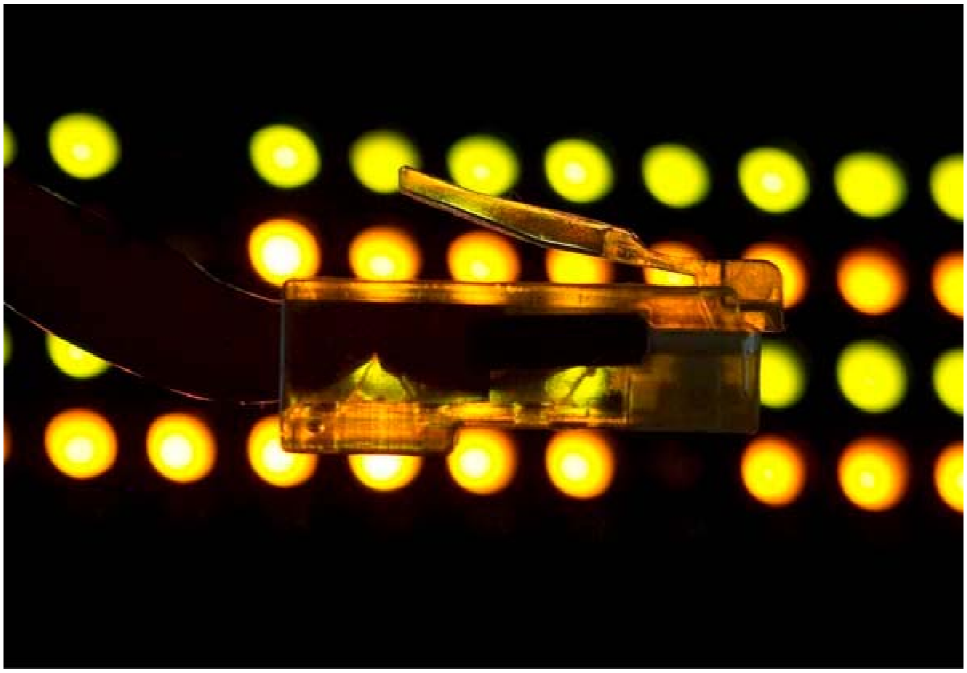
The withering of secrecy: Technology reveals your life on social media

B.C. company combines public data with social media feeds to reveal shocking results

BY GILLIAN SHAW, VANCOUVER SUN MARCH 31, 2014



Social media musings are never secret.
Photograph by: Adrian Wyld, CP

VANCOUVER — How easy is it to use social media to find out what people are doing, without them realizing they are being watched? It took me less than two minutes to not only identify where

a randomly chosen 16-yearold girl lives, goes to school and hangs out with friends, but also to pinpoint within three houses where she babysits. And when she's home alone with the kids.

From the Google Street View of those houses, it's a fair guess she is at the one with all the toys in the yard.

I learned she plays soccer, is in French immersion, and is probably a skier or snowboarder if the resort where she spent Spring Break is any indication. I can probably correctly identify where she went to elementary school. I know what she looks like, and I can recognize her friends. And once I know where she lives, it's not a big stretch to guess her parents' identity.

Creepy? Yes. Hard to do? No. Just ask Karl Swannie, founder of Victoria technology start-up EchoSec, a company that has created a search engine that mines close to 500 data feeds, including social media networks and open data from governments and the private sector - the search engine I used to randomly pick out a traveller at the Vancouver airport to see how much I could learn from their digital trail.

If it hadn't been for EchoSec aggregating everything posted from a location in a single search, it would have been difficult to pick out the teen's single Twitter post from millions of others. What sets EchoSec apart from other search technology is its ability to "geo-fence" - that is, to draw a virtual line around a building or an area, and to tap into all the publicly available data from that location. That means not only social media feeds but open data that could include everything from live webcam feeds to government information.

"It definitely opened my eyes," said Swannie. "There's a level of education that has to happen out there. People have to be aware that (their digital postings are) permanent, it's public. This is definitely a new way to visualize the data."

The public version of Echo-Sec's search technology that I was using has only a handful of feeds. The full version will have close to 500 sources of information that can deliver everything from the risky to the risqué.

The ability to track kids by targeting a school building worried Swannie so much that he disabled the software that made it easy to track an individual. Not that someone still couldn't do it themselves, though.

And he is warning police, governments, companies and even military organizations that they should be aware information is being shared that is timestamped, traceable, and can be "mined, followed and predicted."

Freely available Swannie's company stumbled across its discovery by accident while it was working on a search engine to help urban planners determine how people use public spaces. But the information its search engine taps is freely available, and anyone with the time, the inclination and the tech talent could create similar tracking tools.

"Everything that we're doing is public information," said Swannie. "We're not digging deep. This is stuff that you can freely find."

Using his company's search engine, Swannie draws a circle around a local high school on a map.

From a cloud of icons indicating everything from Twitter posts to Instagram photos, Swannie picks one tweet - from a teenage girl. Another click and clusters of posts indicate where the teen spends most of her time.

"This is where she goes to school," says Swannie, hovering the cursor on one cloud of social media posts. "And this is probably where she lives," he says, hovering on another cluster of tweets.

Google Street View opens and a couple of houses come into view.

"Probably in one of those houses," adds Swannie.

EchoSec's search engine - which mines photos, text and other information posted by social media users and links it to maps - reflects a trend that is seeing companies manipulate large amounts of data in a way that is raising concerns among privacy advocates and prompting warnings from Internet and child safety experts.

"Just because information has been posted and the individual has said yes to Twitter to geo-locate their posts, they don't understand that there are other companies that may be out there mining that data, mashing it up with other data, and creating these new tools," said B.C.'s Information and Privacy Commissioner Elizabeth Denham. "I do think there's a problem in the chain of consent and the kind of ecosystem that has developed around the use of data, and social media in particular.

"It's complicated, but at the end of the day, individuals have a right to know how their information is being used by companies."

EchoSec's search engine depends on the geo-location feature prominent with many social networks - it could be someone checking in on Four-Square (a social media network that identifies a user's location), or someone on Twitter or another social network opting to have public posts appear with location information based on GPS-provided latitude and longitude.

The information is public, but unless someone knows exactly what they are looking for, it's likely to be inaccessible.

EchoSec's full search engine can reveal far more information than the public version, and privacy and security experts point out that others can tap into the same available data - both for good (law enforcement) and for bad.

"I think geo-fencing and this kind of creep factor is something that we all really need to look at," said Denham.

Her office has had discussions with EchoSec and other companies that are developing new technologies, and encourage them to think about privacy implications.

"The technology itself is neutral, but depending on how the technology is used and implemented and whether it's used by government or by commercial enterprises or individuals, they all have different implications," said Denham. "It's a pretty complex area."

Denham said open data is a good concept, "but we really need to think it through because it's never just data."

"It's often personal information about real people, and people who have a right to be informed that businesses are collecting their data and they have a legal right to know how businesses are using it."

In Canada, privacy laws protect people from having data, even public data, used without notice and without their consent.

"Unlike the United States, here in Canada we have these comprehensive privacy laws that apply to publicly available personal information such as that which is found in geolocated social media posts," she said.

But Denham said consumers have a responsibility to protect their own privacy.

"Nobody likes to feel they're being watched. But many people fail to disable GPS, and they also need to change their settings when they get new devices," she said. "Consumers need to do some work. They need to make themselves aware of privacy controls in social media."

Maintaining privacy Swannie said he doesn't think governments or companies realize the extent of the information that employees reveal through social media.

Using the search engine's geofencing tool, Swannie checked out military bases throughout North America and overseas.

"The first thing people check into on any base is the ammo (depot). I can show you the exact point of every ammunition dump on military bases," he said.

Swannie mapped the nearby Esquimalt Canadian Forces

Base and found a wealth of photos and postings. The Vancouver Sun sent examples of the military posts to Daniel Le Bouthillier, head of media relations at the Ministry of National Defence, who said there were "no operational security concerns" with those posts.

Le Bouthillier said members of the Armed Forces are encouraged to communicate publicly about their own experiences and expertise, in accordance with the government's communications policy. Among the requirements of that policy is a provision that employees respect privacy rights and national security.

From military bases, EchoSec started exploring other sensitive locations.

"We started rolling into areas like Fort McMurray and finding equally interesting things," said Swannie. He said the search engine turned up a photo of a person "with big bags of weed," and 15 minutes later was posting pictures showing that person working with heavy machinery.

The information is mapped, so that you can single out anything from your house, to a company's corporate headquarters, to a high school, or riots in the streets of Kiev. The data can also be filtered by date.

Peter Chow-White, a communications professor at Simon Fraser University and associate director of the Centre for Policy and Research in Science and Technology, is a tech-savvy specialist in big data and social media, yet even he was surprised at how much information EchoSec's search engine revealed about people who likely don't realize they could be tracked in such a way.

"This kind of bends our privacy laws into directions they definitely were not intended," he said. "Our current privacy laws were drafted in a time of email, not in a time of geo-tagging social media and big database linkages."

Chow-White drew a geofence around SFU and found photos of children who were at the campus for Spring Break camps.

"On the one hand, these kids are just sharing their information. On the other hand, I don't really want people to know my kids are away at a camp," he said. "It's another example of maintaining privacy. You have to be enormously active and savvy to maintain your privacy in a digital age."

Chow-White said databases on their own may have limited uses, but when they are linked together they can reveal considerably more information. "Obviously, the risks run the gamut from the everyday risks to people's personal information and their own well-being and their own sense of moving around without being watched, but it also raises some larger critical national issues around security as risks for the military and other security agencies," he said.

A free, public version of the search engine is available on EchoSec's website, but that uses only a handful of the sources the company taps into when collecting information for law enforcement agencies or other clients.

Unknowing risks Kelly Sundberg, an associate professor at Mount Royal University's department of justice studies, who has done research on the use of social media in law enforcement, said Echo-Sec's geo-fencing makes it easy to see an entire spectrum of social media feeds, including confidential data about companies and other sites.

"If you geo-fence a sensitive area, you can see even (into) places that have a policy where people shouldn't be taking photos and posting them publicly," said Sundberg.

Sundberg said that with some of the available technology such as facial recognition, people could create search tools to mine data that could become even more revealing.

While many people turn off the geo-locating feature of their social media feeds, others turn it on deliberately, and many aren't even aware that it exists at all.

"I don't think a lot of people realize the default settings of their mobile phones or smartphones is to geo-tag," said Sundberg. "A lot of people don't realize they are being geotracked with their smartphones and mobile devices."

Merlyn Horton, executive director of the Safe Online Outreach Society (SOLOS), which teaches online safety to parents and children, said the EchoSec search engine highlights the risks young people unknowingly take when they publish geo-located posts on the Internet. "There are unintended consequences of the technology. You're taking militarygrade tools and you can apply them to surveying youth and minors, " she said.

The EchoSec search engine doesn't just mine social networking data. It can also tap into video camera feeds that are publicly available, as well as other open data.

"It's getting super creepy," said Horton. "We are living in this age where we are being observed all the time. The issue is people's lack of awareness."

With children getting smartphones at younger ages, they often lack the knowledge and experience to keep themselves safe online, according to Horton. "It's a loaded Uzi in the hands of a Grade 5 student," she said of smartphones filled with social networking apps. "They're always leaving a digital trail."

Horton said SOLOS presentations include advice about turning off geo-location, but even people who are careful are sometimes unaware they are broadcasting their whereabouts.

"When we talk about geolocation in our presentations, they'll turn it off. But often it gets turned back on when you reset your phone," she said.

Const. Mike Russell, a social media officer and spokesman with the Victoria Police Department, said that while the information EchoSec uncovers isn't new, its scope and the way the information can be delivered is. "The fact this information is being aggregated in one spot is new," he said.

Russell said individuals need to check privacy settings on their social media networks, and employees should be aware of their company or organization's social media policy. "If you have location services turned on in your Twitter account, you can pinpoint a house within about three houses," he said. "People need to be aware of that."

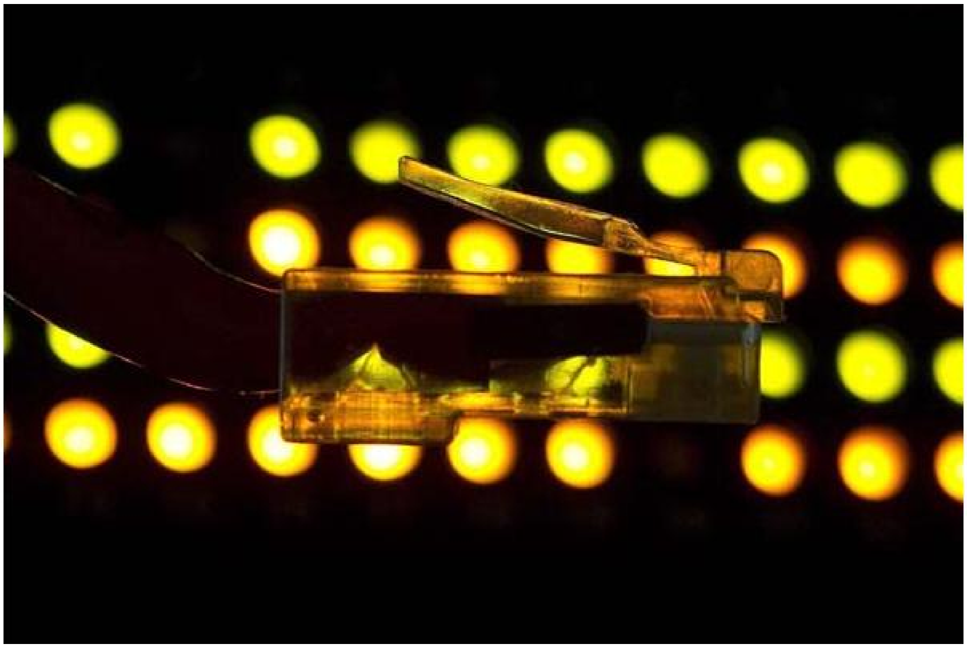
However, geo-located social media posts can also help police. In Victoria, a man boasted on Facebook after a 2013 drive-by shooting that police were after him, and police were alerted to the post. Dennis Fletcher was caught and sentenced to eight years in jail for attempted murder.

gshaw@vancouversun.com vancouversun.com/digitallife

EchoSec's search engine mines photos, text and other information posted by social media users and links it to maps. The cloud of icons above indicates everything from Twitter posts to Instagram photos.

Experts say most people are unaware that location services need to be manually disabled on their smartphones. iPhone settings are shown below.

Previous **Next**



Social media musings are never secret.

Photograph by: Adrian Wyld, CP