SMILE! YOU'RE ON CAMERA

The federal government isn't the only one watching you

By Matt Alderton

WHEN HE FIRST saw them, Seattle City Councilmember Nick Licata didn't know what they were. There were two of them — small, black and industrial. They looked like toy helicopters, or bionic birds. Something that belonged in a *Batman* movie, not hugging the skies around Puget Sound.

And yet, that's exactly what they were intended to do.

"We have nine councilmembers, and every morning we have a briefing session where we talk about upcoming legislation or listen to presentations by various departments," recalled Licata, currently serving his fourth term in the Seattle City Council. "One morning we showed up and there were these strange objects on the table for us to

CONTINUED »

THINKSTOCK

Tourists take photos through the White House fence in September. Legal activity such as photography can seem suspicious in some contexts, especially outside government buildings.

MARK WILSON/GETTY IMAGES

> "It is important to remember that just because someone's speech, actions, beliefs, appearance or way of life is different, it does not mean that he or she is suspicious."
>
> **— Los Angeles Police Department**

look at. We asked, 'What are they?' It turns out they were drones."

The Seattle Police Department (SPD) had acquired the drones in 2010 with the help of a federal homeland-security grant. It planned to use them to take aerial photographs of traffic crashes; to scout crime scenes for hostages, bombs and weapons; and to assist in search-and-rescue efforts.

It wasn't their planned uses that concerned Licata, however. It was the possibility of "scope creep" — that the drones would be used for reasons beyond their original mission. He then drafted a bill requiring all city departments to obtain City Council approval, conduct community outreach and develop strict operational protocols before acquiring surveillance equipment of any kind. Councilmembers unanimously approved the bill in March 2013 — a month after Mayor Mike McGinn ordered SPD to suspend its drone program entirely.

"If we're going to be using surveillance equipment, the public ought to know where it's going to be deployed and how it's going to be used," said Licata, whose legislation was a response not only to drones, but also surveillance cameras in Seattle's parks and ports. "As (historian) Lord Acton said, 'Power corrupts, and absolute power corrupts absolutely.' If we concentrate too much authority to collect information on people's personal lives, I fear we'll be corrupting our democracy."

Licata isn't alone. A July 2014 survey by the Pew Research Center found that 61 percent of Americans say it is "unacceptable" for the U.S. government to monitor American citizens. The feds aren't the only ones watching, however. Joining the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and other federal agencies in surveillance of private citizens are municipal government, local law enforcement, cellphone companies and even retailers.

Surveillance supporters are quick to point out the benefits, which range from increased public safety to improved customer service. Critics like Licata, however, ponder the cost.

SERVE, PROTECT AND SURVEIL

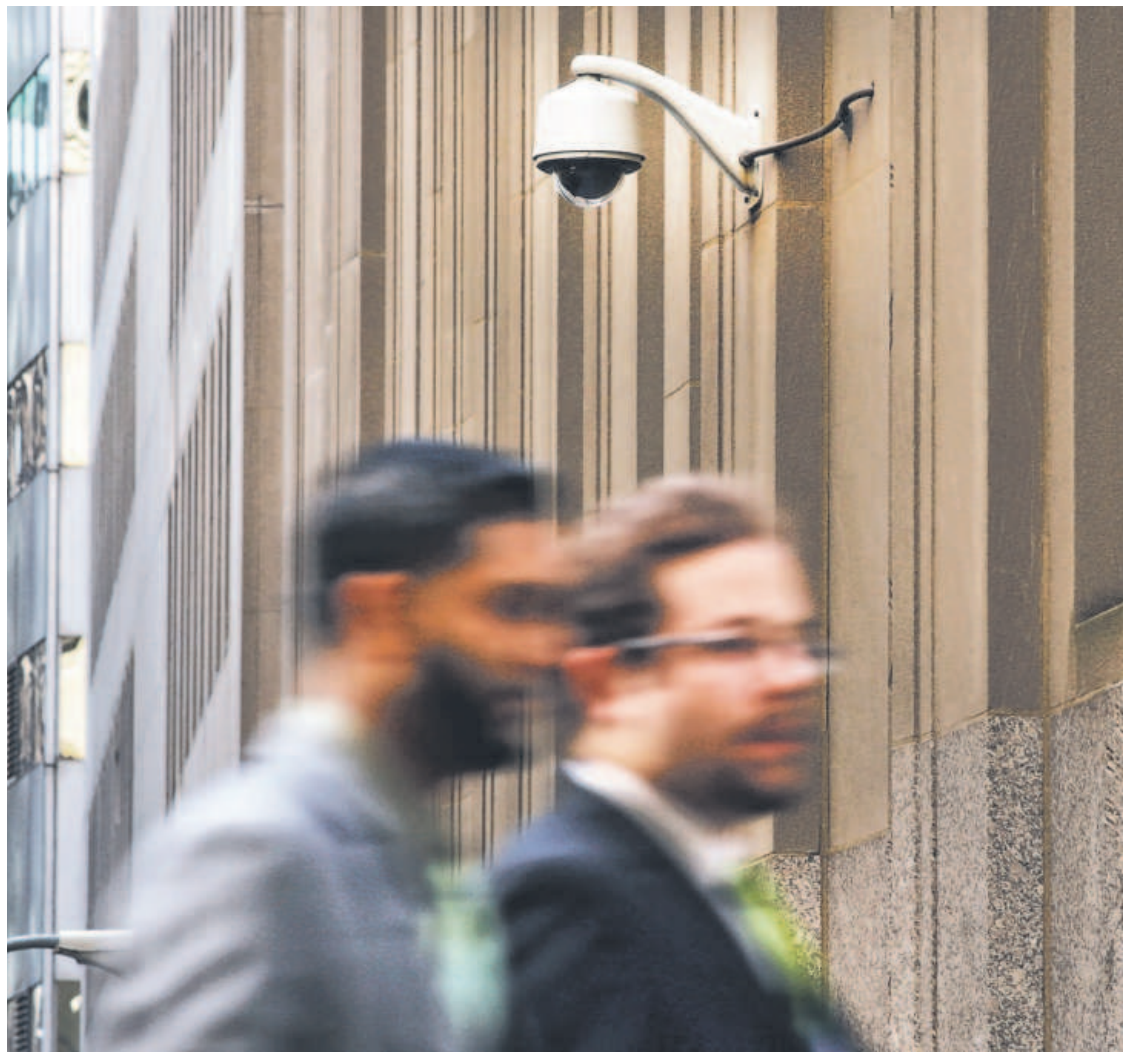
When SPD retired its drones, it donated them to the Los Angeles Police Department (LAPD), which has a long history of citizen surveillance, according to Hamid Khan, campaign coordinator at the Stop LAPD Spying Coalition, an alliance of community organizations and individuals who oppose surveillance by local police departments.

"While a lot of focus both currently and historically is placed on federal agencies, local law enforcement has always been on the front lines of operating covertly and illegally," said Khan, a first-generation immigrant from Pakistan. "In particular, post-9/11, the LAPD … became a poster child for rapidly expanding its surveillance, spy and infiltration programs."

Although LAPD has yet to fly its new drones, it already is keeping a close eye on Angelenos through numerous other programs, such as its counterterrorism "Suspicious Activity Reporting" initiative, which encourages police officers and others — including critical infrastructure operators, firefighters, emergency medical service providers and private security personnel — to report "suspicious" behavior, which is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity."

When program participants see such behavior — including illegal activities, like attempting to acquire illegal firearms or trespassing in secured buildings, as well as legal ones, like taking photographs in public or changing one's appearance — they report them to LAPD's Counter-Terrorism and

CONTINUED »



SPENCER PLATT/GETTY IMAGES

Surveillance cameras, such as this one in New York City's financial district, are becoming more common in public spaces despite privacy concerns.

Surveillance supporters are quick to point out the benefits, which range from increased public safety to improved customer service. Critics, however, ponder the cost.

Criminal Intelligence Bureau, which investigates the reports and submits them to a national network of "fusion centers" charged with collecting, analyzing and sharing data across local, state and federal law enforcement agencies, including the Department of Homeland Security (DHS) and the FBI.

"It requires officers to open up secret files called 'suspicious activity reports' merely on observation of a particular behavior," explained Khan, who said more than 14,000 local law enforcement agencies across the country have adopted similar programs, engaging more than 52,000 local security partners as trained informants. "The ACLU of Northern California has obtained about 1,800 actual suspicious activity reports that show, for example, a college professor whose hobby is taking photographs being stopped and detained and questioned, and next thing you know his name goes into the Joint Terrorism Task Force database. In essence, it criminalizes everyday behavior."

When officers aren't watching, neighbors are, courtesy of programs like iWATCH, a campaign leveraging citizens as tipsters. According to program guidelines, citizens should report obvious incidents such as backpacks left in public places, but also more ambiguous behaviors, like hobby-shop customers who lack enthusiasm about their hobby, or people who loiter in front of pet stores.

"It is important to remember that just because someone's speech, actions, beliefs, appearance or way of life is different, it does not mean that he or she is suspicious," LAPD emphasizes to citizens in its iWATCH guidelines.

Even so, 70 percent of iWATCH reports don't meet program guidelines, according to an analysis of 153 iWATCH reports by the Stop LAPD Spying Coalition.

Other LAPD surveillance tools include controversial StingRay phone trackers, which allow officers to listen in on private cellphone conversations, and TrapWire, software that analyzes footage from surveillance cameras to automatically detect and record citizens engaging in certain behaviors.

"Surveillance and spying by local law enforcement is real, it's 24/7 and it runs much deeper than most people imagine," Khan said.

According to Michael Downing, deputy chief and commanding officer of LAPD's Counter-Terrorism and Criminal Intelligence Bureau, LAPD's surveillance programs aren't unlawful; they're lifesaving.

"Modern-day criminals have proved themselves to be transnational in reach, linked by sophisticated networks and highly adaptive in their thinking. In response, local police agencies such as (LAPD) are developing strategies that are equally adaptive and networked," he wrote in a 2009 article for *The Police Chief,* a monthly magazine for law enforcement agencies.

According to Downing, active terror plots already exist in the Los Angeles area. "In the experience of the LAPD, the principal threats are local, self-generating and self-directed," he continued, citing as an example the 2007 conviction of alleged terrorist Hamid Hayat, a Lodi, Calif., man who sought terrorist training in Pakistan in 2003. "Police hold the key to mitigating and ultimately defeating terrorism in the United States."

CANDID CAMERAS

While surveillance often begins with law enforcement, it doesn't always end there. In Chicago, for instance, the city has commenced what's known as the "Array of Things" project, whereby more than 500 "nodes" equipped with data sensors eventually will be installed on light poles to record information about anything from pedestrian traffic and noise pollution to air quality and weather. Although the researchers behind the project insist no personal or identifying information will be collected, privacy advocates are skeptical.

"If somebody's putting up sensors in a neighborhood to study traffic congestion, you have to ask yourself: What else do those sensors capture?" said Lee Tien, senior staff attorney with the Electronic Frontier Foundation (EFF), a non-profit organization dedicated to maintaining civil liberties in a digital world. "The science has shown that it's much easier than we thought to re-identify people out of datasets that were formerly thought to be de-identified. So when people say no personal or identifying information will be collected, the attitude I take is: Are you sure about that?"

Cameras are inside as well as out, private as well as public. For instance, consider Solink Corp., a Canadian company that specializes in video analytics. Its software processes surveillance video collected by private businesses — including banks, restaurants and retail stores — and analyzes it for patterns. The results can alert companies to employee fraud, help them staff their business based on customer volume and optimize store layouts according to shoppers' traffic patterns.

"Video is the most content-rich source of data there is," said Christopher Beaudoin, Solink's director of marketing. "It's like having someone watching your store that never sleeps and never takes breaks."

Except they're not just watching the store. They're also watching you. And because businesses have a legal right to record their patrons, they typically do it

CONTINUED »

SPENCER PLATT/GETTY IMAGES

Video cameras captured these images of the two men linked to the Boston Marathon bombings in 2013, which led to the arrest of Dzhokhar Tsarnaev, right. His brother Tamerlan, left, was killed during a shootout with police.

without customers' knowledge and consent.

"Whether they're walking down the street or shopping in a store, people have no way of knowing whether a camera is recording their presence there," Tien said. "And even if they do realize their information is being collected, they usually don't understand who's collecting it and what can be done with it."

BIG DATA OR BIG BROTHER?

The most invasive surveillance tool in the world lives in your pocket or purse.

"The most effective tracking device that exists is your cellphone," said Julia Angwin, author of *Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance.* "And it's not just the cellphone companies that take information from your cellphone; it's every app maker, your operating system and, increasingly, anyone who receives your Wi-Fi signal."

Indeed, many businesses are now installing systems that detect nearby Wi-Fi signals and collect data from their source. Nordstrom, for instance, tested Wi-Fi tracking at 17 of its stores, but discontinued the technology in 2013 because of customer complaints. "Stores are setting up little 'sniffers' to see phones that go by. They want to know who the shopper is that's walking by their store several times a day so they can send them a coupon or an ad," Angwin continued.

"Some of this technology is really great," said Chris Babel, CEO of TRUSTe, a San Francisco-based developer of data-privacy solutions. "Not only do you get a criminal off the street, but you also get a 20-percent-off coupon for a pair of shoes you've been standing in front of looking at for the past week."

Along with sniffers, some stores are leveraging facial recognition software and GPS signals to determine shoppers' gender and location. If you're a man in the women's shoe department, they know it.

Data technically is anonymous, but could easily be combined with adjacent data sources to determine an individual's identity, according to Babel. The same store that tracks your Wi-Fi signal and records your face, for example, has a record of your in-store transaction. Because all three data points likely have a time stamp, it wouldn't take much detective work — by the store or a third party — to determine your identity.

> "Whether they're walking down the street or shopping in a store, people have no way of knowing whether a camera is recording their presence there."
>
> **— Lee Tien, senior staff attorney, Electronic Frontier Foundation**

"We're very quickly getting to the point where all these different information sources can be tied together — whether it be for marketing or law enforcement — so that your insurance company, for example, can price your insurance rate based on what aisle you're in at the grocery store," Babel said. "The question is, when is it good for consumers, and when does it violate a person's perception of their civil liberties?"

It's already toeing the line for Angwin, who spent a year of her life trying to live outside the reach of surveillance. During her 12-month experiment, she changed her Internet search engine from Google, which stores users' data, to DuckDuckGo, which doesn't; used disposable cellphones; and unfriended 600 Facebook friends. She even opened a credit card under an alias and used it to make restaurant reservations.

"I was able to avoid about 50 percent of surveillance, but every single day that number falls because surveillance techniques are getting more sophisticated," she said. "Surveillance is getting cheap enough that soon we'll be surveilling each other. It won't be long, for instance, before your neighbors have their own (drones and sniffers). They'll be able to see if you're home or not, which to a lot of people is much more creepy than being watched by the state."

PRIVACY, PLEASE

Surveillance isn't just about prying. One company — Persistent Surveillance Systems of Dayton, Ohio — works with local law enforcement to fly manned surveillance aircraft over cities for up to 200 hours a month. In Ciudad Juaréz, Mexico, aerial images collected in 2009 showed 34 murders as they occurred, including a cartel killing, analysis of which led police to the hitman, his getaway vehicle and several accomplices.

"We can solve crimes dealing with everything from home invasions and robberies to shootings, murders and rapes," said President and CEO Ross McNutt, who is actively pursuing long-term contracts with cities such as Chicago. "Chicago has 675 crimes per square mile per year; in a city like that, we'd witness 30 to 40 crimes per mission."

Images from surveillance video likewise led police to the Boston Marathon bombers in 2013.

Consumers may benefit, too. Data gathered by private companies and apps, for instance, yield more relevant advertisements and offers, personalized service and improved in-store experiences.

"We target quick-service restaurants, doughnut shops, banks — places you don't want to spend a lot of time," Beaudoin said of his company, Solink. "Our video analytics help businesses respond when they have long lines, so you can get in and out more quickly."

Still, risks remain. "Everything now goes on your permanent record in some way," Angwin said. "Everyone who says, 'I have nothing to hide,' is unaware of the fact that it can be illegal, for instance, to have a disorderly home or sagging pants. There are laws on the books that are unbelievably mundane, but when every piece of data about you is available, (law enforcement) can always find something on you."

The result — especially in groups like the Muslim community — often is self-censorship. "For me, it's really a free-speech issue," Angwin said. "As we as a society become more aware of the ubiquity of surveillance, people are beginning to chill their speech. For example, people always ask me if it's safe to Google something. What I have to tell them is: I wouldn't do it."

Like toothpaste, there's no putting surveillance technology back in the tube. Having open dialogue and transparent policies can ensure it's implemented responsibly, according to Licata, who said the Seattle model serves as a good way forward. Governments and companies implementing surveillance technologies should have clear specifics about their use and transparent policies for data collection, storage, access and retention.

"Surveillance can have a positive impact," he said. "Like any tool, it depends how you use it."