Nina Moini and Ellen Finn
January 12, 2026 3:00 PM

How ICE uses phone and internet data to identify and track people

People listen to clergy and faith leaders call for accountability at the site where Renee Good was killed by an ICE agent in Minneapolis on Jan. 8.
Ben Hovland | MPR News

ListenMinnesota Now - How ICE uses phone and internet data to identify and track people
Save
SHARE

What acting ICE Director Todd Lyons called the “largest immigration enforcement operation ever” continues to unfold in Minnesota. And we are learning about the tools federal law enforcement agents use to track the people they're trying to arrest, as well as protesters.

ICE recently purchased two programs called Tangles and Webloc, which are used to track the cell phone activity of entire neighborhoods and monitor people over social media and through internet data, according to reporting by 404 Media. 404 Media journalist Joseph Cox joined MPR News host Nina Moini with insight on those tools and how they’re used to track people.

The following has been edited for length and clarity. Use the audio player above to listen to the full conversation.

People are curious about how much surveillance is going on in society in general these days — and that includes ICE. Let’s start with one of the tools ICE is using: Tangles.

Tangles is a social media monitoring tool. We've seen that before, where companies will scrape sites like Twitter or Bluesky and then make that information much more accessible to the authorities.

What's different here is that Tangles is in combination with the tool call Webloc, the other tool we'll speak about in a minute. But it sort of gives an all-in-one solution for following people online. When it comes to their social media activity, ICE officials can add them to a watch list so they will be alerted whenever this person posts.

They are able to use AI to build some sort of sentiment analysis about what they're posting as well. The idea is that whenever somebody posts something online that ICE is interested in, the officials are going to see it.

How does the program obtain the location data from the phones in the first place? For example, what if you're a person who turns your location off?

If you turn your location off, that is actually probably a very, very good thing to do if you are trying to get around this sort of surveillance. It does not get the data from the telecoms. It doesn't get it from AT&T, Verizon, T-Mobile, that sort of thing. It actually gets it, weirdly, through the online advertising ecosystem.

So whenever that little advert loads in your app, in Candy Crush or whatever, you'll see an advert there in the background. There's all of this tech going on where different companies are trying to get that advertisement in front of you.

There are also spy companies essentially harvesting that data, including phone location data. They then sell access to that to the government. It's basically a side product of the advertising ecosystem we see every day. But of course, somebody who is browsing the internet or just using an app has no idea that this is happening in the background.

What about this other program that ICE is using, Webloc? How does it work?

Webloc obtains information likely that same way — the location data — and it allows a user, in this case ICE, to search a map-style interface for phones and, by extension, people they might be interested in.

You log into the interface, you draw a circle or rectangle around a place of interest, maybe an ICE facility, maybe somewhere where a protest is happening. It then shows all of the location data and phones it has for that location, and the user is able to then track the phones to other places. So maybe this phone went over here and it stayed here overnight. Well, that's probably where the person slept. That is probably where the person lives. You track the phone to another location during the day after a protest. Well, maybe that's where this person works. So it allows users of this program to figure out probably who these people are and where else they're going after the fact.

And of course, that could be useful for ICE in many different contexts. The Wall Street Journal years ago, reported ICE was already using this sort of location data to catch immigrants and Customs and Border Protection was using it to monitor the U.S.-Mexico border as well.

What do you know about how these tools are being used so far here in Minnesota?

That is, unfortunately, the one thing we really don't know. And of course, I would love to have more information on that. All we know is that this tool was bought for millions of dollars. I obtained the information about how it works, but we don't know what exactly they're using it for.

Now, what I would do again is point to that earlier Wall Street Journal reporting where this has been used to catch people that ICE wishes to catch, and it has been used by other parts of DHS to monitor the border. The only thing I would add on there is that, at least in marketing material, the company behind this technology has sort of floated the idea of using it to monitor Black Lives Matter protests as well. So First Amendment protected activity has come up explicitly in the marketing material for this technology.

How have you found that these types of tools are typically used? Is it about mass deportation efforts or is it about tracking protesters?

What I would say is that from everything I've learned, from looking at material from this company others and speaking to government officials as well, these sorts of tools for ICE and other agencies are really good for looking at movements of people or groups of people.

It can actually be quite difficult for ICE to focus on a particular phone and, by extension, the person. They almost have to be lucky that the target is included in that particular data set. But if you see a big group of phones moving to a certain location or away from it, that is probably how this technology is best going to be used.

A U.S. government official told me this data is definitely not as useful as the stuff you would get from AT&T, but that would require a warrant, whereas this data, crucially, they don't need a warrant to use it because they're simply buying it from a government contractor.

What can people concerned about being tracked do about this? Do they have any legal protection? How can people better control whether they're being tracked?

Yeah, you're right about the legal protection. Unfortunately, there doesn't seem to be much around this sort of data at all. On a more technical level, it is simply being more aware of the things you're installing on your phone. Maybe you downloaded a flashlight app and it's requesting location data. Well, does it really need that permission that's requested on my phone? Maybe you can deny that, maybe you can delete that app.

And of course, getting some sort of ad blocker potentially could help. But as I said earlier, I think turning off location services is probably the more solid and robust way to combat this, if you wish to do so.

But no, there isn't really a legal protection. It's more a technical protection that you have to do yourself as an individual phone user.