On the Internet, No One Knows You're a Cop

Albert Fox Cahn 2022-04-05T15:13:48

Across America, police are using an expansive new power to access private social media content, viewing some of our most intimate moments, with absolutely no judicial oversight. This power isn't some unreported provision of the USA PATRIOT Act, it's not some shadowy executive order. No, the authorization for this sprawling surveillance apparatus is just 3 words long: "Accept friend request." Increasingly, internet surveillance is operating under our consent, as police harness new software platforms to deploy networks of fake accounts, tricking the public into giving up what few privacy protections the law affords. The police can see far beyond what we know is public on these platforms, peaking behind the curtains at what we mean to show and say only to those closest to us. But none of us know these requests come from police, none of us truly consent to this new, invasive form of state surveillance, but this "consent" is enough for the law, enough for the courts, and enough to have our private conversations used against us in a court of law.

Police Use of Fake Social Media Accounts

COVID-19 only accelerated our growing reliance on social media and internet platforms, finding digital community amid the constant separation. Our increased reliance on digital platforms has created increased risk of police surveillance, particularly for young Black and Brown Americans. "Anti-gang" policing has driven officers to scrutinize targets' every Instagram selfie and TikTok clip as a potential clue or even a confession. But while police can and do scour public social media accounts with abandon, they need court approval to access private accounts, that is, unless they have our "consent."

To obtain it, officers don't simply stroll up and ask if we'd like to be targets of a police investigation. Instead, they increasingly turn to internet attribution software or technology sold by private vendors to deploy large numbers of fake credentials. One police officer can run a bot network of hundreds or thousands of fake accounts. These accounts are used to harvest private messages and posts for local police databases. Private vendors of social media monitoring software tout their ability to allow bulk creation of undercover accounts and to store unlimited numbers of them in databases.

Private vendors are enabling the deception, selling spying technology to police departments. The LAPD pursued a contract with Voyager Labs to use a software product that allowed them to conduct undercover monitoring using fake social media profiles. As documented by the Brennan Center for Justice, the software surveils more than just the suspect, but also collects data on everyone they know on the platform. These sprawling networks of surveillance are deemed permissible based

on the “consent” given by only the single individual who accepts a request from an officer’s fake account, a remarkably tenuous basis.

Replicating the Harmful Patterns of Undercover Policing

Police use this deceit to replicate the federal government’s bulk data collection programs, mapping out networks of people based on their political and religious beliefs.

This new form of deceptive policing is a digital version of the infiltration of Muslim communities in the post-9/11 era. For more than a decade, undercover officers and informants systemically targeted Muslim New Yorkers for simply practicing their faith, attempting to monitor conversations that took place in mosques, Muslim-owned businesses, religious schools, and community groups. While this program failed to generate even a single credible lead, it sent a clear message to Muslim New Yorkers that their conversations would be watched. Through fake social media accounts, police can replicate this infiltration for online communication, monitoring Facebook groups, WhatsApp chats, and other digital community spaces. Just because this activity is taking place online, it does not make it any less intimate and sensitive, and certainly does not erode the First Amendment interests at stake.

Voyager Labs claims to perceive people’s motives and identify those “most engaged in their hearts” about their ideologies. As part of their marketing materials, they touted retrospective analysis they claimed could have predicted criminal activity before it took place based on social media monitoring. However, the case studies reveal monitoring tools that are designed to profile users for the faith they practice today, not for crimes they might commit tomorrow. Much of the content flagged shows nothing more than the fact that the targets practice Islam or are of Arab descent.

In Memphis, Tennessee, police used multiple fake Facebook accounts to surveil Black Lives Matter activists, accessing private posts and even cataloguing the names of people who had “liked” those posts. The disturbing practice only came to light after activists were arrested, leading Facebook to urge the department to stop the practice.

Police systematically target youth, stifling their ability to engage with the digital communities that we take for granted. Children and teens are increasingly weary of the presence of police online, often self-censoring communications to avoid the danger of being swept up in these digital dragnets. They enjoy a First Amendment right to unfettered internet communications in theory, but they face a very different reality in practice.

Protecting Our Private Communications

As long as police can continue to exploit the legal fiction of user “consent” to access our private communications, our privacy rights will remain just as fictional. While we’re hopeful that the courts will one-day strike this practice down as violating the Fourth Amendment, more urgent statutory protections are needed. The legislation needn’t be lengthy or complex, it’s not a nuanced question. To the contrary, what we need is a complete and categorical ban on the use of fake accounts by police, letting those who’ve been surveilled sue, and suppressing the evidence that’s obtained at trial. The practices have thus-far evaded public scrutiny, with departments refusing to disclose the number of fake accounts they maintain. Left unchecked, this threat to our private communications will only grow. As more of our lives move onto digital platforms, as our real world becomes ever more displaced by augmented and virtual realities, the vaunted rise of the metaverse, much more of what we say will be susceptible to police tracking through these tactics. Yes, we can train the public to be more skeptical of granting consent, yes tech platforms can make it harder for police, but ultimately, none of these steps are a substitute for robust privacy protections that can’t simply be clicked away.
