Civil Rights Concerns about Social Media Monitoring by Law Enforcement

Social media has proven to be an invaluable tool for activists to connect and organize online. Powerful platforms have allowed movements like #BlackLivesMatter, #Not1More, and #MeToo to flourish and influence the national dialogue on issues that affect all Americans, including the most vulnerable people in the United States.[1] But these services have also provided law enforcement with unprecedented power to monitor these growing movements and the people they represent.

Often covert and conducted without oversight, social media surveillance gives law enforcement agencies the ability to monitor and archive information on millions of people's activities.[2] This includes tracking people's political actions, a practice that endangers activists and undermines our First Amendment rights to speech and association. This is particularly concerning given repeated recent reports of targeting and surveillance of Black protesters and activists, family separation protestors, and border groups by the FBI and Department of Homeland Security.[3]

At the same time, few law enforcement agencies have publicly available policies showing how they use social media data on the communities they are supposed to protect. As with other surveillance in the United States, it appears that social media monitoring has been focused disproportionately on communities of color and other marginalized communities.

These monitoring tactics and law enforcement secrecy lead to civil rights and civil liberties harms. Here are six of the harmful impacts from social media surveillance that lawmakers and the public must take into account in any discussion about surveillance of social media users.

---

[1] *See* Monica Anderson, Skye Toor, Lee Rainie, & Aaron Smith, *Activism in the Social Media Age*, PEW RESEARCH CTR. (July 11, 2018), https://www.pewinternet.org/2018/07/11/activism-in-the-social-media-age/ ("Certain groups of social media users – most notably, those who are black or Hispanic – view these platforms as an especially important tool for their own political engagement.").

[2] *See* Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523 (2018), https://docs.wixstatic.com/ugd/cc2615_23ccb9a7aa1a4098b4742b01e5e443e6.pdf#page=43; Rachel Levinson-Waldman, *Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media*, 71 OKLA. L. REV. 997 (2019), https://digitalcommons.law.ou.edu/olr/vol71/iss4/2.

[3] Maya Berry & Kai Wiggins, *Leaked Documents Contain Major Revelations About the FBI's Terrorism Classifications*, JUST SECURITY (Sep. 11, 2019), https://www.justsecurity.org/66124/leaked-documents-contain-major-revelations-about-the-fbis-terrorism-classifications/; Jana Winter & Hunter Walker, *Exclusive: Document Reveals the FBI is Tracking Border Protest Groups as Extremist Organizations*, YAHOO NEWS (Sep. 4, 2019), https://news.yahoo.com/exclusive-document-reveals-the-fbi-is-tracking-border-protest-groups-as-extremist-organizations-170050594.html; Igor Derysh, *Leaked Documents Show FBI Targeted Post-Ferguson "Black Identity Extremists" Over White Supremacists*, SALON (Aug. 14, 2019, 10:00 AM), https://www.salon.com/2019/08/14/leaked-documents-show-fbi-targeted-post-ferguson-black-identity-extremists-over-white-supremacists/; Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests*, INTERCEPT (Apr. 29, 2019, 11:25 a.m.), https://theintercept.com/2019/04/29/family-separation-protests-surveillance/.

1. Social Media Monitoring Can Have a Chilling Effect on First Amendment-Protected Activities

Online surveillance by law enforcement stifles First Amendment-protected activities.[4] This is particularly true when the surveillance targets political speech, such as efforts to petition the government, promote policy change, or connect over shared identities, viewpoints, or advocacy. Local police and federal agencies have monitored hashtags, event pages, location data and other information from social media platforms to track public gatherings and political protests; one investigation found that nearly half the police departments in California had purchased social media monitoring tools that were advertised as a method to keep tabs on activists and protestors.[5] This information may be disseminated to other federal, state, and local government agencies, which leads to further surveillance, watchlisting, unnecessary interactions with law enforcement, and more dire consequences, such as overreaching immigration enforcement.[6]

2. Social Media Monitoring Disproportionately Impacts Communities of Color and Other Marginalized Communities

Media reporting and other publicly available sources suggest that—as with other types of police monitoring—social media surveillance by law enforcement disproportionately targets communities of color and other marginalized communities. In addition to the tools described above, which were directed at activists of color and other individuals speaking out on issues related to racial justice, the Boston Police Department used a social media monitoring tool to track the use of terms like #blacklivesmatter,

---

[4] *See, e.g.*, Alex Marthews & Catherine E. Tucker, *Government Surveillance and Internet Search Behavior* (Feb. 17, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; Leonard Downie Jr. & Sara Rafsky, *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, COMM. TO PROTECT JOURNALISTS (Oct. 10, 2013), https://cpj.org/reports/us2013-english.pdf (quoting national security reporter Dana Priest as saying "I'm even afraid to tell officials what I want to talk about because it's all going into one giant computer.").

[5] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, AM. CIVIL LIBERTIES UNION OF N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, AM. CIVIL LIBERTIES UNION (Sep. 22, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software; *see also* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 2:50 p.m.), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; Antonia Noori Farzan, *Memphis Police Used Fake Facebook Account to Monitor Black Lives Matter, Trial Reveals*, WASH. POST, Aug. 23, 2018, https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/.

[6] *See, e.g.*, Rachel Levinson-Waldman, *Government Surveillance of Social Media Related to Immigration More Extensive Than You Realize*, THE HILL (May 29, 2019, 11:00 AM), https://thehill.com/opinion/immigration/445766-government-surveillance-of-social-media-related-to-immigration-extensive; Joan Friedland, *How ICE Uses Databases and Information Sharing to Deport Immigrants*, NAT'L IMMIGRATION LAW CTR. (Jan. 25, 2018), https://www.nilc.org/2018/01/25/how-ice-uses-databases-and-information-sharing-to-deport-immigrants/.

#Muslimlivesmatter, and #protest.[7] Youth of color are heavily impacted by this surveillance as well; the New York City Police Department has officers devoted solely to online surveillance of young people whom they suspect are in gangs. This is a notoriously unreliable designation used almost exclusively to label Black and Latinx youth.[8]

The information gathered in this surveillance may then be disclosed to other government agencies, resulting in law enforcement encounters, incarceration, detention, and further tracking by federal agencies such as the FBI or ICE.[9] Even when social media surveillance is aimed at uncovering evidence of criminal activity, the disproportionate focus on communities of color puts those communities under perpetual law enforcement scrutiny without justifiable cause.[10]

3. Police are Monitoring Social Media without the Public's Input or Approval

Law enforcement agencies across the country have collectively spent millions on social media monitoring without public debate or consent.[11] As a result, most communities are entirely in the dark as to how their local police track their speech and associations online. A recent survey revealed that 70% of responding police departments used social media to gather intelligence for investigations.[12] A separate review of 157 law enforcement agencies that use these tools showed fewer than 15% had publicly available policies that provided any detail regarding their use of social media for these purposes.[13] Without knowledge of these

---

[7] Nasser Eledroos & Kade Crockford, *Social Media Monitoring in Boston: Free Speech in the Crosshairs*, PRIVACY SOS (2018), https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/.

[8] *See, e.g.*, Jake Offenhartz, *The NYPD's Expanding Gang Database Is Latest Form of Stop & Frisk, Advocates Say*, GOTHAMIST (June 13, 2018), https://gothamist.com/news/the-nypds-expanding-gang-database-is-latest-form-of-stop-frisk-advocates-say; Ben Popper, *How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars*, VERGE (Dec. 10, 2014), https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

[9] *See*, *e.g.*, Police Executive Research Forum, New National Commitment Required: The Changing Nature of Crime and Criminal Investigations (Jan. 2018), https://centerforimprovinginvestigations.org/wp-content/uploads/2018/04/20180000-The-Changing-Nature-of-Crime-and-Criminal-Investigations-Police-Executive-Research-Forum.pdf.

[10] *See* Desmond Upton Patton, Douglas-Wade Brunton, Andrea Dixon, Reuben Jonathan Miller, Patrick Leonard, & Rose Hackman, *Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations*, SOCIAL MEDIA + SOCIETY 3, no. 3, 2017, https://journals.sagepub.com/doi/10.1177/2056305117733344.

[11] *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CTR. FOR JUSTICE (Nov. 16, 2016), https://www.brennancenter.org/our-work/research-reports/map-social-media-monitoring-police-departments-cities-and-counties.

[12] KiDeuk Kim, Ashlin Oglesby-Neal, & Edward Mohr, *2016 Law Enforcement Use of Social Media Survey*, INT'L ASS'N OF CHIEFS OF POLICE & URBAN INST. (Feb. 2017), https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf; *see also 2015 Law Enforcement Use of Social Media Survey*, INT'L ASS'N OF CHIEFS OF POLICE (2015), http://www.iacpsocialmedia.org/wp-content/uploads/2017/01/FULL-2015-Social-Media-Survey-Results.compressed.pdf (reporting that 96% of the agencies surveyed used social media in some capacity, with nearly 88% of those using it for criminal investigations, 58.4% for "listening/monitoring," and 75% for intelligence).

[13] *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, *supra* note 11.

policies, it is impossible for communities to know whether or how departments are protecting individuals' rights or overseeing their officers' use of these technologies. This obscurity is particularly notable at a time when communities around the country are pushing for more transparency around police use of surveillance tools.[14]

4. Suspicionless Monitoring of Individuals Threatens Privacy and Allows Invasive and Persistent Tracking

Monitoring, mapping, and storing users' posts and other activity on social media by law enforcement can intrude upon their privacy rights, even where the data is otherwise viewable by the public or a portion of the public.[15] This data can provide a revealing picture of an individual's personal life, preferences, associates, and activities, particularly when monitored and collected over an extended time period or when combined with network or metadata analysis. As the Supreme Court has recognized, the extent to which data reveals such intimate information is relevant to the question of whether government monitoring should be restricted by a warrant or other heightened protections.[16]

In the absence of written guidelines or other means of accountability, the only limits on the retention of social media information will be those imposed by other departmental policies. Without explicit limitations, data not directly connected to an ongoing investigation may remain in files or databases, waiting to be mined for additional information, location data, or content, or even used for further tracking far beyond the time or original purpose of collection.[17]

---

[14] *See, e.g.*, *Community Control over Police Surveillance*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance; Sidney Fussell, *Oakland Passes Nation's Strongest Surveillance Technology Ordinance Yet*, GIZMODO (May 2, 2018), https://gizmodo.com/oakland-passes-nations-strongest-surveillance-technolog-1825725697; *PAC Surveillance Technology Ordinance Approved by City Council*, CITY OF OAKLAND, https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council. *See also The Public Oversight of Surveillance Technology (POST) Act: A Resource Page*, BRENNAN CTR. FOR JUSTICE (June 12, 2017; last updated Nov. 29, 2018), https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page; Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Andy Rosen, *Somerville Moves to Ban Facial Recognition Surveillance*, BOS. GLOBE, May 10, 2019, 8:45 PM, https://www.bostonglobe.com/metro/2019/05/10/somerville-moves-ban-facial-recognition-surveillance/ebhl0qcX6k14O1H78yrpiI/story.html.

[15] *See*, *e.g.*, Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151 (2017), https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1272&context=jbtl; Jeramie D. Scott, *Selling You Out: Mass Public Surveillance for Corporate Gain*, THE HILL (Mar. 16, 2018), https://thehill.com/opinion/civil-rights/378835-selling-you-out-mass-public-surveillance-for-corporate-gain.

[16] *United States v. Jones*, 565 U.S. 400, 404-05 (2012); *Riley v. California*, 573 U.S. 373, 393, 403 (2014); *Carpenter v. United States*, 138 S. Ct. 2206, 2216-17 (2018).

[17] Note: Under federal regulation 28 CFR 23.20, state and local law enforcement agencies are restricted from including in federally-funded databases information concerning an individual unless there is "reasonable suspicion" that the individual is involved in criminal activity and the information is relevant to that activity. Despite the existence of this regulation, and its likely applicability to state and local law enforcement social

5. Fake Accounts and Other Undercover Law Enforcement Activity Pose Particular Threats

While there are no hard numbers on how many police departments use undercover accounts to connect with individuals online, anecdotal evidence suggests the practice is widespread and often operates with little oversight or departmental controls, despite published guidelines from some social media platforms prohibiting the practice.[18] Online undercover activity can violate the public trust and may be even more insidious than in-person monitoring; this plays out in at least three ways. First, it is harder to verify someone's true identity online. Second, an officer operating undercover could connect with and monitor an almost limitless number of people, while eliciting far more information than could typically be gleaned through face-to-face interactions. Third, a law enforcement agent could adopt multiple undercover personas, a feat that would be nearly impossible in person.[19] And finally – as with in-person undercover activity – using an undercover account in order to connect with someone covertly could allow access to information that would otherwise require a warrant to obtain.

6. Social Media Can Be Highly Context-Dependent, Raising the Stakes When it is Used for Criminal Justice Purposes

Finally, law enforcement reliance on social media is particularly perilous in light of its notoriously contextual nature and the difficulty of accurately interpreting its meaning. One study found that even the best automated tools get the meaning of text wrong 20-30% of the time, and manual review may fare no better, as one couple found when they were barred from entering the United States over a misunderstood joke on Twitter.[20] These challenges are magnified when law enforcement uses a person's social media posts

---

media monitoring systems, the absence of meaningful government transparency, accountability and oversight systems at the state and local level, as well as the failure of the Department of Justice to hold agencies accountable, mean the regulation is too often ignored.

[18] *See* Kashmir Hill, *The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook*, ROOT (Oct. 23, 2018), https://www.theroot.com/the-wildly-unregulated-practice-of-undercover-cops-frie-1828731563; Jon Schuppe, *Undercover Cops Break Facebook Rules to Track Protesters, Ensnare Criminals*, NBC NEWS (Oct. 5, 2018), https://www.nbcnews.com/news/us-news/undercover-cops-break-facebook-rules-track-protesters-ensnare-criminals-n916796.

[19] Documents obtained by the ACLU of Massachusetts show that companies have offered extensive services catering to law enforcement undercover operations online. In response to a request for proposals from the Boston Police Department for social media surveillance systems, for instance, the company Verint produced a nearly 200-page document outlining its offerings, including the maintenance of an "army" of undercover law enforcement bots. This offering came immediately after the major social media platforms made initial changes to make it more difficult for commercial developers to use social media data for law enforcement surveillance tools. *See RFP for Acquiring Technology & Services Of Social Media Threats For The Boston Police Department*, VERINT (Oct. 2016), http://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/wp-content/uploads/2017/01/BRICProposalBaselineDocument27a-Oct-16.pdf; *Boston Police Cancels Plan to Buys $1.4 Million Social Media Surveillance System*, PRIVACY SOS (Jan. 14, 2017), https://privacysos.org/blog/boston-police-cancels-plan-buy-1-4-million-social-media-surveillance-system/; Dell Cameron, *Dozens of Police-Spying Tools Remain After Facebook, Twitter, Crack Down on Geofeedia*, DAILY DOT (Oct. 11, 2016), https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/.

[20] *See, e.g.*, Natasha Duarte, Emma Llanso, & Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, CTR. FOR DEMOCRACY & TECH. (Nov. 2017), https://cdt.org/files/2017/11/Mixed-

and other activity to generate or support criminal charges or prison time.[21] Even something as simple as pressing the "like" button on a Facebook post can be used to scrutinize everyone from individuals seeking information about lawful protests to teens trying to keep up with their neighborhood friends.[22] Law enforcement must tread extremely carefully when turning to a medium that is rife with hidden meanings, innuendo, and misdirection.

Sincerely,

18 Million Rising
Access Now
ACLU
ACLU of Northern California
Albuquerque Center for Peace and Justice
American Friends Service Committee
American-Arab Anti-Discrimination Committee
Arab American Institute
Asian Americans Advancing Justice (AAJC)
Brennan Center for Justice
Center for Democracy & Technology
Center on Privacy and Technology
Color of Change
Council on American-Islamic Relations
CREDO Action
Dangerous Speech Project
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Filipina Women's Network
Free Press
Freedom House
Immigrant Defense Project
Institute for Free Speech
Islamophobia Studies Center
Japanese American Citizens League (JACL)
Jetpac
Lawyers' Committee for Civil Rights Under Law
The Leadership Conference on Civil and Human Rights
Media Mobilizing Project
MediaJustice
Mijente
MPower Change
Muslim Advocates
Muslim Anti-Racism Collaborative (MuslimARC)
Muslim Justice League
Muslim Public Affairs Council (MPAC)
National Association of Criminal Defense Lawyers
National Coalition Against Censorship
National Hispanic Media Coalition

Messages-Paper.pdf; Richard Hartley-Parkinson, *'I'm Going to Destroy America and Dig Up Marilyn Monroe': British Pair Arrested in U.S. on Terror Charges over Twitter Jokes*, DAILY MAIL, Jan. 31, 2012, 8:08 AM, https://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html; *see also* Kashmir Hill, *Call To LAX Tipline Flagged U.K. Tourists' Tweets (Not A DHS Twitter Search Alert)*, FORBES (Jan. 31, 2012, 8:30 AM), https://www.forbes.com/sites/kashmirhill/2012/01/31/call-to-lax-tipline-flagged-u-k-tourists-tweets/#7137e30d1511.

[21] *See, e.g.*, Hill, *supra* note 18; Natasha Lennard, *The Way Dzokhar Tsarnaev's Tweets are Being Used in the Boston Bombing Trial is Very Dangerous*, SPLINTER (Mar. 12, 2015, 6:45 AM), https://splinternews.com/the-way-dzhokhar-tsarnaevs-tweets-are-being-used-in-the-1793846339.

[22] *See, e.g.*, Popper, *supra* note 8; Chip Gibbons, *The Prosecution of Inauguration-Day Protesters Is a Threat to Dissent*, NATION (Oct. 20, 2017), https://www.thenation.com/article/the-prosecution-of-inauguration-day-protesters-is-a-threat-to-dissent/ (describing a Department of Justice warrant for all 6,000 people who "liked" the DisruptJ20 Facebook page, related to protests against the 2016 Inauguration Day).

National Immigrant Justice Center
National Immigration Law Center
National Immigration Project of the National Lawyers Guild
National Organization for Women
New America's Open Technology Institute
Open MIC (Open Media and Information Companies Initiative)
Project South
Public Citizen
Restore The Fourth
S.T.O.P. - The Surveillance Technology Oversight Project
Southern Poverty Law Center
TAKE ON HATE
TechFreedom
X-Lab