

Montreal Gazette

Tracking digital shadows

Sat Sep 18 2010
Page: B1/Break
Section: Saturday Extra
Byline: JASON MAGDER
Source: The Gazette

Illustrations: Colour Photo: Loyalty card programs collect data about clients' purchasing behaviour. Scanning passport bar codes yields a lot of information about a traveller -all part of the digital universe. Your car's black box records speed, braking information and other details. If you've registered your Opus card, its RFID chip contains your personal information. Smart phones are easier to hack into than computers, and are targeted by corporate spies. Digital images like airport body scans -whether or not they're intentionally stored -become part of your digital shadow.; Photo: BLOOMBERG /The Electronic Privacy Information Centre in the U.S. says airport body scanners have the ability to store, record and transmit images, contrary to what security officials have said.;

7 a.m.: You wake up and look outside your window. It's raining, so you decide to check the weather on television. Without realizing it, you've already shared information about yourself, possibly to hundreds of people, and your day has just begun.

In your daily life, there are dozens of ways you transmit personal information -without ever logging on to a computer -from using your credit card, to walking down a city street. Taken together, that information is called a person's digital shadow.

With all the technology advances of the last 20 years, the length of an average person's digital shadow has grown tremendously, and will grow even more in the coming years. The more information out there, the more chances there are that it can be used by others, sometimes against you, either as a way to profile you for a marketing campaign, or for more nefarious uses like stealing your identity, appropriating sensitive corporate data, or stalking your every move.

"It's the sort of trail that you may not be aware of, because you don't have physical contact with the machine that may be collecting the information," said Colin Mc-Kay, the director of research, education and outreach with the office of the Privacy Commissioner of Canada.

"There are a large number of data points that you leave in your daily life that don't necessarily identify you, but certainly identify your behaviours, your preferences and the choices you make."

All the world's digital shadows make up most of the digital universe -all information created and replicated by the world's digital devices. The technology consulting firm IDC conducts an annual study to measure the size of that universe. By the end of 2010, it will be about 1.2 million petabytes, where one petabyte is one million gigabytes, and will be 44 times as large by 2020. IDC estimates that 70 per cent of the digital universe is generated by people going about their daily lives.

It also found that sensitive personal data is the highest-growing portion of the digital universe. It currently makes up about 30 per cent of all data, and will grow to 50 per cent in 10 years.

Despite all the information that we transmit, often unwittingly, on a daily basis, it's still extremely difficult to connect the dots and find out everything about a certain person. However, McKay said, that

possibility is not far off.

"It's startling now how much information people can collect about you if they know how to use the right online databases and search engines," McKay said. "People can draw relatively accurate maps of where you hang out, what purchases you make, and your normal route. If you're a particular specialist, and you can hack into specific databases, you can draw a fairly accurate map, overlying multiple different sources of data."

The hacker might not specifically identify a person, but would come close enough to give them that "icky feeling" that someone is watching, McKay said.

"I think Canadians are only beginning to realize the amount of information that can be collected about them, and they need to become aware of the controls that are available to them."

McKay said the commissioner's office expects digital privacy issues to become a huge preoccupation in the coming years, and is investing in IT analysts to help keep track of the changes in the ever-growing digital universe.

So if you're watching a digital television, you are contributing to the digital universe, because the television box will log the hours you watch and the programs you choose, and possibly the commercials you skip over, and then pass that information on to your cable company, which in turn could share that data with its partners.

8 a.m.: Having noted that the weather forecast calls for rain, you opt to drive rather than take the bus. You walk out of the house toward your car. Your digital shadow grows as the electronic signature of your keys is used to unlock the doors, but that's only the tip of the iceberg in the amount of digital data your car will be transmitting about you as you drive to work. Every car has an event-data recorder, or black box, which records information about the car, such as the speed, braking information, and other details. Even more information can be collected from systems like OnStar, which provide services like unlocking a car that has the keys locked inside, or dispatching a tow truck in the event of an accident. For the purposes of serving you, your OnStar operator has your exact location, which is provided through a GPS chip.

"Every action you take with your car is now being

recorded in some fashion, whether it's being shared outside the car, or simply held within the car," McKay said.

He added insurance companies in Europe and the U.S. are currently toying with the idea of using that information to calculate the risk levels of their customers.

"An insurance company can integrate that information to calculate insurance premiums, because they can get a gauge of your driving behaviour, and then they can integrate that with their actuarial calculations," McKay said.

Some new luxury cars are now gathering information about others on the road as sensors detect an obstacle in front of the car and automatically apply a car's brakes to avoid a collision.

8:30 a.m.: You're running late for work, so you're driving a little faster than normal. Your excessive speed triggers a photo radar system: another addition to your digital shadow. The image of your licence plate is sent to police computers, cross-checked against ownership information, and then a speeding ticket is mailed to your house.

9 a.m.: You arrive at a parking lot and swipe your monthly pass. Information

about your account is transmitted to the lot's computer system, which logs the times and dates of each entry and exit.

9:05 a.m.: You walk to the building from the parking lot. Your image is captured on a video surveillance camera. Although the image is likely not stored and a camera can't identify the names of the people being monitored, this is also part of your digital shadow.

Alex Manfrediz, a consulting director for IDC, says some law enforcement agencies in the U.S. are working on a way to scan people in a crowd to see whether they match the images of known terrorists stored in their databases. Although the technology is commonly used on television shows like *e24*, where Jack Bauer can spot a person on a department store security tape and cross-reference the image against a database of terrorists, this is still a long way from becoming mainstream.

"It is advancing, and I'd say it's prohibitively expensive at this point, so it's not deployed en masse, but are we headed that way? Yeah. I can see that happening," Manfrediz said.

9:10 a.m. You get to work and

swipe your key card to get into the building. The card contains a radio-frequency ID chip, which transmits to a security agent's computer the name of the employee, as well as some personal information, and sometimes his or her picture. As in the parking lot, building security also keeps track of people entering or exiting the building.

The RFID tag emits a digital signature, designed to

be read by a card reader. RFID tags are becoming more prevalent in everyday life. Their principal use is for product inventory, and department stores insert them into items of clothing to keep track of the merchandise. However, the use of RFIDs in government-issued identification cards is also growing.

The new enhanced Quebec driver's licence, which can be used as an alternative to a passport at a land border crossing, has an RFID tag that complies with new U.S. security regulations. Several provinces have adapted similar licences, but the provinces of Alberta, Saskatchewan and New Brunswick decided not to adopt the new IDs, citing cost and privacy concerns. Future passports could also have RFIDs that will store such biometric information as a person's fingerprints.

The privacy commission's McKay said there are some concerns about the growing use of RFIDs, mostly with reference to identification documents.

The tags now in use can be tracked from as far away as about eight metres, but the distance can be boosted using sophisticated equipment. Scanning an RFID tag could give access to a person's identification, and could allow that person to be tracked.

Noon: You get a call from your

spouse on your cellphone to tell you to pick up some milk on your way home. This leads to another spike in your digital data.

Cellphones work by communicating their distinct ID numbers through radio waves with the nearest cell tower. The call travels across the cellular network to the location of the phone at the other end of the conversation. While the data and the voice call are both encrypted, it is possible to intercept that signal. In fact, cellphone spying is a growing problem, especially in the world of business espionage, explains Nigel Stanley, a security expert at London, England-based Bloor Research.

Stanley said there are three common ways to intercept phone calls: One way is to set up a phoney cellphone station. That, Stanley said, can be accomplished with a laptop and some radio equipment, no larger than a small suitcase, from a distance of about 20 metres.

The second way is to intercept calls over the air and to decrypt them.

"We thought encryption was fairly safe, but there are flaws within the encryption models that have

been exploited, and those with the right technology can actually 'unencrypt' the traffic across the air," Stanley said.

The third way to intercept conversations is to install software on a phone, either by taking the phone for a few minutes, or by tricking the phone user to download the software, known as malware, which

can be designed as a computer game. The malware then monitors every bit of information on that cellular phone, including text messages and voice calls, and transmits it back to the originator.

Stanley said with the spread of smartphones, like eBlackberrys and iPhones, malware can access sensitive data like ebanking information, from those who do banking on their phones, and important emails. Most smart phones also contain GPS chips, so hacking into a person's phone can give the exact location of the phone.

He explained that it's relatively easy to hack into cellular phones using software, since their antivirus security systems aren't as advanced as those on personal computers.

"These attacks are all being used today," Stanley said. "There are examples of business people travelling to trade shows where they negotiate multi-billion dollar deals, and their phone calls are intercepted."

He said the technology is increasingly being used for corporate espionage, but also by governments investigating potential threats. And it's being used by stalkers and jealous spouses.

Stanley says you should never allow a stranger to hold your phone, and you should make sure you have a password blocking anyone from accessing the phone. There are also several companies that can provide an extra layer of voice encryption that would guard against interception.

"One of the most common signs that your phone has been compromised is that the battery life is significantly reduced, because it's transmitting more data than usual," he said. "You could also notice that lights or arrows are flashing, that indicate the phone is transmitting data, when it shouldn't be."

12:30 p.m.: You're hungry for

lunch, so you buy a sandwich at a local *depanneur*, remembering to pick up milk at the same time. You swipe your credit card, which collects points for a loyalty program. Lots of data is transmitted, as your credit card communicates its account number to the computer cash register, and the register communicates with the card company. Basic details are revealed, including your name, which may be printed on the bill.

The head office of the credit card company takes note of the user's location, to guard against credit card fraud, then checks the user's credit limit to ensure the purchase is not over that limit. The store where you buy your food may retain the credit card account information, usually for customer service reasons like a return or exchange. But there is a strict security protocol for all companies that store this information. If a database holding credit-card account information is hacked, it could be used to create a cloned card. A spokesperson for Visa would not say how often databases are hacked, but whenever they are, he said, credit companies must be informed. It is then up to the companies whether to

notify cardholders.

Rob Burbach, senior analyst for IDC Financial Insights, said stealing a credit-card number is extremely difficult, and if it happens, very little of the cardholder's personal information can be accessed.

The more valuable information is collected by loyalty cards, like eAir Miles, PC Points or Aeroplan, which collect data about the purchasing behaviour of their users for use in targeted marketing campaigns.

"Part of the deal is, they give you points, and you give them information," Burbach said. "They have been much more active about going out and marketing that information."

Mitchell Merowitz, vice-president of corporate affairs and chief privacy officer for Loyalty One, which manages the Air Miles reward program, said the information is valuable to member companies.

"The partner may say, 'We would like to communicate with 100,000 customers in Montreal, and we want to target people who shop at a grocery store once a week, and fill up on gasoline once every 10 days,'" Merowitz said. "We will take that request and we will analyze shopping behaviour data at an aggregate level and identify those 100,000 people. That contact list will be provided to the grocer, but the partner doesn't get to keep that list and put it in their database. They can only use it for that one time."

The Air Miles and Aeroplan programs don't take note of every item purchased, just the amount spent per visit. While those two companies limit the use of personal information, other loyalty programs don't have such strict policies. They sell anonymous profiles of their members to marketing companies, and that information can also be combined with other information then sold to another party.

"We get into the stage where you get meta data, which is data about data of that original transaction. It can get copied into another server, so that one activity of swiping a card creates a multiplier effect that then generates more information, beyond that original information," said Alex Manfrediz of IDC.

The privacy commissioner's Mc-Kay said law enforcement officials also buy some of this data.

"They use it to analyze specific behaviours of demographic groups, and apply that to their theories of human behaviour, and predilection for crime," McKay said. "So

this marketing data is interesting enough that it's worth paying for it so it can be overlaid on the data they already have."

5 p.m.: It's quitting time, so you

get back into your car and head home. You're low on gas, so you head to a gas station and swipe your

bank debit card into the reader at the pump. Your digital data is transmitted over a phone line in the pump's terminal to your bank, which then asks you a series of questions through the terminal, like your PIN code, and how much you would like to spend.

Gas stations are prime targets for card cloners who can alter the terminal to capture the data on a debit card's magnetic stripe. They can then use a pinhole camera, or even just spy on unsuspecting customers from a distance, to capture PIN numbers, and with that information, they create a cloned debit card. Debit card fraud, although growing, is fairly rare, occurring in less than one per cent of purchases. Last year, 238,000 cards in Canada were cloned, up from 40,000 in 2004, according to statistics from the Interac association. Newer debit cards have microchips inside them, which, unlike the magnetic stripe, are extremely difficult to copy. Chips will become the standard in debit cards by 2012.

7 p.m.: You've been home for an

hour, and now it's time to go to the airport, because you're heading on vacation to Florida. You decide to take the 747 bus to the airport. You press your Opus card against the reader, and it reads how much money is left on your pass. The STM computer system logs the usage of every one of its Opus cards, from how much money is loaded onto them, to where each one is being used. The information is valuable for the transit company to plan its routes. The Opus card has an RFID chip inside, and because you have registered the card, it also has your personal information on it. That information is kept in the STM's computer system. It's used for identification purposes, but kept separately from information about users' trips so they can't be tracked.

8 p.m.: You've checked in for your

flight. You go through customs, showing your passport. The customs agent scans the bar code on his computer. On his screen, he sees your name and citizenship status, to confirm that it's the same information printed in the passport. His computer terminal will also show a record of every time you have crossed the border. Since the system is relatively new, only the last few years of crossings have been collected. The agent will also see whether you have tried to smuggle items in the past, or whether you are a criminal with a warrant out for arrest.

8:15 p.m.: After customs, you

head to the baggage scanning area. Your luggage is scanned by an X-ray machine and its contents are displayed on a television screen. You step into the new body scanners, which were installed in February after an attempted terrorist attack. The scanners allow agents to see underneath the clothing of travellers to make sure they're not concealing anything sinister.

The Electronic Privacy Information Centre in the

U.S. has been fighting the use of body scanners saying they violate constitutional rights protecting against unreasonable search and seizure. The group also found the scanners have the ability to store, record and transmit the images, contrary to what security officials have said.

"We have sued in the U.S. to get this program shut down," said EPIC executive director Marc Rotenberg. "We believe it violates several laws, and it violates the U.S. Constitution. This program is illegal, invasive and ineffective. I think people are angry about it. They say they don't like it and they want it to stop."

Midnight: There's a storm outside

and your plane is delayed. It looks like you'll be sleeping at the airport. Your contribution to the digital universe for the day has ended, but as you sleep into the next day, your digital shadow continues to grow as security cameras scan the hallways of the airport ...

To calculate your daily digital shadow, visit:
www.emc.com/leadership/programs/digital-universe.htm

jmagder@montrealgazette.com