7-12-2009

Peeking in cyberspace's backdoor

James Stribopoulos
Osgoode Hall Law School of York University

Peeking in cyberspace's back door

PATRICK CORRIGAN/TORONTO STAR

July 12, 2009

JAMES STRIBOPOULOS
ASSOCIATE PROFESSOR, OSGOODE HALL LAW SCHOOL

Criminals are innovative. Not surprising then that they have flocked to the Internet to ply their trade. Just like the rest of us, criminals enjoy anonymity when they go online. The law-abiding cherish that anonymity because it keeps our web surfing histories private.

You might leave an electronic trail behind everywhere you go on the Internet in the form of your 10 digit Internet Protocol (IP) address, but there's a world of difference between that and leaving a calling card with your name at every website you visit.

For the not so law-abiding, of course, that anonymity can be used for far more nefarious purposes than guarding against embarrassment.

It seems obvious that the police must have the power to pierce the veil of an IP address so they can figure out who might be behind the distribution of child pornography or an email sent by a suspected terrorist from an anonymous Hotmail account.

For similar reasons, the police must also be able to tap into a cellphone company's system to figure out the location of a cellphone that belongs to a suspected criminal. (Imagine a case of abduction where a kidnapper is making ransom demands from a cellphone.)

In introducing Bill C-46 (Investigative Powers for the 21st Century Act), the federal government said it was trying to ensure that the police would have the tools they require to keep up with the criminals, while also respecting the privacy of law-abiding Canadians as much as possible.

To be sure, much of Bill C-46 does just that. It contains some much-needed amendments to the Criminal Code. Key among them are:

- Preservation orders: a power to direct an Internet provider to essentially freeze data for up to 21 days; anything longer requires a judge's order.

- Production orders: the ability to obtain a warrant compelling a service provider to furnish information regarding the identify of a customer

behind a particular IP or email address.

- Tracking orders: the ability to obtain a warrant requiring a cellphone company to use its network to assist police in tracking the location of a particular cellphone or BlackBerry user.

As a civil libertarian, I am not overly fussed about any of these new powers. For the most part, they seem to strike a relatively fair balance between individual privacy interests and the needs of law enforcement. I say this for two reasons.

First, with the exception of freezing data for up to 21 days, these provisions insert a judge between the police and the individual whose privacy is being affected. I am comforted to know that before the police can snoop into my Internet surfing history or track my whereabouts using my BlackBerry, they will need to convince a judge that they have reasonable grounds to suspect the snooping is necessary to ferret out evidence of a crime.

In addition, the information obtained is rather limited. Under these new powers, the police are restricted to circumventing the anonymity that would otherwise apply. Before they can go further, for instance by gaining access to the substance of one's email correspondence or entering your home to seize your computer, they would still need to obtain a conventional search warrant. That would still require more substantial evidence.

The rather sensible idea behind these key provisions in Bill C-46 is to enable police to gather the building blocks to begin developing a case for obtaining a traditional search warrant. Getting behind the anonymity of an IP

address or unlisted cellphone number will often be the first step in a series of investigative measures that the police will undertake before they can do that. To deny police the ability to take these sorts of preliminary investigative steps would give criminals free reign by simply going online or picking up a cellphone. No law-abiding Canadian wants that.

If the story ended with Bill C-46, the civil libertarian in me would be entirely content. Unfortunately, it would seem that the federal government doesn't have the same faith in the warrant requirement that I do.

There is also Bill C-47 (Technical Assistance for Law Enforcement in the 21st Century Act). Ostensibly, it sets out to address the technical end of the Internet and cellphone business to make sure those industries are well suited to cooperate with law enforcement. Unfortunately, some of the provisions found in it serve as a back door to the balanced approach found in Bill C-46.

Specifically, Bill C-47 allows certain "designated persons" within police forces to entirely circumvent any legal protections that would otherwise apply. Instead, based on the say-so of these specially empowered police officers, Internet service providers and cellphone companies would be required to furnish a host of otherwise private information to the police, on demand, including an individual's name, address, telephone number, email address, IP address, etc. Not only does this specially designated officer not require a warrant, he or she doesn't even have to reasonably suspect that access to the information is necessary to investigate a crime.

One hopes that Parliament will shine a light on this puzzling back door and close it before Bill C-47 becomes law.