# How police might access your Lyft, Tinder and Google accounts in a criminal investigation

*The extensive data that tech companies collect from their users is an invaluable resource for police officers trying to solve crimes. But in order to identify a culprit, police often have to comb through the information of innocent people.*

By Erica Evans
Deseret News
July 28, 2019
https://www.deseretnews.com/article/900081368/lyft-tinder-google-police-data-mackenzie-lueck.html

SALT LAKE CITY — Buried in the terms of service agreements people accept when they sign up for most smartphone apps is a clause that says their personal information could be shared with law enforcement.

Increasingly, police are using that data to identify suspects and solve crimes, said Joseph Giacalone, a retired New York Police Department detective who now teaches at John Jay College in New York City. Police use of data from apps has grown "infinitely" in the past five years "with no abatement in sight," he said.

Tech companies track and record nearly every move users make in order to improve their services and make money from selling the data to marketers. That means today's police officers have the ability to discover people's locations, what they search for on the Internet, what they buy and who they communicate with, in addition to the contents of their private messages, texts or emails.

The fact that tech companies build such detailed profiles of users' daily activities and whereabouts is a boon to investigators seeking to identify dangerous people and keep the public safe. But in order to find a culprit, police often have to comb through innocent people's information, in some cases without a warrant and without demonstrating probable cause.

" Everyone has basically given up their right to privacy on the internet. You trade your privacy for the convenience of using these apps. "
Joseph Giacalone, a retired New York Police Department detective
This could result in police viewing sensitive information about a person when it's not pertinent to an investigation and innocent people becoming suspects based on coincidental connections to a crime.

"Everyone has basically given up their right to privacy on the internet," Giacalone said. "You trade your privacy for the convenience of using these apps."

Recently in Utah, Salt Lake City police worked with the ride-hailing company Lyft to discover where 23-year-old University of Utah student Mackenzie Lueck went on the night of her disappearance and to rule out the driver as a suspect. Police also analyzed Lueck's social media and dating app accounts, according to news reports. Eventually, law enforcement located Lueck's body and arrested a man who is suspected of killing her.

Public information officer Greg Wilking was not able to reveal details of the investigation but told the Deseret News that Salt Lake City police used warrants to access necessary information.

Thanks to a privacy law passed earlier this year, Utah is one of a minority of states, including Washington and California, that require police to obtain a warrant to access stored data, like messages and photos, or location information from tech companies and cell service providers. Elsewhere, officers are able to request and view private data without a warrant, as long as providers cooperate.

That's because companies have full ownership and control over the data they collect. Some companies encrypt certain content so it can only be viewed by the sender and intended recipient. Apple's iMessages and Facebook's WhatsApp are encrypted, and therefore that content is not accessible to company employees or police. But typical SMS text messages and most other forms of electronic communication are not encrypted.

The large amount of data law enforcement can access has the potential to snare the innocent, even if police use a warrant, according to Riana Pfefferkorn, associate director of surveillance and cybersecurity at Stanford's Center for Internet and Society.

In April, The New York Times reported that a man named Jorge Molina from a suburb of Phoenix was wrongfully arrested on suspicion of murder and jailed. Police obtained a warrant that required Google to provide information on all devices it recorded near the location of the killing. They found Molina's phone was in the area at the suspected time of the crime. His car also matched the make and model of the one in surveillance footage.

Molina, 24, told The New York Times he was shocked that police were able to arrest him based largely on data and feared it would take months or years to be exonerated. Luckily, it only took police a week to recognize their mistake.

"Absolutely, requests for large swaths of data increase the chances for innocent people to be swept up in investigations," said Pfefferkorn.

"Users should know and be aware that their information can be disclosed to law enforcement," she added. "As we continue to deepen the amount of data we generate about ourselves, there will naturally be a move for police to get access to that."

**What it takes for police to get into your data**

If you're an innocent person who happens to walk near the scene of a murder, uses a dating app that matches you with someone who later goes missing or has a Facebook friend who sells drugs, how likely is it that police will search through your private information?

While states like Utah, as well as many tech companies, have rules that require police to file a subpoena or obtain a warrant in order to access personal data, there are no real limits on how much information police can request. Rather, police self-restrict their own data collection based on time constraints, said Gary Ernsdorff, a senior prosecutor in Washington state who has sought data from Lyft, Uber, Facebook and Google.

"Law enforcement does not have the time and resources to snoop for snooping's sake," said Ernsdorff. "If you had a private, intimate conversation with a victim, that's going to be exposed to law enforcement for a very defendable reason. If your conversation was a month ago, the odds of someone reading it go down dramatically."

Facebook and Instagram require police to obtain a warrant in order to see the stored contents of an account, such as messages, photos, comments and location information. But police can get other information like your name, address and telephone number, credit card information and IP address (used to identify the computer used to sign into an account), with a subpoena, which, unlike a warrant, does not require a demonstration of probable cause of suspicion.

Other companies have rules that are more vague. Snapchat's says, "We may share information about you if we reasonably believe that disclosing the information is needed to comply with any valid legal process, governmental request or applicable law, rule or regulation."

Emergency exceptions allow police to request information without a subpoena or warrant if someone's safety is in danger.

"You can see how the emergency carveout could be vulnerable to potential abuse as well," said Pfefferkorn. "Law enforcement might portray something as being an emergency when they do in fact have the time and opportunity to get a warrant."

She added that providers might feel pressure to comply with an emergency request because they want to have a good relationship with government.

Ernsdorff said he is aware of cases where law enforcement overstepped its bounds and sought more information than was reasonably needed for an investigation. In the past, he said, law enforcement "didn't grasp the magnitude of data out there and the privacy implications."

Now, police and judges are learning and getting better at making sure warrants are narrowly focused, he said.

When it comes to Google location data, law enforcement may request data from hundreds of accounts that appeared in a certain area during a certain time, but that data will be anonymized until investigators identify a handful of accounts that are of interest.

“We don’t want to be intruding on private matters that are not evidence of a crime. Because we understand the privacy concerns,” said Ernsdorff.

**Concerns about surveillance**

With all the data that exists about people’s daily interactions, Pfefferkorn fears we are moving toward a world where it is impossible to do anything privately.

In 2015, records obtained by the American Civil Liberties Union of Northern California revealed that a police department in Fresno used a social media monitoring firm that boasted it could “avoid the warrant process when identifying social media accounts for particular individuals,” and could “identify threats to public safety” by monitoring terms including “police brutality,”“dissent” and “black lives matter.” Other law enforcement agencies in California used a similar service with marketing materials that referred to unions and activist groups as “overt threats,” the American Civil Liberties Union reported.

“People should be free to live their lives without the worry of being surveilled at all times,” said Pfefferkorn, who is particularly concerned about police access to a growing trove of data.

Matthew Tokson, associate professor of law at the University of Utah, is less concerned that police have access to personal data and more concerned that it is being collected in the first place.

“There are so many forms of personal information that are easy to access and so many ways for private companies to record what you are doing and saying,” said Tokson. “It’s the private side that is eroding privacy by collecting and selling all this data. Anyone might be able to get their hands on it, including the police.”

Ernsdorff said he has tried to reduce his own data footprint and realized it's nearly impossible to live in the modern world and avoid using the everyday technologies that gather personal data.

"Even very wary people are still leaving a trail," Ernsdorff said. He simply advises people to be aware of the information they are giving away.

Last year in June, the Supreme Court revised its long-held “reasonable expectation of privacy” test and ruled in Carpenter vs. USA that police need a warrant to obtain seven days or more of location data from cell phone carriers or tech companies. When it comes to requesting six days or fewer of location data, the ruling provides little guidance.

According to Tokson, this Supreme Court ruling and Utah's privacy law passed earlier this year are "steps in the right direction." Utah's law states that location information and stored data obtained without a warrant will be excluded from evidence, "as if the records were obtained in violation of the Fourth Amendment." Tokson says the law is a model for others states when it comes to protecting privacy in a digital world.

While lawmakers are gradually updating privacy laws, Tokson said the process is not happening quickly enough and that the nation is behind when it comes to accounting for new forms of data collection and technology such as facial recognition, drones and smart home devices.

"These technologies are the new frontier," said Tokson. "We need more controls that will keep up with the technology as it develops."