You are being watched

"We're seeing just an unbelievable intensification of monitoring capacity. There's an ability to connect all of this stuff across realms that is just a little unnerving," said Kevin Haggerty, a sociology professor at the University of Alberta.

Photograph by: Courtesy of Kevin Haggerty, University of Alberta

OTTAWA — David Lyon is studying the ceiling in an Ottawa coffee shop, searching for hidden cameras. A leading figure in the fast-growing field of surveillance studies, the Queen's University sociologist is only too aware of the many ways we're all being watched.

Closed-circuit TV cameras, like the ones likely concealed in the coffee shop ceiling, are among the most common. Since 9/11, their use has exploded worldwide. Britain now has an estimated 4.2 million CCTV cameras — one for every 14 citizens. People in central London are now caught on camera about 300 times a day.

One estimate puts the number of public and private CCTV cameras in the United States at 30 million. So far, similar estimates are lacking for Canada. But experts agree camera surveillance has been growing steadily here as well.

"I find it mind-boggling when I see what they do in Britain," Lyon says. "Police officers on bicycles now have video surveillance cameras in their helmets," he exclaims, then blurts, "What kind of a world are we living in?"

A very different world. Enabled by computer technology and algorithms, driven by a mania for security, safety and certainty, and engineered by a class of mathematicians and computer scientists that author Stephen Baker has dubbed "the Numerati," surveillance is emerging as the dominant way the modern world organizes itself.

"We're seeing just an unbelievable intensification of monitoring capacity," says the University of Alberta's Kevin Haggerty, a surveillance expert. "There's an ability to connect all of this stuff across realms that is just a little unnerving."

Surveillance is a condition of modernity, integral to the development of the nation-state and to global capitalism, writes University of Victoria political scientist Colin Bennett in his new book, The Privacy Advocates: Resisting the Spread of Surveillance. "It is that important."

More than ever before, our lives are visible to others, from government agencies and security services to the owners of the websites we surf

and the stores where we shop. They track us in public, in workplaces and online, compiling our personal information in massive databases and sorting us into categories of risk, value and trustworthiness.

Their accomplices are companies that mine our personal data using sophisticated technologies to extract and refine what they gather to slot us into ever-finer slices and segments.

CCTV cameras are just one of their tools. Others include radio frequency identification (RFID) chips, GPS location trackers, website cookies, facial recognition software and store loyalty cards. Computer programs used by security services can monitor and analyse billions of phone calls and e-mails in real time. We even make it easier for our trackers by willingly disclosing pieces of our lives on social networking sites like Facebook or in online contests and questionnaires.

"We are inadvertently handing over to centralized authorities an infrastructure of visibility the likes of which no society has ever seen before," Haggerty says.

"We're talking about something that is frequently invisible," says Lyon, director of the New Transparency Project, a $2.5-million research program involving leading surveillance scholars, including Haggerty. But it can do harm to real people, he says.

In one form or another, surveillance has always been part of human society. What's new is computer technology that has made it possible to integrate vast and diverse bits of information.

As well, our post-9/11 obsession with eliminating risk has produced an architecture of mass surveillance in which everyone is treated as a suspect. "We've inverted the relationship between the citizen and the state," says University of Ottawa criminologist Valerie Steeves. Our governments should be transparent to us, so citizens can hold them to account, she says. Instead, it's citizens who are being made transparent, because we're all viewed as potential risks. "We got it backwards."

The fact that we are increasingly identified as we go about our daily business means anonymity is under threat, Steeves observes. "And anonymity is essential if I'm going to be able to exercise free speech and freedom of assembly."

Moreover, the ubiquity of surveillance is creating societies of suspicion. "The presence of surveillance feeds the whole notion of the risk society and engenders more mistrust between members of society," says Jane Bailey, a law professor at the University of Ottawa.

Yet most surveillance today isn't done for sinister reasons. It's usually well intended, designed to improve security or organizational efficiency. But those good intentions often have unintended consequences.

Surveillance is no longer primarily a function of the state. Businesses collect as much information about individuals as governments — or more. Google and Yahoo routinely track online behaviour and use what they learn for targeted advertising. Retailers collect personal information and track consumer purchases though loyalty cards that offer points and other rewards. Data brokers sort and sell our personal information to the highest bidder. And there are plenty of bidders.

"In the 1980s, I would have said that government was the biggest threat to privacy," says Bennett. "Now, I don't think you can tell the difference between the two. You can't really tell where one database ends and another one begins these days."

In Canada, governments have long tapped into consumer credit industry data. "Anything that the private sector is collecting can, in theory at least, be accessed by government," says Teresa Scassa, Canada Research Chair in information law at the University of Ottawa. "It's all out there."

In the United States, the Department of Homeland Security openly uses information from the direct marketing and consumer credit industries to augment its profiles of individuals. The Patriot Act allows government agencies to access phone records.

The surveillance society is even further advanced in Britain and Europe. The European Union has endorsed proposals empowering police to conduct remote searches of personal computers. UK police no longer need judicial authority to access telecom records. In 2007, they used those new powers 500,000 times.

Britain is proposing a monster database containing information on every phone call, e-mail and Internet visit made in the U.K. The EU plans something similar, along with mandatory fingerprinting of all passport holders. Until it was scaled back last September, France was compiling a database on millions of citizens — politicians, religious figures, business and union leaders, and anyone "likely to breach public order" — that even included information on their sexual preferences.

According to Statewatch, a non-profit watchdog group, the EU "is set to become the most surveilled place in the world." That is leading it "further down the road to authoritarianism, a path which looks less and less likely to be reversible."

Surveillance isn't yet as widespread in Canada, thanks in part to more robust privacy laws. But Canada is lagging other nations in ensuring the security of personal information, says federal Privacy Commissioner Jennifer Stoddart. "No matter how well-meaning you are, if your technology is not secure, the confidentiality of the personal information will be lost."

As well, Canadian government agencies can access private sector information to track people for national security purposes. "It's kind of a seamless world in which traditional civil liberties have been suspended to some extent," Stoddart says.

"Privacy advocates are in despair," says Ron Deibert, director of The Citizen Lab at the University of Toronto's Munk Centre. "Things have gone so far beyond the kind of worst-case scenarios they imagined that they just kind of throw their arms up. It really is hard to find meaningful protections for privacy these days in any sector of life."

Yet so far, there's been little public outcry about the explosive growth in private and public monitoring. In part, that's because many of us are simply unaware of the extent of contemporary surveillance.

"For most of us," Haggerty says, "the surveillance is a mile wide and an inch deep. Nobody's paying attention to it. But if you suddenly become a person of interest, there's just an unbelievable infrastructure of information that could be suddenly and almost immediately drawn upon."

Even if we understand we're being watched, many of us are willing to trade some privacy for perceived benefits. We use our personal information as a kind of bargaining chip, swapping it for better social connection, discounts on merchandise and free flights.

There's also a widespread belief that visible surveillance, such as CCTV cameras, makes us safer. But that's simply wrong, Lyon argues. Mick Neville, who heads the police video unit in London, recently described Britain's costly investment in CCTV cameras as an "utter fiasco," saying they've only helped police solve three per cent of street crimes.

So far, most of the push-back has come from federal and provincial privacy commissioners and advocacy groups such as the University of Ottawa's Canadian Internet Public Policy Clinic (CIPPIC).

In the past year, CIPPIC has filed complaints about alleged violations of privacy law by Facebook with Stoddart and asked her to investigate possible online tracking by Internet service providers.

In some ways, corporate surveillance worries Philippa Lawson, who was CIPPIC's director until this year, even more than government snooping. The image of Big Brother makes it easier to shine a light on government if it strays from its public interest mandate, she says. "The private sector, on the other hand, has only recently come under the spotlight, and the spotlight has been very, very weak."

When Google tried to introduce its new Street View application, which displays street-level images of houses, cars and people, Stoddart challenged the company's presumption that anything Canadians do in public is fair game for video surveillance.

That's not Canadian law, she told Google officials. "You don't expect to be on the Internet, beamed around the world, as you go around to the convenience store to buy some milk."

After consultations with her office, Google has agreed to blur the faces of people and car licence numbers — even houses, if their occupants object — on Street View.

Stoddart has also commissioned research into the extent of CCTV use in Canada and whether the 2010 Winter Olympics will lead to new and enduring surveillance efforts here.

That's quite likely, according to Haggerty. CCTV cameras installed for the 2004 Athens Olympics have remained in place. London is planning 50,000 additional cameras for the 2012 summer Games. One legacy of the Vancouver Olympics will likely be CCTV cameras in the city's troubled Downtown Eastside, an idea that's been debated for years. "Now, I think it's inevitable," says Haggerty. "The Olympics tipped the balance."

Like others privacy advocates, Stoddart worries about the surveillance potential of radio frequency identification technology. RFIDs are tiny chips that store data — usually a unique identifier — that's communicated to a reader by radio transmission.

Already widely used in workplaces and for inventory control, RFIDs may someday be embedded in almost everything, allowing each of us, at least in theory, to be monitored wherever we go.

Within a decade, RFID chips could replace universal product codes, meaning every item on Earth would have its own unique identifier. We might find ourselves "covered with tags shouting out information about the clothing you're wearing, or what's in your purse or wallet," says Scassa.

Workers already carry RFIDs in the access cards they use to enter and exit their workplaces. Some employers deploy readers throughout the building, Scassa says. "So the employer knows when you go to the bathroom, how long you're in there, how long your cigarette break was. That happens all the time."

Within a human lifetime, RFIDs will likely be routinely embedded in everyone alive, Haggerty predicts. The process will start in developing world countries, then spread to stigmatized groups in the West, such as pedophiles and those on social assistance. Employers will start making implants a condition of employment. Chipped individuals will get discounts and other privileges. Eventually, having a chip will be essential for everything from voting and driving to shopping and medical care.

An implant society need not be a nightmare, Haggerty maintains. Making people and processes more visible makes them easier to regulate, he says. And that can be a good thing. The flip side, though, is that you might wake up one day and find you're on the wrong side of some new definition of normal.

Technologies are morally neutral, but their potential uses are not. During the Second World War, the Nazis used IBM punch cards to identify Jews. "If the government project is coercive, if it's totalitarian," says Haggerty, "it makes for a more perfect coercive, totalitarian governance. You can get more than the trains running on time."

For ages, he says, we've tried to track and monitor people by putting numbers on things like shirts and bracelets. But those can be removed. "What this does," Haggerty says of RFID implants, "is it ultimately reproduces the Nazi tattoo on the body."

http://www.canada.com/technology/being+watched/1709205/story.html