Print Story | Email Story | Subscribe Now!

Canada

November 21, 2005

You are exposed

When even the privacy commissioner's cellphone records are available online, we've all got security problems.

JONATHON GATEHOUSE

See also:
A little privacy please
In the wake of the *Maclean's* privacy report, there's a scramble to plug the breaches

Jennifer Stoddart is a dedicated public servant who has spent years -- first working for the province of Quebec, and since 2003 as the federal privacy commissioner -- trying to protect Canadians' personal information from prying governments and greedy businesses. A lawyer by trade, she has impeccable qualifications for the job, with a strong background in constitutional law and human rights.

But there's a point to be made about the type of highly confidential data that can be obtained by anyone with an Internet connection and a credit card, and Stoddart has the misfortune of being the perfect illustration. Not that she's pleased about it. Her eyes widen as she recognizes what has just been dropped on the conference table in her downtown Ottawa office -- detailed lists of the phone calls made from her Montreal home, Eastern Townships' chalet, and to and from her government-issued BlackBerry cellphone. Her mouth hangs open, and she appears near tears. "Oh my God," she says finally. "I didn't realize this was possible. This is really alarming."

Continue Article

When police are investigating a crime and want phone records, they must seek a court order. Recent commissions of inquiry, like Justice John Gomery's probe of Adscam or the investigation into the computer leasing fiasco at Toronto city hall, had to issue subpoenas to compel telecom companies to share such data. Government efforts to expand their phone monitoring powers as part of the war on terror are being fought tooth and nail by privacy and civil liberties organizations. Most Canadians consider their call records privileged information, and the courts have backed them up time and time again.

Yet *Maclean's* was able to purchase the privacy commissioner's phone logs online from a U.S. data broker, no questions asked. For about US$200 per order, Locatecell.com delivered months of long-distance records from her Bell Canada home and cottage accounts. They were also able to access her Telus Mobility cellphone call logs for October -- a monthly bill she probably hadn't even received at the time. And all the Internet requests were turned around in a matter of hours. (In a test run, the company was also able to obtain the cell records of a senior *Maclean's* editor from Fido, a division of Rogers, the company that owns this magazine.) Reverse phone number lookup engines on federal government and phone company websites provided the identities of many of the people Stoddart called, or who called her. On Sept. 15, for example, there was a call from her Montreal home to a relative in Frelighsburgh, Que. On Oct.

15, she called the house of one of her communications advisers from her cellphone. And on Oct. 27, she twice called the desk of another. While many of the numbers on the bills were cellphones or unlisted, anyone looking to fill in the blanks would only have to call until they hit voicemail recordings.

Confidential phone records are just the latest breach in the levee of government laws and corporate policies intended to protect private and personal data. Abuses -- whether it is medical records being scattered about a Toronto street as "garbage" for a film shoot, or Edmonton police running the names of pesky reporters and lawyers -- are reported almost every week. And in the wired world, almost anything is available for a price. A British teen recently tracked down his sperm-donor father using his own DNA and two different for-hire databases.

Many of the same websites that offer call records advertise even more invasive services like "personality profiles," complete with sexual preferences, names of exes, and gossip from neighbours. Or email and instant messenger traces that will provide the name of the person who owns the account, and their location, sometimes down to the street they live on. While some of the sites demand a signed release from the person being sought for items like credit reports and driver's records, the "verification" process wouldn't be much of an impediment for anyone willing to commit some garden-variety forgery.

Stoddart, whose office website offers tips to foil those trying to access or steal personal information -- including the prompt removal of incoming mail from your mailbox and shredding those pre-approved credit card applications -- was not a particularly easy catch. Despite her years in the public eye, and the numerous interviews she has given to journalists, there was little on the record beyond her professional qualifications. No one *Maclean's* contacted had her cellphone number, knew her home address, or even basic family information like the name of her spouse. "I've always been fairly mistrustful of people," she says. "If people want my personal data, I want to know why." Nonetheless, a thorough Internet search with Google yielded enough bits and pieces of information to start the process rolling.

Although Locatecell and other data brokers that *Maclean's* contacted claim to be able to find someone's cell number with simply a name and address, they failed in the privacy commissioner's case. (Locatecell did, however, provide the cellphones of four other Jennifer Stoddarts across the country.) But they were able to quickly provide long distance records from her home, when furnished with the name, address and Stoddart's date of birth -- obtained from publicly available property deed and mortgage papers in Montreal. Those phone records showed numerous calls to the townships chalet, listed under her husband's name. By obtaining call records for that number and cross-referencing, *Maclean's* was able to identify Stoddart's Ottawa cellphone. Armed with the actual number, Locatecell obtained her Telus Mobility records in a matter of hours.

As that proves, even the most cautious people are vulnerable if someone cares to expend the effort and money. What might be even scarier, as information flows faster and faster, is that no one -- governments, industry, federal and provincial privacy commissioners -- really seems to know how to hold back the tide.

Online data brokers have been selling Canadian and U.S. phone records for at least three years, and haven't been shy about advertising the fact. By the count of one American privacy group, there are more than 40 websites like Locatecell vying for your snooping business. But that's not something that anyone in the highly competitive telecom industry has been warning their customers about. Or apparently doing much to stop.

Mark Langton, a Telus Mobility spokesman, says the company was aware that these data brokers existed, but had no idea about his company's own

vulnerability. A "full-court press" investigation into the security breach is underway, says Langton, and new countermeasures will soon be put in place, though he declined to specify what. The company also refused comment on whether it plans to add extra security measures for its sensitive government clients. Rogers Wireless spokesmen say they learned of the problem from a U.S. newspaper article this past summer, but also decline to reveal what specific steps, if any, the company is taking to deal with the issue. "Criminal elements will continually refine their methodology to get around systems," says Dawn Hunt, Rogers' vice-president of government and inter-carrier relations. "We're trying to keep ahead of them." A Bell Canada executive says the company was unaware that such a security threat existed until *Maclean's* brought it to its attention, but now intends to quickly tighten its procedures. "As we get more details, we'll be all over this," says David Elder, Bell's vice-president of regulatory law. "We will be investigating this and we will not hesitate to prosecute, where applicable."

A complicating factor is that no one seems to be sure exactly how the data brokers are getting their information. One theory is that they have an inside connection. Another is that they are hacking online customer accounts. The most likely explanation is that they simply call up and ask for it. Phone companies, it seems, are rather easily duped. If a caller posing as a customer furnishes them with the right name, number and address -- sometimes they will also ask for a postal code or date of birth -- they will take that person at their word. (The misrepresentation and trickery apparently works with some cellphone owners as well. Stoddart reports that someone, presumably an agent for one of the data brokers, recently called her Montreal home claiming to be a phone company representative, and demanded her cellphone number. Her son refused to provide it, despite threats that his mother's service would be cut off.) Locatecell did not respond to *Maclean's* requests for an interview.

Just what Canadian authorities can do about the problem is unclear. The databrokers are ensconced south of the border, outside of their legal jurisdiction. And they are often hard to pin down -- Locatecell, which is owned by a Tennessee company, Data Find Solutions Inc., operates out of Florida, with a North Carolina phone number. As Stoddart lamented in her own annual report to Parliament earlier this fall, "privacy threats seem to be multiplying like a bad virus, threatening to overwhelm us." The increasing transborder flow of information from government and business is one of the biggest challenges, she added, because it takes data out from under the umbrella of Canadian law into "a legal vacuum." And while the phone companies' disclosure of these records violates the privacy law that covers corporations -- the Personal Information Protection and Electronic Documents Act (PIPEDA) says that such information cannot be disclosed without the express consent of the consumer, or a court order -- that is not a guarantee that any substantive action will be taken against them. Unlike many of her provincial counterparts, the federal privacy commissioner functions like an ombudsman, seeking to settle disputes rather than punish offenders. Her rulings are not legally binding (although she can seek to have them made so in Federal Court), and in most cases don't even identify the transgressors by name.

Michael Geist, a University of Ottawa law professor who specializes in privacy issues, says Canadian corporations have been treated with kid gloves since PIPEDA came into force in 2000. "There's a great reluctance to name names, or launch audits or take anything to the Federal Court," he says. Part of the problem is the government's reluctance to strengthen the laws or see the boat rocked, he says. Another factor is the privacy commissioner's relatively meager $11-million-a-year budget -- a legacy of the expense account scandal that enveloped Stoddart's predecessor, George Radwanski. "People in that office are very committed to the job, but it's clear they feel they are swimming against the tide," says Geist.

The Canadian Radio-television and Telecommunications Commission, which regulates telecom companies, has a little more power to punish privacy

breaches -- its rulings have the force of law. But the maximum fine for a corporation's first offence is $50,000 -- not much of a deterrent when you consider the multi-million-dollar penalties handed down by its American counterpart, the Federal Communications Commission. (Bell recently filed a brief with an Industry Canada telecom review panel arguing that the CRTC should get out of that aspect of the business altogether and leave such matters to the privacy commissioner.) On very rare occasions, Canadian police will get involved in a privacy issue, but only if the breach results in a serious crime -- like the 2002 case of the Quebec government employee accused of helping the Bandidos motorcycle gang plan hits by providing them with the driver's licences of rival Hells Angels.

Rooting out the problem in the United States, which doesn't have national privacy laws like Canada, might be even more difficult since it's not clear that the practice of scooping other people's phone records is actually illegal. Wireless and land-line phone companies fall under different regulatory regimes. And a couple of decades of mergers, acquisitions and rapid cellphone growth has created a landscape where no one is sure exactly who is in charge. "It's a mess, a complete hodgepodge," says Chris Hoofnagle, West Coast director of the Electronic Privacy Information Center (EPIC), a public interest watchdog. EPIC recently filed complaints with the FCC and the Federal Trade Commission, seeking to force the telecom industry to tighten up its internal policies and prevent data brokers from obtaining customer bills. The response from the phone companies has been "openly hostile," says Hoofnagle. "They say it's not really a problem, and it can be dealt with in other ways."

To date, only one carrier, Verizon Wireless, has gone after the data brokers, filing a civil suit against a different Tennessee company, Source Resources, alleging fraud and civil conspiracy. The suit was settled in September with the online service agreeing to stop the practice and provide details about its methods. On the legislative side, Senator Chuck Schumer, a Democrat from New York, vowed to introduce a bill to criminalize the cellphone data black market, and create a special unit in the FTC to tackle the problem, but his efforts haven't progressed very far either. EPIC is trying to step up the pressure, and will soon launch a series of professional complaints against the data brokers' main clients -- lawyers. "We think in most cases that it's being used for infidelity investigations, in anticipation of divorce litigation," says Hoofnagle.

Regardless of what does or doesn't happen south of the border, Canada's privacy commissioner doesn't seem to be in the mood to let the matter drop. Last winter, she raised the issue of transborder data brokers with the FCC, and now she says she intends to do so again. And with her own purloined phone records in hand, Stoddart will be going after the phone companies. "This data originated in Canada," she notes. It's not just a matter of privacy, in the case of her cell records, it's also government security that has been compromised. "It's a stunning example," she says. "I think this calls for drastic action."

To contact the writer, email **jonathon.gatehouse@macleans.rogers.com**

To comment, email letters@macleans.ca