# Canada: Conservatives to revive Liberals' Internet surveillance legislation

**David Adelaide**
**9 September 2006**

The minority Conservative government of Stephen Harper is widely expected to revive legislation, originally introduced by the preceding Liberal government, that would expand the ability of the Canadian state to spy on domestic Internet communications.

Bill C-74, the Modernization of Investigative Techniques Act, was introduced by the minority Liberal government of Paul Martin in November 2005 only to die when the minority government was brought down later that month. The two main planks of the Liberal bill were a requirement that facilities to intercept communications be built into the telecommunications apparatus, and a requirement that the telecommunications companies hand over "subscriber information" to the authorities upon request—i.e., the name, address, contact information, and IP address of particular Internet users. The legislation would have established financial penalties of up to $500,000 for violations of its provisions.

Attempting to forestall public opposition to the bill, the Liberals emphasized that under its provisions the police and the Canadian Security Intelligence Service would still have had to obtain a warrant before fully intercepting Internet communications. In other words, the principal thrust of their legislation was to expand the technical capacity rather than the legal basis for interception, by legally compelling the telecommunications companies to install "backdoors" facilitating the surveillance of Internet communications.

As such, the legislation *did* and will, if revived by the Conservatives, constitute a mechanism for expanding the surveillance capabilities of the state, as does the requirement that the telecommunications companies provide information linking persons to IP addresses. With such information, it would be easier to identify the authors of anonymous newsgroup postings, chat participants, or file-sharers. Under the Liberals' bill, it need be added, these requests for "subscriber information" were not to be subject to any judicial oversight.

The effort to increase surveillance of the Internet in Canada is clearly modeled on precedents established by other governments around the world, which, like Canada's, have seized on the events of September 11, 2001, and the so-called "War on Terror" to dismantle longstanding democratic rights and push for police-state measures.

In the United States, the Communications Assistance for Law Enforcement Act (CALEA), originally passed in 1994, was recently extended to cover wireless and Voice-over-IP (VOIP) services. The US legislation obliges telecommunication companies to install interception equipment and to provide subscriber information. Earlier this year, the Australian government rammed through its Telecommunications Interception (Amendment) Act 2006, under which the courts are instructed to grant interception warrants even if surveillance is deemed merely "likely to assist" in obtaining intelligence "related to security."

Officially, the Harper Conservatives have said very little about their plans to revive the Liberal legislation. "We're working on it," commented Melissa Leclerc, a spokesperson for Public Safety Minister Stockwell Day, indicating that the Liberals' Internet surveillance legislation could well be revived as soon as the fall session of Parliament.

There is every reason to expect that the Conservative legislation will be at least as permissive vis-à-vis the security and intelligence apparatus's capacity and legal power to spy on Internet communications as was the Liberal bill. Harper, before and since his election, has invested much effort in courting the Canadian security apparatus and the military. These efforts were repaid during the election campaign itself when the Royal Canadian Mounted Police (the paramilitary federal police service) took the unprecedented step of making an election-time announcement that they were opening an investigation into the Liberal Party around the issue of Liberal Party insiders benefiting from prior knowledge of a forthcoming pronouncement on the taxation of income trusts.

Since the election, the Harper government has enthusiastically embraced the Bush administration's "War on Terror" and has extended and expanded the involvement of the Canadian Armed Forces in the occupation of Afghanistan. In June 2006, the government, together with the media and the security forces, seized on the alleged Toronto terror plot in order to claim that Canada was not immune to terrorism, the better to push for increased repressive powers for the state.

The Conservatives have yet to make public their full intentions regarding the Internet surveillance legislation, doubtless because they are hoping to avoid rousing public opposition not only to that legislation but also to the 2001 Anti-Terrorism Act, which is currently facing a mandatory five-year parliamentary review of its draconian provisions.

Nevertheless, the telecommunications companies have already gone out of their way to signal their eagerness to comply with whatever new surveillance regime is instituted.

Bell Sympatico made headlines in the middle of June by unveiling a new customer service agreement that gives the

company the right to "monitor or investigate content or your use of your service provider's networks and to disclose any information necessary to satisfy any laws, regulations or other governmental request."

The other large telecommunications providers have introduced similar clauses in their customer service agreements. The *Globe and Mail* (which is owned by the same parent company as Bell) cited the insistence of a Telus spokesman, Jim Johannsson, that "if the law changes, we could comply with the law as long as the party has legal authorization to see the information."

A number of theories have been put forward in the press as to why the telecommunications companies are so eager to comply with legislation that has yet to be reintroduced, let alone passed by the current minority parliament. A *Globe and Mail* article cited comments by University of Ottawa professor Wade Deisman to the effect that the companies had been "intimidated" into putting forward such customer service agreements by a threat that the forthcoming legislation would require the companies to have staff available on a round-the-clock basis in order to respond to warrants from the authorities.

Another theory was advanced in a *Globe and Mail* online forum hosted by Jack Kapica. Kapica suggested that the big telecommunications companies hope to use the government's demand for interception technologies as a pretext for introducing bandwidth-shaping technologies useful in clawing back profits from the often much smaller companies that are promoting services like VOIP. According to Kapica, "These tools could be used to gather information about subscribers' activities, as Ottawa would demand, and Bell could therefore use the argument of compliance to justify buying the technology."

There is doubtless some truth to each of the above theories. Nevertheless, what they both tend to downplay is the significant extent to which the large telecommunications companies, as major players in the big business milieu to which the Canadian government is oriented, have a direct interest in the anti-democratic right-wing agenda promoted now by the Harper Conservatives and earlier by the Martin Liberals.

Recently, the government's privacy commissioner, Jennifer Stoddart (a Liberal appointee), singled out the forthcoming Internet surveillance legislation as a harbinger of more strident inroads against democratic rights to freedom from unreasonable search and seizure. In an interview published by *canoe.ca*, Stoddart said, "What we see is the foreshadowing of a regime that could come in, which would allow for warrantless searches of telecommunications material."

Separately, in an audit of the Canada Border Services Agency delivered at the end of June (available online), Stoddart highlighted the extent to which Canadian authorities are freely and unaccountably sharing information with their US counterparts. Wrote Stoddart, "[m]any of the information exchanges between the CBSA and the United States at the regional level are verbal, and are not based on written requests. These exchanges are not recorded consistently and do not follow the approval process as established under CBSA policy."

Elsewhere in the same report, the privacy commissioner cites a 2004 study commissioned by her own office showing that 85 percent of the Canadian population had a moderate or high level of concern about transfers of personal information to the United States, a concern no doubt fueled by high-profile travesties such as the case of Maher Arar. An Ottawa engineer, Maher was "rendered" by US authorities to Syria, where he was incarcerated and tortured, as a result of "intelligence"—a chain of guilt by association established on the basis of covert surveillance—passed to American authorities by Canada's security forces.

This high level of potential public opposition compels the Canadian ruling class to adopt an incremental approach to implementing the kind of rollback of democratic rights that has proceeded more forthrightly elsewhere. Significantly, the Liberals' original legislation, Bell's revised customer service agreement, and the privacy commissioner's report on the Canada Border Services Agency have all received precious little attention from the press or from the opposition parties in the House of Commons.

The telecommunication companies' willingness to comply with legislation yet to be passed is of a piece with this incremental strategy. From the standpoint of the Canadian ruling elite, the hope is that, if the technical and contractual implications of increased Internet surveillance are already taken care of, then the Canadian public will essentially be presented with a *fait accompli* by the time the legislation again comes before parliament.

It is interesting to note that the legislation drafted by the Liberals would have required the telecommunications companies to assist in the decryption of encrypted communications, but only in the case where they themselves provided the encryption technologies. The legislation explicitly exempted them from doing the (nearly) impossible—i.e., decrypting communications encrypted with software (such as GnuPG), the open-source replacement for PGP) where control over the keys remains with whoever has control over the computer sending the message.