ANALYSIS

Study Reveals Inadequacy of Police Departments' Social Media Surveillance Policies

DrAfter123/Getty

Hundreds of law enforcement agencies lack the safeguards needed to prevent officers from misusing social media to target First Amendment activity and minorities. Our best practices show how to fill the gaps.

Rachel Levinson-Waldman

José Guillermo Gutiérrez

February 7, 2024

Protect Liberty & Security

Social Media

Social media has become instrumental for exercising free speech and other rights, and its improper use by law enforcement can squelch those rights — often in discriminatory ways. That's why the Brennan Center and other advocates have long voiced concerns about the dangers of allowing law enforcement agencies to freely access social media in the name of public safety. It's essential that when and how officers use social media be subject to tight restrictions and transparency rules.

But an extensive, **nationwide analysis by the Brennan Center** reveals that virtually all available policies governing police use of social media have serious deficiencies that can lead to grave consequences for those

who are monitored or tracked. In response, we're also releasing a set of **principles and best practices** to guide law enforcement agencies' use of social media to ensure the public's constitutional rights are protected.

The risk of police using social media to surveil constitutionally protected activity is not hypothetical. For example, the Los Angeles Police Department has a history of using social media monitoring tools to **surveil** online activity related to protest movements. The ACLU of Massachusetts **revealed** that the Boston Police Department used a social media monitoring tool to surveil Black and Muslim communities.

The Brennan Center's new, comprehensive **examination** shows that despite these dangers, most police departments allow their officers virtually free rein. We found that while social media use by local law enforcement agencies is **widespread**, many departments do not have policies in place to regulate the practice. Where policies do exist, robust guidance and guardrails are the exceptions rather than the rule.

For this review, the Brennan Center looked at the police departments of all 328 localities with populations of 100,000 people or more. Of those, fewer than half — 162 agencies — had publicly available policies on their websites. With a few exceptions, it is unknown how many of the nearly 200 departments that lack a policy nevertheless use social media for monitoring or information collection. In light of the widespread use of social media, it seems highly likely that at least some of them do.

We analyzed the available policies according to a list of factors, such as whether they set out requirements for investigative and undercover use or contained provisions protecting the public's constitutional rights. Our analysis found that the policies rarely include adequate descriptions of how the department intends to use social media. Even the most complete policies lack robust safeguards to prevent misuse by officers, imperiling individuals' civil rights and civil liberties.

For example, almost all the policies we reviewed state that social media can be used to assist with investigations. Yet only 74 policies, or fewer than half of those our research uncovered, articulate standards for how officers may use social media in investigations. Moreover, many of these merely instruct officers to verify the information they collect from social media and explain how to document and retain it but do not impose any limitations on officers' online monitoring or the information that can be retained. Indeed, only 8 policies require officers to have reasonable suspicion of criminal activity to seek or retain information from social media, providing the remainder with a virtual invitation for fishing expeditions.

The possibility of abuse becomes even more pronounced when police use covert or undercover accounts to connect with people on social media. For example, the ACLU of Tennessee successfully sued the Memphis Police Department after an officer **masqueraded** as a Black activist on Facebook to "friend" activists, infiltrate their groups, and gather information to build dossiers on activists. Police use of fake accounts also violates major platforms' policies, as Facebook's owner Meta has **repeatedly warned** law enforcement agencies.

Nevertheless, the language on undercover accounts is typically quite permissive. Of the 162 policies we identified, 92 address covert or undercover activities. While all but 4 require officers to obtain some supervisory authorization to conduct covert or undercover activities, almost 80 percent do not rise above the bare minimum of supervisory oversight, as 68 of the 88 policies requiring supervisory approval do not set out any additional procedural measures or guardrails, such as regular, ongoing reauthorization of alias accounts, audits to detect misuse, or limits that would restrict their use to a narrow set of serious crimes.

The few policies that do build in important limits, such as a prohibition on using undercover social media accounts in the absence of reasonable suspicion of criminal activity or a threat to public safety, are weakened by the failure to narrowly define public safety. For example, if a Black Lives Matter rally was

marred by a violent police response or a troublemaker who threw a bottle, there is a risk that the next similar event could be categorized as a public threat, justifying intrusive, undercover online surveillance.

While none of the policies we analyzed are sufficiently robust to serve as an adequate check on a department's use of social media, some do have useful elements. The **Austin Police Department**, for example, requires a supervisor to review undercover activity every 90 days to ensure its continued necessity, while the **Detroit Police Department** directs employees to delete information gathered from social media when a criminal nexus is not established.

Of course, even the best policy cannot prevent all misuse or abuse, particularly in light of the **known shortcomings** of social media as an interpretive or decision-making tool. Information found on these platforms is highly contextual, and the stakes of misinterpretation are high when law enforcement is involved. For example, police in Wichita, Kansas, **arrested** a Black teenager in 2020 on the grounds that his Snapchat post incited a riot, when in reality his post warned people to stay away from protests in his hometown. And social media posts are commonly used as thin evidence to tag youth of color as **gang members**, a designation that can have dire consequences.

Nonetheless, public policies are essential to provide guidance to officers, prevent misuse and abuse, and ensure accountability when violations happen. Toward those ends, we are releasing **principles and best practices** to help guide law enforcement agencies' use of social media for investigative and other purposes while protecting Americans' civil rights and civil liberties. Social media is a powerful tool that also poses serious risks, and it is critical that police departments adopt clear, robust, publicly available policies to mitigate the risks and most effectively serve their communities.

RELATED ISSUES: **Protect Liberty & Security**
Social Media

Related Resources

RESOURCE

Directory of Police Department Social Media Policies

While many departments have policies addressing the use of social media data, most are too permissive or provide little transparency about actual practices.

February 7, 2024

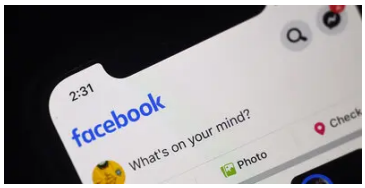
Rachel Levinson-Waldman

RESOURCE

Principles for Social Media Use by Law Enforcement

February 7, 2024 Rachel Levinson-Waldman

SEE ALL IN LIBRARY



ANALYSIS

FTC Must Investigate Meta and X for Complicity with Government Surveillance

These platforms promised to protect their users. Are they?

Ivey Dyson , Jake Snow
December 12, 2023

ANALYSIS

We're Suing the NYPD to Uncover Its Online Surveillance Practices

Police officers have spent a decade using social media and third-party tools to monitor New Yorkers with little transparency or oversight.

Emile Ayoub, Helen Griffiths
November 20, 2023

Senate AI Hearings Highlight Increased Need for Regulation

October 13, 2023 Faiza Patel, Melanie Geller

Documents Reveal Widespread Use of Fake Social Media Accounts by DHS

September 5, 2023 José Guillermo Gutiérrez, Rachel Levinson-Waldman

Is Meta Up for the Challenge Now That It Has Reinstated Trump?

March 17, 2023 Faiza Patel, Emile Ayoub

MORE NEWS & ANALYSIS