ACLU

SPEAK FREELY

Why Government Use of Social Media Monitoring Software Is a Direct Threat to Our Liberty and Privacy

By Kimberly McCullough, Legislative Director, ACLU of Oregon
MAY 6, 2016 | 3:30 PM

TAGS: Big Data, Surveillance Technologies, Privacy & Technology, Racial Justice, Social Networking Privacy, Internet Privacy

Photo: Rena Schild / Shutterstock.com

A version of this post originally appeared at the ACLU of Oregon.

As we've previously written about, analysts at the Oregon Department of Justice used a tool called Digital Stakeout to surveil people — including the

department's very own director of civil rights — who used over 30 hashtags on social media, such as #BlackLivesMatter and #fuckthepolice. While an internal investigation confirmed the illegal surveillance and made recommendations to ensure it doesn't happen again, much less attention has been paid to the tool itself.

Digital Stakeout is social media monitoring software (SMMS) that can be used to covertly monitor, collect, and analyze our social media data from platforms like Twitter, Facebook, and Instagram. It is part of a rapidly expanding industry that the public knows little about. Our goal here is to answer a few basic questions about SMMS: What can the technology do? How widespread is the use of SMMS by law enforcement in Oregon? What privacy concerns does it raise? And how we can protect free speech and privacy moving forward?

In summary, SMMS is a high-tech tool for surveilling and engineering our future world.

What is SMMS?

SMMS is a booming industry. Products like XI Social Discovery, Geofeedia, Dataminr, Dunami, and SocioSpyder (to name just a few) are being purchased in droves by Fortune 500 companies, politicians, law enforcement, federal agencies, defense contractors, and the military. Even the CIA has a venture fund, In-Q-Tel, that invests in SMMS technology.

This isn't just about searching for key words. Instead, SMMS performs highly sophisticated fishing expeditions across the internet, using complex algorithms to analyze and organize data into much more than a set of search results.

Social media monitoring software can be used to geographically track us as we communicate. It can chart out our relationships, networks, and associations. It can monitor protests, identify the leaders of political and social movements, and measure our influence. It is also promoted as a predictor of future events, including threat assessment, and as an instrument for manipulating public

opinion. In summary, SMMS is a high-tech tool for surveilling and engineering our future world.

By its very nature, SMMS improperly blankets a whole range of innocent people without any evidence of wrongdoing. Instead of specific criminal activity prompting an investigation, investigators use SMMS to cast nets so wide they encompass the entire internet.

What are the risks?

This type of government surveillance raises many privacy concerns. Rather than accepting its use by law enforcement as our inevitable future, we should consider the serious implications for our society.

Silencing discourse. It should give us great pause to hear that SMMS is being used to politically profile, track, and target innocent people who express political opinions online. People like Erious Johnson, director of civil rights at the Oregon Department of Justice, and who knows how many more.

A recent study revealed what really happens when we know we are being constantly watched — voices are silenced. Professor Elizabeth Stoycheff of Wayne State University has shown that people who support surveillance and say they have nothing to hide are actually the most likely to avoid sharing unpopular opinions when they know government is watching. We lose the ability to discuss ideas openly when we fear we will be punished for them.

Even innocent people who know they are being watched are intimidated into self-censorship. Yet robust public conversations and debates about controversial and difficult topics make us stronger as a nation. That is exactly why our founders enshrined strong protections for a broad marketplace of ideas in the First Amendment.

Targeting innocent speech. When everything and everyone is potentially suspect, innocent people become targets. Despite claims to the contrary by the companies that market this technology, we can't accurately predict the future by measuring sentiment and profiling people on the internet. Internet speech

is often hyperbolic and inflammatory, but that doesn't necessarily mean a person or group is dangerous. Internet speech can also be easily misunderstood, particularly when it is interpreted by a system that relies on the biases of its users and programmers.

Making devastating mistakes. False alarms and mistakes, such as mistaking the Public Enemy logo as a threat to law enforcement, can be devastating — even when we are innocent. Unjustly becoming a target can be frightening, feel like an intrusive violation, result in embarrassing and uncomfortable public exposure, and threaten our civil liberties.

Misuse and abuse. SMMS can easily be aimed at anyone who threatens existing power, whistleblowers, people who have reported misconduct, or someone an agent personally dislikes. In a country with a long history of targeting dissent, often in communities of color, we should be wary anytime a tool of this nature is wielded.

Which Oregon law enforcement agencies are using SMMS?

Like many of the ever-evolving and new forms of technological surveillance, it is hard to know just how many law enforcement agencies in Oregon are using SMMS. In fact, when a reporter asked Attorney General Ellen Rosenblum whether the public would have ever learned of the DOJ's tracking of social media hashtags with DigitalStakeout had it not ensnared her own director of civil rights, she said she didn't know.

If national trends are any indication, it is likely there are other agencies in Oregon using this type of powerful surveillance tool. Since we don't know exactly who is using it, we also don't know how SMMS is being used, what policies and training (if any) are being implemented or followed, and who is being watched.

What can we do to protect to our privacy?

As technology gets more and more sophisticated, it is a critical time to protect privacy. It is not about putting blinders on law enforcement but rather about

setting appropriate limits that protect our rights and liberties. Oregon law enforcement and policy makers should consider the following guidelines:

1. **The public needs to know what government agencies use digital surveillance tools, like SMMS, and how extensive their use is.** Ultimately, this comes down to transparency and accountability. Without knowing what our government is doing, we cannot ensure that our rights will be protected or that wrongdoing will be corrected.
2. **The public should have an opportunity to provide input on if, when, and how surveillance tools like SMMS are used.** We should understand the risks and benefits and be involved in the conversations and decision making before government starts using new technologies to watch us. If the risks are too great, particularly if innocent people are bound to get caught up in intrusive government surveillance, we should be allowed to say no, or at the very least, to set strict limits.
3. **Government officials should take a hard look at their use of surveillance technology and regularly report on its use.** More specifically, government agencies should be required to publicly assess privacy risks, adopt strict privacy policies and training, and be proactive to mitigate potential risks before new technology is used. Government agencies should also be required to routinely audit their surveillance systems and regularly report to the community about whether technology is achieving its public safety purpose and whether civil liberties protections are being followed.
4. **There must be clear consequences for violating surveillance rules and policies.** This should include exclusion of evidence in criminal prosecutions, potential termination of anyone engaged in misconduct, fines against the offending agency, and civil rights actions.

We can be safe *and* free, and we must insist on it now.

This post is part of a series exploring what we have learned about the DOJ surveillance of Black Lives Matter in Oregon. Click here to see all of our posts on this topic.

Fight for everyone's rights - support the ACLU.

DONATE NOW

RELATED STORIES

How Artificial Intelligence Can Deepen Racial and Economic Inequities

JULY 13, 2021

Those “Free” Remote Learning Apps Have a High Cost: Your Student’s Privacy

MARCH 27, 2020

STAY INFORMED

Your email address

ZIP code

JOIN OUR NEWSLETTER