Police watch your social media posts. Invasion of privacy or fair game?

November 10 2021, by George Hunter

Credit: Pixabay/CC0 Public Domain

Since the platform MySpace was launched in 2003, police have monitored social media searching for suspects and trying to predict crime trends, giving pause to civil liberties advocates concerned about

authorities peeking over citizens' virtual shoulders.

Michigan law enforcement officials say there's no expectation of privacy when posting to public platforms and point out that multiple cops have been disciplined or fired for their own social media posts.

But some critics say the same biases that taint police investigations in the physical world also infiltrate online probes. They say there's not enough oversight to ensure officers don't unfairly target minorities or conduct inappropriate searches while combing social media.

Concerns about the intersection of police and social media were rekindled recently when a nonprofit magazine revealed that Michigan State Police contracted with a Colorado firm last year to use software that allows the agency to quickly scan thousands of public social media posts from more than 120 platforms, from Facebook to Amazon wish lists.

The article by The Intercept published details about the five-year, $3.5 million state police contract with Kaseware, a firm that describes itself on its website as an "incident, case management, records management and analytics platform" for law enforcement.

Through the Kaseware contract, state police purchased software made by ShadowDragon, a company whose stated mission is "to make the world a safer place by developing easy-to-use digital investigation tools."

According to the ShadowDragon website, SocialNet extracts information from social media networks along with RSS feeds, data dumps and the dark web—networks that require specific software, configurations, or authorization to access.

State police are using ShadowDragon's SocialNet and OIMonitor

software.

The OIMonitor software "lets you broaden your scope and monitor on your terms—being alerted to relevant keywords so you can identify threats before they become problems," the company site promises.

Although the OIMonitor software touts its ability to predict threats, Michigan State Police spokeswoman Shanon Banner said in an email: "The MSP does not use these tools to perform predictive policing."

Still, Christopher White, director of the Detroit Coalition Against Police Brutality, said he's wary of the software.

"Technology can be an easy way out sometimes for police," White said. "You'll hear police say, 'If you're not doing anything wrong, you shouldn't care if you're being monitored,' but how many times have we seen people who weren't doing anything wrong get caught up in the criminal justice system, particularly African Americans?

"That's my first question. Will this technology be fairly applied to everyone?"

The state police agency practices constitutional policing when using the software package that was purchased in January 2020, Banner said.

"The MSP uses these tools when conducting criminal investigations, following all applicable state and federal laws," she said. "Examples include human trafficking investigations and investigations into the sale of stolen credentials on the dark web."

Banner said she couldn't provide specifics about those investigations because it "would put us at an investigative disadvantage for future cases."

Police contract stirs concerns

The Kaseware contract was posted to the state of Michigan's primary procurement website, Michigan Contract Connect, briefly before being removed. The Intercept obtained a copy of the contract while it was online. Banner confirmed the authenticity of the magazine's copy.

"Given this contract pertains to the investigative tools of a law enforcement agency, it was given a security exemption from being displayed on the Michigan Contract Connect website," Banner said.

Phone calls to ShadowDragon and Kaseware were not returned.

After the Kaseware contract was signed, the company praised the pact in a Jan. 11 statement.

"Kaseware is excited to announce that our platform is now live at the Michigan Intelligence Operations Center," the statement said. "The MIOC provides 24 hours a day statewide information sharing among local, state and federal public safety agencies, as well as private sector organizations. Most importantly, they facilitate the collection, analysis and dissemination of intelligence relevant to terrorism and public safety.

"This launch is the first step in a multi-year plan that will provide Kaseware to hundreds more members of the Michigan State Police ... gradually expanding across the entire state," the statement said. "We're thrilled at the opportunity to provide MSP with the tools to modernize their intelligence management, analytics, and data sharing capabilities."

Michigan Sen. Jim Runestad, R-White Lake, said he's concerned about the lack of information available about the software and said he plans to question state police officials about it.

"Millions of dollars were spent to get a system that can collect and collate data on just about any individual, and it really creates a remarkably large database," Runestad said. "There needs to be more public input and guidelines with a system like this."

Monitoring demonstrations

Detroit Police Department investigators don't use the same software but do search social media, Assistant Chief David LeValley said.

"We have dashboards we've created that allow us to search keywords in Facebook, Instagram and the others," he said. "We use their own search engines to search the keywords, and it's all open-source public posts, so anything we're looking at, anyone else can look at."

LeValley said police have an obligation to search any allowable physical or virtual space, including social media, when investigating crimes or tracking suspects.

"We have analysts at the Gang Unit who follow open-source pages of gang members," he said. "That's just part of responsible policing. We can't look at people's private pages without showing probable cause and getting a judge to sign a warrant."

Photos posted publicly to social media are used in the department's facial recognition process, LeValley said.

"During an investigation, if we determine someone is a suspect we go into their open-source social media pages and use those photos to feed into (facial recognition software)," he said. The searches sometimes yield photos of co-suspects, which also are run through the software, LeValley said.

Concerns that included potential invasions of privacy and a flaw in facial recognition technology that reportedly misidentifies a higher percentage of African Americans prompted Detroit police officials in 2019 to revamp the department's policy governing the use of the software. The provision that allowed police to scan faces in real-time was jettisoned, and other safeguards were implemented.

Under Detroit police guidelines, investigators may only use facial recognition software on suspects in violent crimes or Home Invasion 1 cases, which are break-ins where a weapon is used, someone is home during the invasion or the burglar intends to commit a felony.

LeValley said police monitored the public social media pages of protest groups and activists during more than 100 days of demonstrations in the summer of 2020.

"We gathered information on where the events were happening, when, the approximate size, or if there were any threats to the events," LeValley said.

Social media posts have led to several arrests in Detroit, LeValley said.

"We've gotten videos from social media to make arrests in a lot of the drag racing cases," he said. "We've made arrests in other crimes based on things people have posted online."

In a case that made national news last year, Detroit police arrested Jadon Hayden after he allegedly posted a video to YouTube showing him beating 75-year-old Norman Bledsoe at the Westwood Nursing Center in Detroit.

Bledsoe suffered a broken jaw and broken ribs and fingers after the May 15, 2020, incident. He died two months later after relatives said he sank

into depression and would not eat.

Hayden was charged with assault with intent to do great bodily harm and credit card theft but was found incompetent to stand trial. He is in a psychiatric facility awaiting a scheduled Jan. 19 hearing for an update on his mental condition, Wayne County Assistant Prosecutor Maria Miller said.

Like Detroit, officials at the Wayne, Oakland and Macomb County sheriff's offices said they don't use software to aid in social media investigations.

In Michigan's third-largest city, Warren investigators also manually search social media, Cpl. Brandon Roy said.

"Social media is growing as a medium to commit crimes, particularly to set up robberies," he said. "We're getting a lot of robberies from people using Facebook Marketplace, just like you see with Craigslist, where someone will arrange a meeting for a sale and then get robbed when they show up."

Technology growing too fast?

Detroit activist Tawana Petty said she's concerned police biases can taint internet investigations.

"I don't think there's been enough work to increase equity within law enforcement to allow for cops to analyze these massive amounts of data," Petty said. "There isn't enough regulation. I think advances in data extraction and technology are moving way too fast, and we haven't had conversations about how these things are being handled."

Runestad said he'd also like to see more oversight of how police conduct

investigations online.

"If there isn't some kind of policy, you could have police officers checking up on old boyfriends or girlfriends, or doing other inappropriate searches," he said. "I think there has to be a policy in place."

Runestad said when he was a state representative, he pushed for a Legislature-appointed privacy protection board, "which would work with stakeholders to ensure there were policies governing this activity that were in the best public interest. It may be time to revisit that again."

Banner said her agency already has such policies in place.

"The MSP Michigan Intelligence Operations Center (MIOC) maintains an extensive privacy, civil rights and civil liberties policy," she said.

The policy requires the agency to appoint privacy committees "that are available to interact with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the MIOC's information collection, retention and dissemination processes and procedures."

Robert Stevenson, director of the Michigan Association of Chiefs of Police, said most police departments in the state have enacted strict social media policies governing officer searches and posts.

"We have had many training classes for police chiefs on that practical issue and types of policies that need to be put out, so employees will know exactly what they can or can't do," Stevenson said.

While police are watching citizens' social media posts, he said, the officers' posts also are being scrutinized.

Recent controversies involving cops' social media posts included the 2019 firings of former Detroit police officers Gary Steele and Michael Garrison after Steele's Snapchat video showed the White officers taunting Black motorist Ariel Moore as her vehicle was being impounded.

In 2017, former Michigan State Police Col. Kristie Kibbey Etue was docked five days' pay for violating the agency's social media policy after she shared a Facebook meme that criticized National Football League players who knelt during the national anthem. Etue also issued a written apology.

Stevenson said: "Nobody ever talks about the officers' privacy when they get in trouble for something they posted on social media. It's a double-edged sword. Officers have to walk a fine line between expressing themselves and the negative implications a post can bring on a department or the profession."

State Rep. Tyrone Carter, D-Detroit, a former Wayne County Sheriff's lieutenant, argues police aren't violating people's rights by searching their public social media posts.

"The moment you hit send on a public page, that post is no longer yours," Carter said. "People get in all sorts of trouble because of things they post because social media is the biggest self-snitch I've ever seen."