiry would be on the likelihood that even a single occasion of the surveillance would "disclose membership in expressive associations," as well as on its "susceptibility to misuse as a means to target unpopular organizations or political opponents" – dangers that are omnipresent in the context of social media surveillance. *Id.* at 802–03.

CONCLUSION AND RECOMMENDATIONS

Social media has helped spark protests and even revolutions across the globe, from protests in Ferguson, MO, after the shooting of Michael Brown, to Women's Marches across the globe after President Trump's inauguration, to uprisings in Egypt to Turkey.[192] It has become an extraordinary organizing tool that has allowed movements to take shape and change the national and international landscape at unprecedented speed.[193] Indeed, it is an irreplaceable forum for communication of all kinds – personal, political, artistic, and more.[194]

In light of this wealth of information, it is no surprise that law enforcement agencies and other government entities have found Facebook, Twitter, Instagram, and other social media sites to be rich sources of data to mine for a variety of purposes. To be sure, much of the information on social media is public by design – it is precisely that public nature that makes it so valuable. But its public nature does not render it either constitutionally defenseless or undeserving of protection through policy.

This Essay has suggested some ways that the First, Fourth, and Fourteenth Amendments could be brought to bear to constrain unfettered law enforcement access to social media. In the meantime, some policy prescriptions would help relieve the pressure while the courts are working through these challenges.

(1) Publicly Available Policies and Practices. A 2016 study by the Brennan Center revealed that of the 150+ police departments that

192. Erin Carson, *How Facebook, Twitter Jumpstarted the Women's March,* CNET (Apr. 20, 2017, 3:46 PM), https://www.cnet.com/news/facebook-twitter-instagram-womens-march/; Sam Gustin, *Social Media Sparked, Accelerated Egypt's Revolutionary Fire*, WIRED (Feb. 11, 2011, 2:56 PM), https://www.wired.com/2011/02/egypts-revolutionary-fire/; Selena Larson, *Facebook is Playing an Increasingly Important Role in Activism*, CNNtech (Feb. 17, 2017, 12:38 PM), http://money.cnn.com/2017/02/17/technology/womens-march-facebook-activism/index.html; Carlos Lozada, *Twitter and Facebook Help Spark Protest Movements. Then They Undermine Them.,* WASH. POST (May 25, 2017), https://www.washingtonpost.com/news/book-party/wp/2017/05/25/twitter-and-facebook-help-spark-protest-movements-then-they-undermine-them/?utm_term=.80ae40fc337e; *They Helped Make Twitter Matter in Ferguson Protests*, N.Y. TIMES (Aug. 10, 2015), https://www.nytimes.com/2015/08/11/us/twitter-black-lives-matter-ferguson-protests.html.

193. Bijan Stephen, *Social Media Helps Black Lives Matter Fight the Power*, WIRED (Nov. 2015), https://www.wired.com/2015/10/how-black-lives-matter-uses-social-media-to-fight-the-power/.

194. Homero Gil de Zúñiga, Logan Molyneux, & Pei Zhang, *Social Media, Political Expression, and Political Participation: Panel Analysis of Lagged and Concurrent Relationships*, 64(4) J. COMM. 612 (2014); Elizabeth Kulze, *Instagram is Now One of the Most Common Forms of Artistic Expression,* VOCATIV (Jan. 13, 2015, 4:43 PM), http://www.vocativ.com/culture/art-culture/instagram-artists/index.html.

used social media monitoring software, only eighteen had publicly available policies detailing how social media is used for investigative or intelligence purposes. All law enforcement agencies engaging in social media monitoring – whether through third-party analytic tools or more focused efforts – should have a publicly available policy describing their use of social media. The policy should detail (1) who is authorized to access social media, (2) how the information obtained may be used, (3) how long it is stored, (4) with whom it may be shared, (5) the protections in place to protect privacy, speech, and association, and (6) what training is provided to officers or detectives who access social media as part of their law enforcement work. It should also set out mechanism and schedule to conduct publicly available audits of the department's use of social media.

(2) Safeguarding of Constitutional Values. The policy should specify that law enforcement agents may not target people on the basis of impermissible factors, including First Amendment-protected speech and membership in a protected category, such as race, religion, or ethnicity. The provisions of the Handschu Agreement, the product of a lawsuit against the NYPD for engaging in discriminatory surveillance, may be helpful in this regard.[195] The Handschu agreement states, among other things, that investigations should "not be based solely on activities protected by the First Amendment" and "[should] not intrude upon rights of expression or association in a manner that discriminates on the basis of race, religion or ethnicity."

(3) Use of Undercover Accounts or Personas on Social Media. Law enforcement should use undercover online personas with extreme caution. As in the real world, an officer should engage in undercover interactions only during a predicated investigation, only where no less intrusive means are available, and only where the information sought could not be obtained through other methods. This condition could be given teeth by requiring the officer to demonstrate these facts to

195. *See, e.g.*, *Revised Settlement Enhances Protections From Discriminatory NYPD Surveillance of American Muslims*, N.Y.C.L. UNION (Mar. 6, 2017), https://www.aclu.org/news/revised-settlement-enhances-protections-discriminatory-nypd-surveillance-american-muslims. Among other things, the Handschu agreement states that investigations should "not be based solely on activities protected by the First Amendment" and "[should] not intrude upon rights of expression or association in a manner that discriminates on the basis of race, religion or ethnicity." Revised Handschu Guidelines § II, Handschu v. Special Servs. Div., No. 71-cv-2203 (CSH) (S.D.N.Y. Mar. 13, 2017), https://www.clearinghouse.net/chDocs/public/NS-NY-0005-0005.pdf.

the prosecutor's office in his or her jurisdiction and to obtain an opinion approving their use or confirming that the information sought will contribute materially to prosecuting the case. Online undercover work must also be closely monitored to safeguard the safety and privacy of third parties who might unsuspectingly interact with the undercover officer.

The Handschu agreement may be useful in this context as well. The agreement specifies that requests to use undercovers or confidential informants must "be in writing and must include a description of the facts on which the investigation is based and the role of the undercover," with time limits on how long an undercover or informant may be used.[196] The agreement also prohibits undercover officers from "engaging in any conduct the sole purpose of which is to disrupt the lawful exercise of political activity, from instigating unlawful acts or engaging in unlawful or unauthorized investigative activities."[197]

(4) Prohibitions on Monitoring Juveniles. Finally, in light of rules preventing law enforcement officers from interviewing minors without notifying their parents, officers should be prohibited from connecting with juveniles online, whether undercover or not.

These policies would go a significant way towards establishing practical, workable guardrails around access for law enforcement purposes while ensuring that social media continues to play a rich, catalyzing role in modern-day communications and organizing.

196. §§ VII(3)(a)(i), VII(3)(a)(ii).
197. § VII(3)(a)(iii).