FBI agents monitor social media. As domestic threats rise, the question is who they're watching

September 1 2022, by Will Carless, USA Today

Credit: Pixabay/CC0 Public Domain

On Aug. 11, Adam Bies logged into his account on Gab and started typing:

"I sincerely believe that if you work for the FBI, then you deserve to DIE."

Bies, 46, was an aspiring freelance photographer who had filled his website with action photos of fast cars and outdoor sports. He had been fired from his day job in marketing for refusing the COVID-19 vaccine, he wrote online, and had struggled in his efforts to file an unemployment claim.

As federal prosecutors would later describe in court filings, Bies was filling his days posting under a pseudonym on Gab, a social media service popular with right-wing extremists.

His post included a link to a Fox News story about FBI Director Christopher Wray decrying the wave of violent threats directed at the agency in the three days since the search of former President Donald Trump's home and club Mar-a-Lago. He compared federal agents to Nazi forces. He fumed about "police state scum." And he composed what might have been seen as a final plan.

"I already know I'm going to die at the hands of these ... law enforcement scumbags," he wrote, interspersed with profanity. "My only goal is to kill more of them before I drop."

Four days later, warrant in hand, armed federal agents and SWAT teams surrounded Bies' home, near a tumbling waterfall in the deep-forest hunting country of western Pennsylvania. Inside the house were Bies and his 12-year-old son. It was dark, near midnight.

Officers called Bies on his cellphone, over and over, 16 times in all. They issued orders through a loudspeaker to surrender.

Finally, Bies emerged, carrying an assault rifle. Officers ordered him to put down the weapon.

In those four days between Bies' threatening posts and the moment he faced off with armed agents, he had been snared by a complex, little-known practice within the FBI called social media exploitation, or SOMEX—one that might, at this moment, be monitoring the online activities of anyone in America.

Top FBI leaders have sought to downplay the extent to which agents can legally monitor public online activities of people who aren't under investigation. But in reality, the bureau can conduct almost unlimited monitoring of public-facing social media, as long as it's doing so for law-enforcement purposes, FBI officials told U.S. TODAY.

Experts say that gives the FBI more power than it has been willing to acknowledge publicly—power the bureau and other security experts say they have a

responsibility to use to prevent terrorism.

But critics say social media exploitation also means agents are allowed to review online posts at will, with no oversight, yet vast authorities.

"FBI officials have put out a lot of misinformation about the scope of their authorities," said Michael German, a former FBI special agent and a fellow with New York University's Brennan Center for Justice. "The FBI has tremendous powers to investigate long before there's a reasonable criminal predicate."

SOMEX, involves agents who develop their own leads and receive information from a network of contractors and collaborators, such as a terrorism research group that first flagged the posts by Bies.

But the bureau has been criticized for how its investigators have reacted—as in the case of online posts made by liberal activists during the Black Lives Matter protests of 2020—and how they failed to react—as in the right-wing build-up to the Jan. 6 insurrection.

The FBI has long been under scrutiny for overreach in creating files on public figures and others, even if they were not under criminal investigation. And some experts say the agency has a history of focusing on left-leaning groups like environmentalists and racial justice activists, while ignoring threats from white supremacists and others on the right. They say this tendency carries over into the digital era.

And internal records obtained by one advocacy group appear to show agents in cyber-research specifically focusing on anti-police and racial justice rallies instead of armed counterprotesters or white supremacists.

"The problem with social media surveillance is often the problem with policing at large, which is that police cannot predict crime, all they can do is make an assessment of what type of person is most likely to commit crime, and put that group under surveillance," said Matthew Guariglia, a policy analyst at the Electronic Frontier Foundation. That "knee-jerk reaction," Guariglia said, ends up meaning more surveillance and harassment of people of color and marginalized groups.

But as outrage over Mar-a-Lago now spurs threats from right-leaning extremists to historic levels, longstanding questions about how the FBI really monitors Americans online encounter a new twist: What happens when the people being threatened are the FBI agents themselves?

FBI has wider latitude than many realize

In June of last year, in a hearing of the House Committee on Oversight and Reform, New York Congresswoman Alexandria Ocasio-Cortez grilled Wray about the FBI's failure to foresee the chaos of the Jan. 6 insurrection.

"We now know that the attacks were planned out in the open on popular social media platforms," Ocasio-Cortez said. "Does the FBI regularly include social media monitoring as part of its efforts to combat violent extremism?"

Wray's response was emphatic:

"We have very specific policies that have been at the department for a long time that govern our ability to use social media. And when we have an authorized purpose and proper predication there's a lot of things we can do on social media," Wray said. "But what we can't do on social media is without proper predication, and an authorized purpose, just monitor."

Months earlier, the FBI's former executive assistant director for national security, Jill Sanborn, gave a similar explanation to the Senate Committee on Homeland Security and Governmental Affairs. "We cannot collect First Amendment-protected activities without sort of the next step, which is the intent," she said.

Sen. Kyrsten Sinema followed up, asking, "So the FBI does not monitor publicly available social media conversations?"

"Correct, ma'am. It's not within our authorities," Sanborn replied.

The FBI's own rules say otherwise.

FBI officials told U.S. TODAY that Wray's statement was correct, while acknowledging that an "authorized purpose" means simply doing anything in line with the duties of an FBI agent.

That "authorized purpose" is actually extraordinarily broad. Policy would forbid agents from looking at social media to, for example, keep tabs on a romantic partner, or monitor for some other non-law enforcement use. But it would allow an agent to look at essentially anything online, proactively, if the intent was to stop a crime or to keep Americans safe. An FBI official called this falling within the "penumbra of national security, enforcement of federal law, or foreign intelligence."

German, a fellow with the Brennan Center's Liberty and National Security Program, argued in a recent report that individual FBI agents have extraordinary leeway to look through public-facing social media posts without seeking authorization from their superiors in advance or even keeping an official record of their actions.

The FBI rules, laid out in their handbook and periodically updated Attorney General's guidelines, allow agents to conduct "pre-assessments" of possible threats, German said. Those pre-assessments can be conducted "without any factual basis to suspect wrongdoing," German writes in his report.

He and several other experts agree that the FBI certainly can, then, proactively monitor Americans' social media for signs of unrest, dissent or violence that might lead to criminal activity.

FBI officials told U.S. TODAY this is correct. There's no need for "proper predication," or evidence of a crime, when conducting a pre-assessment of a subject.

German's analysis of the rules was echoed by Brian Murphy, a former top FBI official who helped pioneer the FBI's social media exploitation efforts.

He cited Sanborn's statements, telling U.S. TODAY, "I just think that she was wrong." He said the agency has a risk-averse culture that prevents agents and managers from taking the steps necessary to fully protect Americans.

Sanborn, who is no longer at the FBI, did not respond to messages seeking comment. An FBI spokesperson said Sanborn's comments referred specifically to "conversations" on social media and not to public-facing posts by individuals.

While the bureau describes its authorities carefully, its agents—and third party contractors—can track critics of the government like Adam Bies, watching until their online rantings cross a line into outright threats.

Then the FBI can act.

What SOMEX really looks for

The FBI's SOMEX team, which sits within the agency's National Threat Operations Center in Clarksburg, West Virginia, receives and investigates tips on imminent social media threats from concerned citizens, other law enforcement agencies, independent monitoring organizations and others.

But the effort involves more than just acting as a catcher's mitt for incoming tips. It also develops its own social media intelligence.

Documents obtained by the open-government group Property of the People (and first reported by Rolling Stone) give insight into the broader social media monitoring role SOMEX plays inside the FBI. The documents detail reports from the team to federal and local law enforcement in the Seattle area during the civil unrest that unfolded in the wake of the murder of George Floyd.

"While overnight social media activity was very light, the SOMEX team did find some tweeting by individuals stating they would monitor police radio activity," reads a typical extract from the documents, taken from a June 2, 2020 situation report emailed to dozens of FBI agents.

"The FBI aggressively scours social media for information related to topics of Bureau interest,"

said Ryan Shapiro, executive director and co-founder of the nonprofit group, which provided U.S. TODAY with hundreds of pages of documents about the FBI's social media monitoring that it acquired through open records requests. "This routinely includes surveillance of Americans who are not the subject of an investigation or even suspected of committing a crime."

In a statement, the FBI said that SOMEX was created to assist in identifying "unknown subject, victim, or location information" when there's a threat to life by using publicly available information. The team then forwards information to the appropriate agency for further investigation and appropriate action.

FBI officials told U.S. TODAY that agents are not allowed to use specific SOMEX tools without additional training in privacy and civil liberties protections. Those tools include commercial software the FBI purchases to use in-house. The FBI also works with third-party contractors for social media analysis, the officials said.

One contractor is the private intelligence firm the Hetherington Group, which has trained law enforcement and the military on conducting online investigations.

Cynthia Hetherington, the firm's founder and president, said the company identifies "actionable intelligence" that can be used to protect life or someone's reputation by helping those it trains learn how to hyperfocus and efficiently identify a key collection of terms that demonstrate legitimate threats, such as "kill," "die," "shoot," "fire," "bomb," "rob."

"Individuals should be allowed to say what they want to say on the internet, but should also understand that it's open source and the parties concerned will trace it back" to them, Hetherington said.

Another way of saying that, said Shapiro, who holds a doctorate from the Massachusetts Institute of Technology focusing on government surveillance, is that the FBI can, and is, monitoring practically whoever it wants, whenever it wants.

"The FBI is almost entirely unhindered in its ability to monitor American social media postings," Shapiro said, "So when the FBI reported to Congress that it was unable to do so—I mean, that is a bald-faced lie. That's what the bureau does. They lie."

As the FBI becomes more interested in specific posts, the bureau can also ramp up its monitoring in more "intrusive" ways, FBI officials said. With additional internal approvals, FBI agents can access not just public-facing social media, but also private groups and chat rooms.

Even when accessing this more private information, the FBI's internal checks don't protect Americans' civil liberties, several experts told U.S. TODAY.

The FBI has a long and troubled history of focusing on groups on the left of the political spectrum while largely turning a blind eye to domestic extremists on the far-right, said Guariglia, who holds a doctorate in the history of police surveillance.

"Both historically speaking, and in current events, we've seen the amount of surveillance that has been marshaled specifically against groups fighting for racial justice increased exponentially than from what we've seen being monitored on the right," Guariglia said.

The FBI pushed back on this assessment. "The FBI aggressively investigates threats posed by domestic violent extremists," a bureau spokesperson wrote in a statement. "We do not investigate ideology and we do not investigate particular cases based on the political views of the individuals involved."

Are there enough resources to do the work?

The FBI isn't the only law enforcement agency doing social media exploitation.

The bureau's SOMEX team is part of a constellation of social media analysis that has occurred across the national security apparatus over the few years. The Department of Homeland Security has its own SOMEX team plus social media analysts at dozens of "fusion centers" across

the U.S. sharing intelligence with local, state and federal law enforcement, said Mike Sena, executive director of one of those fusion centers, the Northern California Regional Intelligence Center.

The FBI also works to train and assist local police departments in their social media exploitation efforts, a tactic that came to light earlier this year in a report by the Intercept, which detailed how the bureau provided the Chicago Police Department with fake social media accounts to investigate demonstrators outraged at the Floyd murder by police officers in 2020.

The San Bernardino terrorist attack in 2015 turned out to be a "proof of concept" on the efficacy of social media analysis, Hetherington said, when reporting from Facebook to a fusion center social media analyst helped the FBI quickly identify the people involved.

But using social media analysis to identify future crimes, rather than research past ones, is a broader net. That federal effort to prevent crimes is still small given the scale of the internet, Sena said.

"Most people would be shocked in America," Sena said. "There's a small number of folks trying to deal with these threats that are huge."

Sena and Hetherington told U.S. TODAY that after the ACLU of California publicized law enforcement's use of commercial software to "monitor activists and protesters" in 2016, many companies stopped selling their software to law enforcement or minimized their capacity to use it to track online activity.

As a result, Sena said, "our people are manually doing things, they're doing the work, but they're having to work 10 times as hard as they used to."

That's why agencies plan to bring their teams together, at least virtually, to break up siloes and avoid duplication, Sena said. One byproduct of this effort, he said, will be fewer blindspots or gaps that can be used to accuse law enforcement of bias.

"Even if you're being proactive, it's basically walking with a teaspoon at a river and trying to put that in a bucket," Sena said. "We're not getting everything, but it's better than nothing."

But German argues in his report that the majority of social media exploitation work is actually counterproductive. The sheer volume of tips generated by contractors and the FBI's own analysts results in an "information overload," German writes.

"Obviously, the multiple forms of social media monitoring that the FBI and other law enforcement agencies conducted prior to January 6 was not helpful in preparing for the attack," the report states. "Yet after the Capitol insurrection, the FBI invested an additional $27 million into social media monitoring software, effectively doubling down on a failed methodology."

Ongoing investment in social media exploitation

Those efforts continue even in the weeks since the Mar-a-Lago search and backlash.

Three days after the FBI executed its Aug. 8 search warrant on Mar-a-Lago and was inundated by right-wing threats, Ricky Shiffer, a 42-year-old Navy veteran, walked into the FBI office in Cincinnati armed with a nail gun and an AR-15 rifle.

As U.S. TODAY reported, Shiffer had spent the last nine days of his life ranting on Truth Social, the social media company founded by Trump. His hundreds of posts included explicit threats against the federal government including "Kill F.B.I. on sight."

When his attack failed, Shiffer fled north along rural highways and into a standoff where was ultimately shot and killed.

The FBI said in a statement that it had been informed of Shiffer but that "the information did not contain a specific and credible threat."

Wray told the agency in a message the day after that attack that the FBI's security division would be adjusting its "security posture accordingly."

A $32,400 contract approved Monday—after discussion that started weeks before the search of Mar-a-Lago, Hetherington said—notes that the agency will hire the Hetherington Group to train its agents on SOMEX later this month.

According to a document the bureau filed to justify making the purchase without opening it up to bidding, "it is an immediate need to expand and broaden the social media knowledge for the NTOS SOMEX team." The FBI wrote that the training can provide it with expertise in the "forces and factors that lead to the radicalization of terrorism specifically white supremacy extremism."

That document was filed Aug. 11, the same day Shiffer carried a nail gun into an FBI office, then fled into the Ohio cornfields.

It was also the same day Adam Bies was logging post after post on Gab.

'Why don't you send them my threats'

As Bies tapped out his messages, he wasn't just speaking to his 1,600 followers. According to court documents, he also deliberately tagged Gab founder Andrew Torba in his posts, goading him to report Bies to the federal government.

"Why don't you send them my threats so that they'd at least have something credible to show on Fox News," Bies wrote in the post. "Just scrub my timeline for the posts you didn't delete after you threatened to ban me."

Also watching Bies' posts was a third-party media monitoring and analysis firm, the Middle East Media Research Institute. MEMRI cut its teeth monitoring Middle Eastern media for English-speaking audiences, but over the last three years has expanded to real-time social media monitoring, specifically for threats from white supremacists and other homegrown extremists.

"We're consistently in communication with (law enforcement and government) agencies at the local, state and national level, and providing" them with actionable intelligence, said Simon Purdue, director of MEMRI's Domestic Terror Threat Monitor team. "Having people like us helps speed things along."

MEMRI alerted the FBI, according to a later criminal complaint. The FBI contacted Gab, who handed over Bies' subscriber information and Internet Protocol logs for his computer connection. Soon, agents were outside his Mercer County home.

After a 30 or 40 minute stand-off at his home, Bies eventually emerged carrying an assault rifle, an FBI agent testified in court. Agents told him several times to drop the weapon, which he eventually did.

Had he not done so, the agent testified, according to local media reports, "It would have ended differently."

Bies' son left the house safely. Inside the home, agents found 12 other guns and a compound bow. Bies was taken into custody and charged under a law that covers making threats against a federal law enforcement officer.

He has pleaded not guilty and is being held awaiting trial.

APA citation: FBI agents monitor social media. As domestic threats rise, the question is who they're watching (2022, September 1) retrieved 8 December 2022 from https://techxplore.com/news/2022-09-fbi-agents-social-media-domestic.html