Social Media Surveillance And Law Enforcement

According to a 2014 LexisNexis online survey, eighty percent of federal, state, and local law enforcement professionals use social media platforms as an intelligence gathering tool, but most lack policies governing the use of social media for investigations. Law enforcement agencies utilize social media for a wide range of reasons, including: discovering criminal activity, obtaining probable cause for search warrants, collecting evidence for court hearings, pinpointing the location of criminals, witness identification, as well as broadcasting information and soliciting tips from the public. Social media surveillance includes both manual and automated practices, and methods may be targeted or general.

- Several factors challenge the efficacy of social media surveillance, including the difficulty of interpreting online speech, and the existence of outdated, inaccurate, or incomplete information online.
- New tools facilitate automated continuous monitoring of online activity using algorithms set to trigger words and phrases that can alert police to potential illicit activity. In some cases, social media data is being incorporated into predictive policing.
- One area of concern has been the use of social media to identify criminals based on online associations, which may not accurately reflect realities on the ground. This practice has had some successes, but has been critiqued for potentially criminalizing innocent people, particularly minors who may have outgrown past criminal activities or associations.
- Social media monitoring is also used in the surveillance of activists (for instance #blacklivesmatter activists by the Department of Homeland Security), raising Fourth and First Amendment concerns about unreasonable search and seizure, and the protection of public speech online.
- In certain instances, social media surveillance strategies have led to lawsuits, like when police impersonate real people or create fake online personas to infiltrate networks online, a practice that is against the terms of service of many social media platforms. Such cases underscore the need for better policies and training to avoid violating people's rights.
- To balance the protection of constitutional rights and civil liberties with the tactical utility of social media surveillance tools for law enforcement, we need to create standards, education, training and protocols to aid law enforcement professionals in using social media for investigations.

Critical Questions

- What are appropriate limits or guidelines to surveillance of social media activity?
- Should certain types of online activity be off-limits to law enforcement intelligence gathering? What about community organizing or protest planning? Are there chilling effects on free speech?
- With automated surveillance tools that replace human discretion, are there avenues for identifying potential systemic biases?
- Might new forms of training, or other interventions, help equip police, judges, and lawyers to better interpret the fast-changing modes of expression that people use?
- Do low-cost, largely scalable surveillance technologies deserve their own limits? If so, what would those limits look like?
- When and how should social media companies work with law enforcement? Should users – as a group or individually – be notified of such investigations?
- Are new rules needed to govern police impersonation of real people on social media?
- How should social media companies engage with this process? Are there ways for companies to incorporate police use in transparency reporting?