Social Media Surveillance and Law Enforcement

10.27.2015

ALEXANDRA MATEESCU, DOUGLAS BRUNTON, ALEX ROSENBLAT, DESMOND PATTON, ZACHARY GOLD, and DANAH BOYD

Introduction[1]

Law enforcement monitoring of social media is a widespread and growing practice. In 2014, a vendor's online survey of more than 1,200 federal, state, and local law enforcement professionals found that approximately 80 percent used social media platforms as intelligence gathering tools.[2]

The adoption of these new tools may not come as a surprise given their low cost compared to other forms of surveillance. But their adoption also reflects a broader trend: law enforcement's response to public pressure to investigate crimes online. For example, after a number of highly publicized violent attacks — from the Boston Marathon bombing, to the killing of churchgoers in Charleston, to mass shootings on school campuses – journalists have unearthed social media profiles full of warning signs: posts about hate, weapons, and more. Those discoveries have contributed to mounting pressure on law enforcement to do more to identify potential offenders before they act.

And there are some successes: social media data has helped law enforcement solve murder cases where perpetrators boast of their crimes online,[3] detect potential human trafficking activity[4], as well as more mundane crimes such as car thefts.[5]

But certain law enforcement uses of social media have raised questions. Debates so far have focused on instances where law enforcement have used social media tools to monitor peaceful protests,[6] assembled potentially innocuous social media activity as evidence for criminal conspiracy charges,[7] or created fake profiles or impersonated individuals online.[8] And because social media dramatically reduces the cost of police surveillance, it breathes new life into longstanding concerns over potentially disproportionate law enforcement focus on people of color, religious minorities, and low-income communities.[9] More broadly, there is increasing scrutiny over how social media surveillance affects First Amendment rights, which protect free speech, and

Fourth Amendment rights, which protect against unreasonable search and seizure by the government.

How law enforcement uses social media

The relationship between law enforcement agencies and social media has changed significantly in the last ten years. More often than not, law enforcement officers are doing their work manually, perusing public profiles, doing searches on various sites, or creating profiles to connect with targets of interest. But as Internet penetration, social media usage, and mobile device usage have all increased, law enforcement agencies and technology vendors alike have begun focusing on new forms of training and technology, including systems that would automate social media surveillance activities.

Today, law enforcement agencies employ social media for a wide range of reasons; respondents to the 2014 LexisNexis survey cited strategies such as discovering criminal activity and obtaining probable cause for a search warrant, collecting evidence for court hearings, pinpointing the location of criminals, managing volatile situations, witness identification, and broadcasting information or soliciting tips from the public.[10] Investigative uses of social media are either targeted – focusing on individuals and their networks – or general – concentrating on monitoring a delimited geographic area – either for identifying specific incidents or producing predictions of criminal risk.

Sources of intelligence can include publicly accessible posts shared by users who have not limited their privacy settings, information obtained by accessing a user's social network (e.g. adding a criminal suspect as a "Friend" on Facebook to view private posts), or the use of a search warrant to obtain a user's private communications from social media platforms themselves.

How social media platforms enable surveillance

Some social media platforms are more amenable to monitoring than others. Factors like default privacy settings play a role in the visibility of users' online speech to law enforcement.

Additionally, sites like Facebook make social networks visible beyond their immediate circles. These features raise new questions about how social media monitoring and law enforcement investigative practices on the ground intersect and shape each other.

Law enforcement uses the tools at their disposal to help identify networks of criminal activity. In 2014, for example, police in Cleveland were able to crack down on the Heartless Felons gang after a rapper affiliated with the gang posted videos on YouTube where he seemingly admits to

selling drugs.[11] This was possible through observing a visible nexus between the individuals, their social network, and the crime committed. But such connections are often unclear in the decontextualized space of social media, where specific social cues, figurative speech, and offline dynamics make meaning very difficult to parse.

Social media also shifts the boundaries of what counts as private and public space, generating anxieties about the very visible and permanent nature of social media activity. Given the history of disproportionate surveillance among people of color by law enforcement through practices such as profiling and heightened presence of police in minority---dominant urban neighborhoods, it is important to ask what is new and different about social media that may risk exacerbating these inequalities. For instance, social media creates permanent and public archives of people's lives[12] in ways that can come back to haunt individuals. One example of this arose out of the New York Police Department's Operation Crew Cut, which used social media to crack down on teen "crews," largely over concerns that they were settling turf disagreements through gun violence.[13] The NYPD considers "crews" to be proto-gangs and tracks more than 300 of them, but crews can also be a building- or neighborhood-based group of friends or clique without any criminal connection. One story that drew media attention was that of Asheem Henry and his younger brother Jelani, who had been part of a small teen "crew" beginning at ages 13 and 12. After pleading guilty to a weapons possession charge and doing five years' probation, Asheem had made an effort to leave his past associations behind and enrolled at William Patterson University in New Jersey. But when the NYPD began its crackdown on teen crews, Facebook photographs of him and his brother, dating back to when they were 14 or 15, were part of the evidence used to prove their association with the crew, alongside the past gun charges in Asheem's case. Asheem was arrested and charged with third degree conspiracy. Five months later, prosecutors charged his younger brother Jelani with attempted murder in another case, and, with only two conflicting eye witness identifications to support the charge, used Jelani's Facebook "likes" and other social media connections to his brother's crew to pressure Jelani to accept a plea deal. The District Attorney's office placed Jelani in Riker's Island jail and delayed his trial for 19 months, but Jelani maintained his innocence until, finally, the judge dismissed the case.[14] Examples like these raise questions about how social media not only presents a new space for surveillance, but also changes the dynamics of policing itself.

The market for third-party monitoring tools

The proliferation of stand-alone technical products offered by third-party vendors has made possible new investigative practices and surveillance strategies. Some products marketed to law enforcement today were initially designed for commercial or journalistic use. For example, SAS's TextMiner promises to discover underlying themes and concepts of text in order for businesses to analyze customer comments online,[15] but the product and others like it are now being adopted by local law enforcement.[16]

A common type of web surveillance tool allows law enforcement to conduct automated and continuous monitoring of day-to-day online activity, with the aid of algorithms designed to capture words and phrases designated as trigger words on sites like Twitter, Facebook, and Instagram. BlueJay software, made by BrightPlanet, touts the capacity to monitor high profile events and illicit activities, aiding in the collection of incriminating evidence.[17] OpenMIND advertises the ability to run lead-based investigation into the "deep web" – inaccessible to search engines but available through their software.[18] LexisNexis offers Social Media Monitor, which provides keyword, geographic, and individual targeted searches for investigations such as gang violence, drug dealing, crimes against children, and human trafficking.[19]

Another important feature of some monitoring tools is the ability to connect social media activity to location. Companies like Geofeedia offer products that use the location data of social media posts, when available, and map them. Using these maps, clients are able to specify a delimited geographic area and view all geotagged posts coming from that location in near real-time.[20] Use of geotagging features to map social media activity has been touted as a crucial tool in assisting first responders in emergencies,[21] as well as surveilling areas of concentrated activity, such as concerts or public protests.

Finally, some products are designed for preemptive action, incorporating social media data into predictive policing. Currently, a tool developed by the company Hitachi is being tested on a trial basis in various U.S. cities beginning in October 2015, which will incorporate social media activity, alongside other data, to identify geographic concentrations of online speech that may indicate issues like flaring neighborhood tensions.[22]

Training and policy

The growing market for increasingly efficient and far-reaching web surveillance tools has outpaced our understanding of how they are transforming policing. While more police forces are starting to incorporate social media data into their investigations, law enforcement personnel are primarily self-taught in their usage of social media.[23] Police departments often have policies regarding social media use by law enforcement officers themselves, such as what kinds of images they can share and other codes of conduct for personal use, but there is a growing need for policies governing use of social media for investigations.[24] In the 2014 survey conducted by LexisNexis, only 9% of officers indicated that they had received formal social media training at their agencies.[25] Moreover, 52% of the law enforcement agencies surveyed had no policy in place for the use of social media for investigative purposes,[26] and industry actors report that they are working without case law to guide their efforts.[27]

As a result, there is a considerable lack of clarity around various practices, which have led in the past to lawsuits and the violation of people's rights. One salient example is the practice of creating

fake online personas and impersonating actual persons to further investigations. In one case, the Drug Enforcement Administration created a decoy Facebook profile using the actual identity of Sondra Prince – an individual arrested on drug charges in 2010 – without her express consent, in order to investigate a drug ring.[28] However, Prince sued the government and eventually settled her lawsuit for $134,000.[29] But the questions her lawsuit raised over the nature of consent in online surveillance remain unresolved. Moreover, questions still linger even in cases where law enforcement do obtain consent from individuals to impersonate them online. The terms of service and policies for many social media platforms, like Facebook or Instagram, explicitly ban law enforcement from creating fake identities on their service. In such cases, law enforcement policies are often nonexistent or outdated. For example, though the ACLU recently obtained a copy of the DEA's consent form ("Consent to Assuming Online Identity: Adult Consent"), it was fifteen years old and outdated in its formulation.[30]

Some initiative has been taken to develop policies and transparency around practices. The International Association of Chiefs of Police (IACP), for example, has established a Center for Social Media in partnership with the Bureau of Justice Assistance, Office of Justice Programs, and the U.S. Department of Justice,[31] which provides access to a survey on law enforcement's use of social media,[32] a primer for such agencies' establishing a social media presence,[33] as well as a list of key elements of a social media policy.[34] What follows is a general, but not exhaustive, overview of some of the emerging issues that may shape policies around social media in the future.

Social media surveillance and protest

Social media monitoring has been touted as an important element of what the Department of Homeland Security (DHS) has defined as "situational awareness," an active awareness of the surroundings and possible threats thereof, made possible through monitoring social media feeds about events in localized geographies.[35] Response and recovery efforts during Hurricane Sandy in 2012 proved the utility of large-scale online monitoring during exigent circumstances.[36] However, concerns have emerged over these practices in the context of law enforcement, such as federal surveillance of protests on social media.[37] Such tactics raise questions about the impact of social media surveillance on free expression and Fourth Amendment rights.

Documents show that DHS monitored the #blacklivesmatter hashtag on Twitter during lawful protests across the country. The movement arose following the acquittal of George Zimmerman in the shooting death of Trayvon Martin and has grown in response to other recent police shootings of black men and women. Other documents show that DHS monitored the social media activity of prominent #blacklivesmatter activists, such as DeRay McKesson.[38] In these efforts, DHS has been collecting real-time, content-rich video, photo, and status updates across Facebook, Twitter, Vine, and Instagram to enhance its "situational awareness."[39] Though a 2013 privacy impact statement by DHS claimed that their National Operations Center does not engage

in "monitoring of First Amendment protected activities for public dissent," questions remain about the Fourth Amendment protections for public speech.

The Fourth Amendment restricts government searches and seizures where individuals have a reasonable expectation of privacy. Historically, those protections have not prevented law enforcement from observing what happens in public, including posts on social media.[40] But existing Fourth Amendment doctrine may not satisfactorily address large-scale law enforcement surveillance of public speech on social media. The ability to cheaply monitor huge quantities of public information raises an important legal question: Do low-cost, largely scalable surveillance technologies deserve their own constitutional limits? If so, what would those limits look like? Kevin Bankston and Ashkan Soltani offer one potential, rough rule of thumb: "if the new tracking technique is an order of magnitude less expensive than the previous technique, the technique violates expectations of privacy and runs afoul of the Fourth Amendment."[41]

Challenges in context and interpretation

Interpreting behavior on social media is a difficult task for anyone. Without a doubt, inaccurate interpretations of social media data are not unique to law enforcement, but the consequences in a criminal justice context can be uniquely severe. On most social media sites like Facebook and Twitter, individuals construct public or semi-public profiles where they not only interact with their friends, but also with their networks of friends.[42] Interpreting those social media interactions can be challenging for a number of reasons. One is "context collapse," a feature of online communication where messages intended for a limited audience become misconstrued for a wider audience once original context is lost.[43] There is also a limit to what can be extrapolated from social media activity – it only reflects a cross-section of people's lives, and in the absence of the physical cues that frame face-to-face interactions, messages can be interpreted incorrectly. For example, flashing a gang sign on Facebook may be a way to joke with friends, proclaim solidarity or neighborhood affiliation, or harmless posturing. Sociologists have noted that many youth who live in violent neighborhoods may project a tough image or follow a "code of the street" in their community in order to stay safe and be protected.[44]

But for law enforcement these types of messages can be confounding. Is an individual who posts about drugs and violence on social media actually engaging in those activities? One worry is that a lack of training for and understanding by investigators about what they are seeing online could lead to the criminalization of innocent individuals – particularly minors. And that fear is rooted in past practice: the NYPD's online surveillance under Operation Crew Cut, for example, included monitoring of black children as young as 10 years of age.[45]

The high visibility of young people and their activities on social media also complicates surveillance and interpretation of online speech. According to a 2015 Pew Research Survey, 90%

of young adults (ages 18 to 29) are active on social media,[46] and another Pew study found teens (ages 13 to 17) are active across a wide variety of social media platforms.[47] As a result, one concern is the potential overcriminalization of youth, particularly minority youth. Some surveillance products, like LifeRaft, are designed to detect 'cyberbullying' and school-related threats such as potential school shootings, by monitoring social media feeds and delivering automated alerts to the mobile devices of school administrators and law enforcement.[48] On the one hand, monitoring youth on social media can provide opportunity for intervention. Researchers at MIT and Columbia University have worked to find ways to detect cases of gang-related violent threats over social media in order to reach out to youth before those threats are acted upon.[49] But there is also potential for abuse and misunderstanding that can exacerbate existing practices of institutional discrimination and excessive disciplinary action. Today, many public schools have zero-tolerance policies, which increasingly rely on police action to handle student disciplinary issues, creating what has been called the "school-to-prison pipeline."[50] Moreover, schools are more likely to disproportionately apply serious disciplinary action and referrals to law enforcement against African American and Hispanic students.[51]

Social media evidence and accuracy

Surveillance technologies can grant an air of objectivity to assessments that are not necessarily indicative of realities on the ground, due to outdated, inaccurate, or incomplete information. For example, it is not always possible to trace a social media posting back to an individual, given the existence of fake and shared online accounts.[52] Moreover, ephemeral details become permanent records that individuals are not always able to redress in retrospect.

Inaccurate or incomplete information poses significant problems for surveillance technologies, like the online monitoring application Beware. Beware scans commercial and public databases, as well social media activity, in order to assign individuals a "threat rating." That rating is then sent directly to a police officer, whose actions will naturally be informed by the threat assessment. But officers are left in the dark as to the various data points actually factored into the score. Similarly, individuals are unable to see or contest their "threat rating," or to correct errors in cases of mistaken identity.[53]

These concerns are also relevant where social media surveillance is beginning to inform predictive policing tools. For example, the predictive tool developed by Hitachi, factors social media activity into its forecast of criminal activity.[54] However, it is unclear how, if at all, the tool addresses risks of bias, such as in the patterns of language that it flags as suspicious. Absent careful review, machine learning techniques applied to social media could easily reinforce existing patterns of enforcement, which partly reflect a disproportionate focus on people of color. To the extent that they replace human discretion, these automated systems may be trading individual bias – malicious or otherwise – for a new, systematic bias.

Legal questions for social media surveillance

Social media surveillance of law enforcement clearly raises a number of legal questions. Historically, Fourth Amendment protections have not limited law enforcement from observing what happens in public. But the digital dynamic at play may not be that simple. For example, large-scale law enforcement surveillance of social media during protests – and that of Black Lives Matter activists – raises a concern of scale and proportionality. In a concurring opinion in United States v. Jones, Justice Alito wrote that, "in the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[55] Today, large-scale and low-cost technologies have changed what law enforcement are capable of. As Kevin Bankston and Ashkan Soltani argue, that new dynamic is constitutionally significant, and might deserve its own constitutional limits.[56]

Similarly, the use of a person's social media network as evidence of a crime raises its own set of legal concerns. Law enforcement will continue to use social media to surveil individuals – including juveniles – before they have an actual criminal record. Given that, what type of social media activity is likely to constitute sufficient evidence of criminal activity? For prosecutors, what type of social media activity should be allowed as evidence when a person is charged under conspiracy statutes? Are there certain social media attributes – like a person's social network – that should not be considered as evidence?

Impersonation online raises its own set of legal considerations. Importantly, there seems to be an emergent fault line between the creation of an undercover, fake profile compared to the impersonation of an actual person online. While courts have generally accepted law enforcement's use of deception – like the use of undercover officers, offline and online – the same cannot be said for actual impersonation of individuals.[57] Consequently, new rules need to be considered. When is it permissible for a law enforcement agent to ask for an individual's consent to impersonate them online? Is it ever impermissible? How can law enforcement personnel reconcile their legitimate investigatory needs with the policies of social media platforms that expressly forbid the impersonation or creation of fake profiles? Could a court ever authorize a warrant for the impersonation of someone online?

Critical Questions

Law enforcement use of social media is a powerful new investigative tool. Its growing use opens new questions that will need clear answers in order to ensure that civil rights are protected as law enforcement moves increasingly online. Specifically:

1. Should certain types of online activity be off---limits to law enforcement intelligence gathering? For example, what limits, if any, should apply to law enforcement surveillance of community organizing activity, including public protest messages on social media?

2. Are new rules needed to govern police impersonation of real people on social media?

3. How can policy and technology be used to ensure that social media surveillance is used in an equitable way, and is not unduly focused on certain communities or groups?

4. Might new forms of training, or other interventions, be necessary to equip police to accurately interpret the meaning of fast---changing and sometimes figurative modes of expression that young people may use online?

5. When and how should social media companies work with law enforcement? Should users – as a group or individually – be notified of such investigations?

6. Are specific protections needed to guarantee that social media is not taken out of context or used to suggest actions or relationships that might be performative?

7. What training might be necessary for judges, prosecutors, and defense attorneys to responsibly use social media data in cases?

---

1 We are very grateful for the strong contributions and insights made by Logan Koepke, David Robinson, Harlan Yu, Corinne Yu, Jeffrey Lane, Patrick Davison, and Angie Waller in the research and production of this primer.

2 "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." *LexisNexis*, Nov. 2014. Available at http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf.

3 One example is the case of Maxwell Marion Morton. See "Snapchat Selfie Unmasked Pittsburgh Killer, Police Say." *BBC News*, February 9, 2015. http://www.bbc.com/news/world-us-canada-31294752.

4 Latonero, Mark. "The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking." *USC Annenberg Center on Communication Leadership & Policy*, November 2012, https://technologyandtrafficking.usc.edu/files/2011/08/HumanTrafficking2012.pdf.

5 Wang, Amy X. "How a Selfie Got Car Thieves Arrested." *The Atlantic*, October 3, 2015, http://www.theatlantic.com/technology/archive/2015/10/riding-in-cars-with-selfies/408850/.

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

7 Broussard, Meredith. "When Cops Check Facebook." *The Atlantic*, April 19, 2015, http://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/. See also Ben Popper, "How the NYPD Is Using Social Media to Put Harlem Teens behind Bars." *The Verge*, December 10, 2014, http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

8 Palazzolo, Joe and Jacob Gershman. "Police Online Impersonations Raise Concerns." *Wall Street Journal*, January 22, 2015, sec. US. http://www.wsj.com/articles/police-online-impersonations-raise-concerns-1421895089.

9 Lye, Linda. "Unchecked Mass Surveillance of the Entire City of Oakland Is Not OK." *ACLU of Northern California*, March 4, 2014, https://www.aclunc.org/blog/unchecked-mass-surveillance-entire-city-oakland-not-ok.

10 "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." *LexisNexis*, November 2014, p. 9. Available at: http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf.

11 McCarty, James F. "Police Arrest Dozens of West Side Cleveland Gang Members Accused of Waging Reign of Terror." *Cleveland.com*, October 29, 2014, http://www.cleveland.com/court-justice/index.ssf/2014/10/policearrest38membersofwc.html.

12 Broussard, Meredith. "When Cops Check Facebook." *The Atlantic*, April 19, 2015, http://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/.

13 New York Police Department, Press Release. "Operation Crew Cut Results." *NYC.gov*, November 25, 2013, http://www.nyc.gov/html/nypd/html/pr/pr20131125operationcrewcutshomicideamongyouthinhalf.shtml.

14 Popper, Ben. "How the NYPD Is Using Social Media to Put Harlem Teens behind Bars." *The Verge*, December 10, 2014, http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

15 "SAS Products: SAS Text Miner." *SAS*, accessed October 7, 2015, http://support.sas.com/software/products/txminer/.

16 Schulz, G.W."Web Surveillance Through Social Media Sites A Powerful Tool For Local Law Enforcement." *The Huffington Post*, September 4, 2012, http://www.huffingtonpost.com/2012/09/04/web-surveillance-social-median1854750.html.

17 BlueJay, "What You Can Do With BlueJay." accessed October 7, 2015, http://brightplanet.com/bluejay/.

18 OpenMIND, "OpenMIND." accessed October 7, 2015, http://www.3i-mind.com/solutions/openmind/.

19 LexisNexis, "LexisNexis Launches New Social Media Investigative Solution for Law Enforcement." *LexisNexis*, October 15, 2013, https://www.lexisnexis.com/risk/newsevents/press-release.aspx?id=138185119773530 5.

20 Geofeedia, "Location-based Public Safety Social Media Intelligence." *Geofeedia*, accessed October 7, 2015, https://geofeedia.com/solutions/public-safety/.

21 Department of Homeland Security, "Using Social Media for Enhanced Situational Awareness and Decision Support." June 2014, p. 10. Available at: http://www.firstresponder.gov/TechnologyDocuments/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf.

22 Captain, Sean. "Hitachi Says It Can Predict Crimes Before They Happen." *Fast Company*, September 28, 2015, http://www.fastcompany.com/3051578/elasticity/hitachi-says-it-can-predict-crimes-before-they-happen.

23 LexisNexis, "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." *LexisNexis*, Nov. 2014. Available at http://www.lexisnexis.com/risk/insights/law-enforcement-social-media-infographic.aspx.

24 Graham, Rick. "Social Media Policy For Law Enforcement: Is It Necessary?" ***LexisNexis** Public Safety Briefing Room*, accessed September 26, 2015, http://blogs.lexisnexis.com/public-safety/2015/03/social-media-policy-law-enforcement/.

25 LexisNexis, "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." ***LexisNexis***, Nov. 2014, p. 7. Available at http://www.lexisnexis.com/risk/insights/law?enforcement?social?media?infographic.aspx.

26 LexisNexis, "Social Media Use in Law Enforcement: Crime prevention and investigative activities continue to drive usage." ***LexisNexis***, Nov. 2014, p. 8. Available at http://www.lexisnexis.com/risk/insights/law?enforcement?social?media?infographic.aspx.

27 Hogan, Hank. "DHS Fusion Centers: Coping With 'Data Crush'." *Homeland Security Today*, February 8, 2012, http://www.hstoday.us/channels/federalstatelocal/single-article-page/fusion-centers-coping-with-data-crush/2bc9d3e4ffab59e0a7fc388f92060dc0.html.

28 McCoy, Terrence. "DEA Created a Fake Facebook Profile in This Woman's Name Using Seized Pics — Then Impersonated Her." *The Washington Post*, October 7, 2014, https://www.washingtonpost.com/news/morning-mix/wp/2014/10/07/dea-created-a-fake-facebook-profile-in-this-womans-name-using-seized-pics-then-impersonated-her/.

29 Answer to the Complaint, Arquiett v. U.S., No. 13-CV-0752 (N.D.N.Y. Aug. 6, 2014) Available at https://www.documentcloud.org/documents/1309428-justice-department-answer-to-arquiett-civil.html.

30 Roubini, Sonia. "Here's How Law Enforcement Agencies Impersonate Your Friends." *American Civil Liberties Union*. August 31, 2015, https://www.aclu.org/blog/free-future/heres-how-law-enforcement-agencies-impersonate-your-friends. See also "'Consent to Assume Online Identity: Adult Consent' Form." *American Civil Liberties Union*, accessed October 5, 2015. https://www.aclu.org/other/consent-assume-online-identity-adult-consent-form.

31 International Association of Chiefs of Police, Center for Social Media, Accessed October 12, 2015. http://www.iacpsocialmedia.org/.

32 International Association of Chiefs of Police, Center for Social Media, "2014 Survey Results." Accessed October 1, 2015, http://www.iacpsocialmedia.org/Resources/Publications/2014SurveyResults.aspx.

33 International Association of Chiefs of Police, Center for Social Media, "Ready, Set, Go: Creating an engaging social media presence is about more than tools." Accessed October 1, 2015, http://www.iacpsocialmedia.org/Portals/1/documents/Guides/ReadySetGoAccenture.pdf.

34 International Association of Chiefs of Police, Center for Social Media, "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities." *International Association of Chiefs of Police*, p. 9. Available at: http://www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf.

35 Department of Homeland Security, "Using Social Media for Enhanced Situational Awareness and Decision Support." June 2014, p. 8. Available at:

http://www.firstresponder.gov/TechnologyDocuments/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf.

36 Department of Homeland Security, "Lessons Learned: Social Media and Hurricane Sandy." *FirstResponder.gov*, June 2013, https://communities.firstresponder.gov/DHSVSMWGLessonsLearnedSocialMediaandHurricaneSandyFormattedJune2013FINAL.pdf.

37 Joseph, George. "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson." *The Intercept*, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/. See also Logan Koepke, "The Feds Are Tracking #BlackLivesMatter. But Does That Violate Anyone's Rights?" *Equal Future.*, July 29, 2015. https://www.equalfuture.us/2015/07/29/feds-tracking-blacklivesmatter/.

38 Leopold, Jason. "Emails Show Feds Have Monitored 'Professional Protester' DeRay Mckesson." *Vice News*, August 11, 2015, https://news.vice.com/article/emails-show-feds-have-monitored-professional-protester-deray-mckesson.

39 Department of Homeland Security, "Using Social Media for Enhanced Situational Awareness and Decision Support." June 2014, p. 10. Available at: http://www.firstresponder.gov/TechnologyDocuments/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf.

40 N.Y. v. Harris, 36 Misc.3d 868 (N.Y. Crim. Ct. 2012) Available at https://www.aclu.org/files/assets/owsharristwitterdec63012.pdf.

41 Bankston, Kevin S. and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones." *Yale Law Journal*, Vol. 123, January 9, 2014, http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

42 boyd, danah and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no. 1 (October 1, 2007): 210–30. doi:10.1111/j.1083?6101.2007.00393.x.

43 boyd, danah. "Taken Out of Context: American Teen Sociality in Networked Publics." PhD Dissertation. University of California-Berkeley, School of Information, 2008. Available at: http://www.danah.org/papers/TakenOutOfContext.pdf.

44 Anderson, Elijah. *Code of the Street: Decency, Violence, and the Moral Life of the Inner City*. Reprint edition. New York: W. W. Norton & Company, 2000.

45 Hackman, Rose. "Is the Online Surveillance of Black Teenagers the New Stop-and-Frisk?" *The Guardian*, April 23, 2015, sec. US news. http://www.theguardian.com/us-news/2015/apr/23/online-surveillance-black-teenagers-new-stop-and-frisk.

46 Perrin, Andrew. "Social Media Usage: 2005?2015." *Pew Research Center: Internet, Science & Tech*. October 8, 2015, http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

47 Lenhart, Amanda. "Teens, Social Media & Technology Overview 2015." *Pew Research Center: Internet, Science & Tech*. April 9, 2015, http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/.

48 Social LifeRaft, "Social Navigator Launches LifeRaft Cyberbullying and Threat Detection Solution for Schools and Law Enforcement." *Social LifeRaft*, Accessed October 16, 2015. http://www.socialliferaft.com/about/press-releases/social-navigator-launches-liferaft-cyberbullying-and-threat-detection-solution-for-schools-and-law-enforcement/.

49 Corley, Cheryl. "When Social Media Fuels Gang Violence." *NPR.org*. October 7, 2015, http://www.npr.org/sections/alltechconsidered/2015/10/07/446300514/when-social-media-fuels-gang-violence.

50 ACLU, "What Is the School-to-Prison Pipeline?" *American Civil Liberties Union*. Accessed October 16, 2015. https://www.aclu.org/fact-sheet/what-school-prison-pipeline.

51 U.S. Department of Education Office for Civil Rights, "Civil Rights Data Collection - Data Snapshot: School Discipline," p. 1. Available at: http://ocrdata.ed.gov/Downloads/CRDC-School-Discipline-Snapshot.pdf.

52 Fuchs, Christian. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Routledge, 2012, p. 200.

53 Skorup, Brent. "Cops Scan Social Media to Help Assess Your 'threat Rating.'" *Reuters Blogs*. December 12, 2014, http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/.

54 Captain, Sean. "Hitachi Says It Can Predict Crimes Before They Happen." *Fast Company*, September 28, 2015, http://www.fastcompany.com/3051578/elasticity/hitachi-says-it-can-predict-crimes-before-they-happen.

55 U.S. v. Jones, 132 S.Ct. 945, 12 (2012), Available at http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

56 Bankston, Kevin S. and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones." *Yale Law Journal*, Vol. 123, January 9, 2014, http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

57 Roubini, Sonia. "Here's How Law Enforcement Agencies Impersonate Your Friends." *American Civil Liberties Union*. August 31, 2015, https://www.aclu.org/blog/free-future/heres-how-law-enforcement-agencies-impersonate-your-friends.