STREET LEVEL SURVEILLANCE

SOCIAL MEDIA MONITORING

How It Works

Social media includes some of the most intimate details of our lives, including our health information, likes and dislikes, political views and religious beliefs, sexual orientation, and people with whom we associate. Its content includes usernames, bios, contact information, status updates, comments, photos, videos and streams, event postings, friend or follower lists, friend requests, groups, private messages, account creation dates, location, and more.

Law enforcement agencies including the Department of Homeland Security and U.S. Immigration and Customs Enforcement monitor the social media posts of asylum seekers, tourists seeking visa waivers, or people applying for immigration benefits. Social media information is collected from travelers–including American residents–even when they are not suspected of any illegal activity. This surveillance extends to anyone in these people's networks. The Department of Homeland Security has offered no transparency about its multi-million dollar program of spying on immigrants' and other foreign visitors' social media posts, which it uses as evidence in deportations and visa denials.

While this has typically been done to surveil political activists, at times this has been much broader. For example, LAPD officers were ordered to note the social media information (including Facebook, Instagram, Twitter, and other social media accounts) of every civilian they questioned, according to an internal July 2020 memo obtained by the Brennan Center. This included those who were not arrested or even accused of a crime, let alone found guilty of committing one.

Police may combine social media monitoring with other technologies, such as face recognition, to identify individuals.

Since social media posts are highly contextual, police may misinterpret innocuous language, song lyrics, or inside jokes, leading to criminal consequences for individuals who may not have even been aware they were under surveillance.

How Law Enforcement Monitors Social Media

Police may use a fake account to search through publicly available posts for names of groups or individuals, or for specific keywords and hashtags. They can scour social media pages and groups to determine names and affiliations of people posting in the group, the time of a planned event, and other information.

In addition to monitoring asylum seekers and tourists, police have used social media monitoring to gather information about planned protests or activities, identify protesters and protest organizers, data mine information in an attempt to learn identities and affiliations of people engaged in legally protected conduct, or search for what they perceive as threats to national security.

Sometimes they may want additional information that's not publicly available, or that would take too long to scrape. They may use a subpoena or warrant to request social media data as part of a criminal investigation.

But police officers have also set up fake or imposter accounts. For example, in 2010 a DEA agent created a phony Facebook account in the name of a young woman without her knowledge or consent, even posting photos from her seized photos, including pictures of her son and niece, who were young children. He then sent a friend request and accepted other friend requests from this imposter account. DHS created fake profiles and pages to trick immigrants into registering with a fake college called The University of Farmington. This led to more than 170 arrests. And the Memphis Police Department created fake profiles to monitor Black Lives Matter activists.

swaths of social media data. These tools often allow police to search by hashtag or keyword and which may even generate profiles and predictions.

For example, the United States Postal Inspection Service, the law enforcement arm of the post office, were found to have conducted blanket keyword searches (such as "protest," "destroy," and "attack") across social media in its iCOP surveillance program. The Office of Inspector General later determined that the USPIS did not have legal authority for these searches, since they were not connected to mail or the post office.

Who Sells It

Police have used firms such as Babbel Street, Cobwebs, COGITO, Dataminr, DigitalStakeout, EDGE NPD (ABTShield), Geofeedia, Giant Oak (GOST), Kapow Software, Kaseware, LookingGlass Cyber Solutions, Media Sonar, NICE (NiceTrack Intelligence Services), NTREPID, Palantir Technologies, Pen-Link, ShadowDragon (SocialNet, OIMonitor), Skopenow, and Voyager Analytics.

Due to a lack of transparency on these tools, information is only gleaned from documents obtained via public records requests, some of which are several years old. It's therefore not entirely clear which of these firms are still being used and by whom. There are likely other firms not on the list. Additionally, some of these firms are no longer used by law enforcement, which may be due to a loss of access to data. For example, police have used Geofeedia in the past. Technology companies including Facebook, Instagram, and Twitter gave Geofeedia special access to its APIs. However, Geofeedia lost access to this data shortly after responses to ACLU of North California's public records requests showed that the company was pitching its product as a resource to surveil people lawfully protesting against police violence.

Some tools combine social media history with other information. For example, the data mining company Palantir provided software to the New Orleans Police Department. The software combined social media history with additional data for its so-called predictive policing, or an attempt to predict the likelihood that certain individuals would commit acts of violence or become victims themselves. Additionally, the Minneapolis Police Department used Clearview AI to power its facial recognition, and Clearview AI scraped billions of photos from social media.

Police have also created dossiers of individuals, combining social media data with other information. For example, Customs and Border Patrol was found to have inappropriately

at the U.S.-Mexico border in Tijuana, Mexico.

Threats Posed by Social Media Monitoring

Social media monitoring can chill protected speech and association due to a valid fear someone engaging in protected speech or simply traveling to the U.S. may have of being screened for their political opinion, being subjected to increased interrogation (or even not allowed into the country), exposing others to surveillance, being included in a police database, or even facing criminal charges.

Social media monitoring has indeed been used to target nonviolent protesters engaging in protected speech. ICE kept tabs on anti-Trump protesters in New York City, LAPD monitored social media accounts belonging to both protesters and journalists during protests following the murder of George Floyd, seeking copies of communications containing the keywords "black lives matter," "BLM," "demonstration," "protest," and "protester." It also monitored terms such as #BLMLA, #SayHerName, Sandra Bland, Tamir Rice, #fuckdonaldtrump and the names of other people killed by LA police. DHS collected data on Black Lives Matter activities posted on social media accounts even for events expected to be peaceful. LookingGlass Cyber Solutions gathered information on more than 600 protests against forced family separation. It shared the information it had gathered with DHS and state fusion centers.

Some law enforcement agencies didn't just surveil Black-led protests against police violence, but other events as well. For example, a fusion center in Texas surveilled not just protests but also social gatherings and Black cultural events, including a Juneteenth celebration that took place online. It then shared organizer names and social media information, notable guests, and attendance numbers with other law enforcement agencies on the local, state, and federal levels. Similarly, DHS circulated information on a nationwide series of silent vigils. It planned to monitor a community parade in the predominantly black neighborhood Congress Heights, a funk parade in the historically black neighborhood of U Street, and a walk to end breast cancer.

Although social media monitoring allows law enforcement to monitor thousands of accounts with the push of a single button, it is subject to extremely minimal oversight and transparency. It is also highly susceptible to misinterpretation. Since social media posts are highly contextual, police may misinterpret innocuous language, leading to severe consequences for individuals who may not have even been aware they were under surveillance. Police and prosecutors have also used Facebook photos, "likes," photos, and associations to make false allegations of criminal gang activity.

threats to national security. Interpretation may be even more difficult for non-English languages and unknown cultural contexts.

It is not always easy to correctly link an individual with their account. Exacerbating this problem is the fact that so many law enforcement agencies partner with data mining companies, they risk adding large amounts of unverified information into their databases. This data is often shared with other organizations, all with different retention policies. The longer the data sits in their system, the more opportunity there is for misuse.

EFF's Work Related to Social Media Monitoring

We sued DHS under the Freedom of Information Act (FOIA) to obtain records on its Visa Lifecycle Vetting Initiative, its social media program to spy on immigrants. DHS released no records in response to the request, which is unacceptable and illegal. We are seeking information on the program's current status, including whether the government is monitoring people's social media profiles and for what purpose, how this impacts visa approvals and denials, and details about a $4.8 million transaction last spring. We are also requesting VLVI contracts, notes on how the program works, performance work statements, recent datasets used for input, training materials, operating procedures, privacy impact statements, audits, and reports to legislative bodies.

EFF opposes the U.S. government's monitoring of anyone's social media accounts and internet activity, and in this case, the government is targeting potential immigrants who risk being unfairly labeled a threat and denied access into the U.S. EFF previously urged DHS to abandon any such vetting program because social media surveillance invades privacy and violates the First Amendment by chilling speech and allowing the government to target and punish people for expressing views it doesn't like. Any vetting based on speech on social media would be ineffective and discriminatory.

We also sued the U.S. Postal Service and its inspection agency seeking records about a covert program to secretly comb through online posts of social media users before street protests, raising concerns about chilling the privacy and expressive activity of internet users.

Working with the Samuelson Law Technology and Public Policy Clinic at the University of California Berkeley School of Law (Samuelson Clinic), we filed suit on December 1 2009 against a half-dozen government agencies for refusing to disclose their policies for using social networking sites for investigations data-collection and surveillance.

Facebook by calling on Meta to publish the number of such accounts it has identified in its regular transparency reports, along with information on which agencies the accounts belonged to and what action was taken. We have also pushed the company to alert users and groups that interacted with these fake or impersonator accounts, to amend its documentation for U.S. governments to make their terms barring such accounts more explicit, and to take steps to notify departments that have a written policy of engaging in this behavior that it is in violation of their rules.

EFF Legal Cases

EFF v. DHS (VLVI)

EFF v. USPS

Suggested Additional Reading

The Public Has a Right to Know How DHS is Spending Millions to Spy on Immigrants on Social Media

Four Steps Facebook Should Take to Counter Police Sock Puppets

Social Media Monitoring | Brennan Center for Justice

LAPD Social Media Monitoring Documents | Brennan Center for Justice

Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color | ACLU of Northern CA

How to reform police monitoring of social media

TECHNOLOGIES