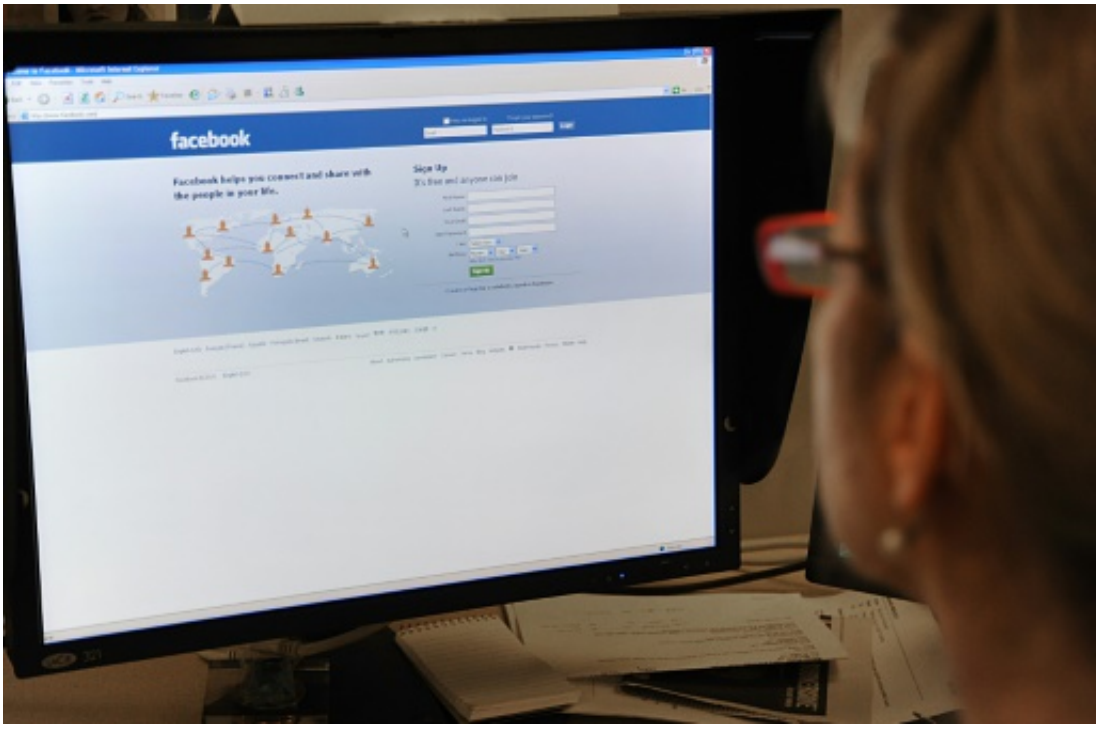
Online sharing a treasure trove for snoops

October 19 2016, by Sophie Estienne



Social networks offer windows into people's lives, and exploiting those insights is big business—with some sounding the alarm over the ever-growing intrusion from corporations and governments alike

They show what we like, reveal who we've been with and flag where we are going.

Social networks offer windows into people's lives, and exploiting those insights is big business—with some sounding the alarm over the ever-growing intrusion from corporations and governments alike.

"There is a thin line of difference between surveillance of individuals and monitoring for research purposes," Gartner analyst Jenny Sussin told AFP.

Even when espionage is not the original goal, nothing prevents someone from creating streams of Twitter posts based on where information is shared or who is doing the sharing.

Twitter and Facebook last week revoked data access for an analytics firm which, according to a civil liberties group, helped law enforcement track people protesting the police shooting of black men in several US cities.

The American Civil Liberties Union reported that Geofeedia had been marketing its services to US police agencies to help track activists using their social media posts and location data.

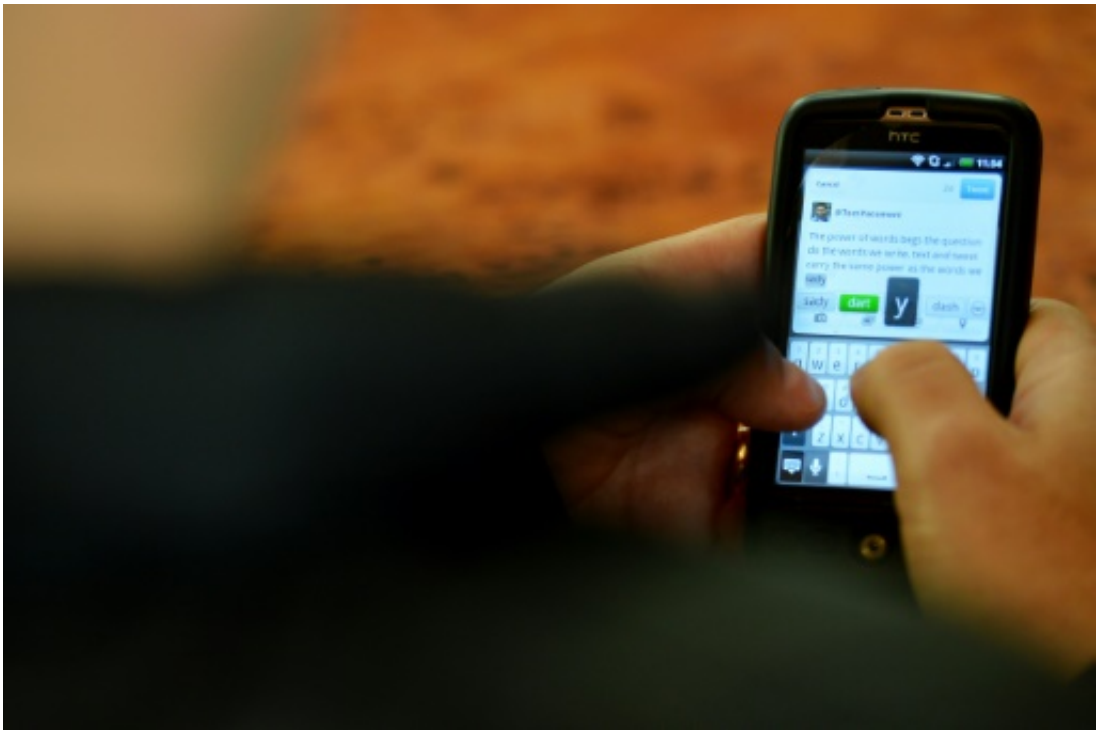
According to internal documents published by the ACLU, Geofeedia boasted that it "covered Ferguson/Mike Brown nationally with great success," referring to the wave of protests in the Missouri community after the shooting of an unarmed African-American man.

The ACLU documents showed that Geofeedia claimed to have access to the Twitter "firehose" or full stream of data which can be analyzed and interpreted by location and other factors.

Geofeedia is one of an array of companies built on the ability to mine insights from the massive amount of information freely shared on social networks.

Twitter had previously barred US intelligence from using the Dataminr analytical tool to scan missives sent via the one-to-many messaging service.

The ACLU, however, wants online social networks to ramp up efforts with moves that include the blocking of applications used as tools for spying or police surveillance.



Twitter and Facebook last week revoked data access for an analytics firm which, according to a civil liberties group, helped law enforcement track people

Companies processing people's personal data have a responsibility to find out who the end user is going to be, Sophia Cope, a lawyer specializing in civil liberties at the Electronic Frontier Foundation (EFF).

She encourages firms to ask specific questions to find out what use the data will be put to.

Privacy vs Security

The degree to which internet firms should cooperate with police or intelligence services is a long-running debate.

In France, there were concerns that data-mining companies put their software to work for parties interested in monitoring opponents of regimes in Libya or Syria.

Internet pioneer Yahoo was recently accused of scanning messages at its email service for a snippet being sought by US authorities.

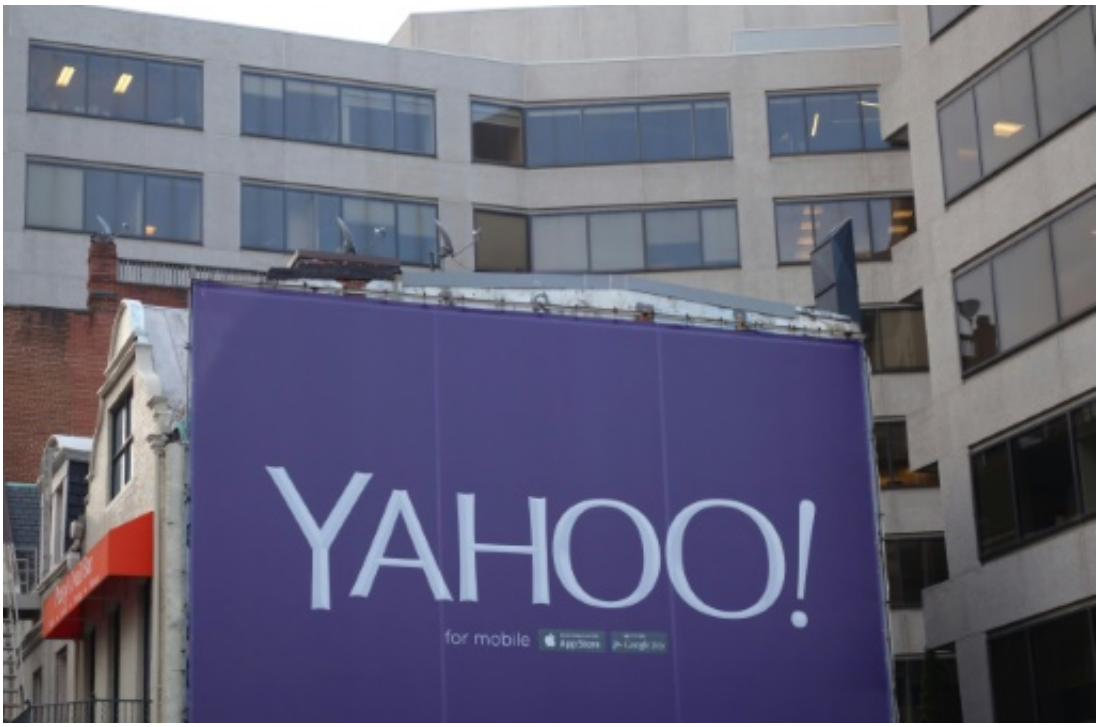
Social networks, however, differ in that the data being perused is typically on public display and not private.

The US government has employees who monitor social networks, but the time and effort involved has created business opportunity for companies such as Geofeedia.

Analytics firms often have the advantage of being directly connected, usually for a fee, to streams of data at social networks.

This lets the process of drawing out details, insights or patterns be done automatically with software that promises to only get smarter due to improvements in artificial intelligence.

Use of the data can range from benign to troubling.



Internet pioneer Yahoo was recently accused of scanning messages at its email service for a snippet being sought by US authorities

Data mined by firms can help target ads, meaning that people see marketing messages that might spark interest instead of annoyance.

Researchers can seek clues to causes or spreads of illness, or measure public sentiment during political campaigns.

IBM announced this summer a collaboration with a Brazilian research center to track the spread of diseases such as Zika, dengue or Chikungunya by studying Twitter posts.

In Los Angeles, the Department of Justice funded research to see if the police could prevent racist crimes by figuring out where hateful comments on social networks were originating to determine at-risk

neighborhoods.

Analysis of social media data can also be abused, Cope cautioned.

For her, any kind of monitoring is problematic but government keeping tabs on people comes with the added offense of violating constitutional rights.

Think before posting

Facebook, Twitter and other online venues use terms of service that set limits on what those tapping into data are permitted to do with the information.

Sussin would like to see internet firms do more to make people mindful of moments when they are sharing their locations.

"You voluntarily participate in your own monitoring," said Endpoint Technologies Analyst Roger Kay.

"Many people live their lives quite publicly," allowing spies, or criminals to track them, the analyst maintained.

In one dramatic illustration: images shared by social media queen Kim Kardashian were believed to have played a role in her being robbed in Paris recently. She has since become much more discreet.

Citation: Online sharing a treasure trove for snoops (2016, October 19) retrieved 25 April 2024 from https://phys.org/news/2016-10-online-treasure-trove-snoops.html