Canadian Conservatives' cyber-bullying bill—a pretext for expanding police surveillance

Dylan Lubao
10 December 2013

Under legislation now before parliament, Canada's Conservative government is seeking to greatly expand the state's power to spy on Canadians' use of the Internet, including authorizing warrantless investigations of Internet activity.

Entitled the *Protecting Canadians from Online Crime Act*, Bill C-13 was presented by Justice Minister Peter Mackay as a measure to combat online harassment, so-called cyberbullying, when he tabled it in the House of Commons in late November. The issue of cyberbullying has received widespread coverage in Canada's corporate media in the wake of the tragic suicides of teenagers Rehtaeh Parsons and Amanda Todd, both of whom were victims of cruel Internet harassment. The sustained media furor surrounding the girls' deaths has fed directly into the push by the ruling class to increase the surveillance powers of the state.

Exploiting the public grief and anger over these tragedies, the Conservatives have crafted an omnibus bill that under the cover of fighting cyberbullying greatly expands police powers to search and seize personal Internet data. Measures that sanction warrantless searches and water-down the criteria for obtaining warrants are wedged between clauses that impose severe penalties for sharing "intimate" images of an individual over the Internet without that person's consent, including prison terms of up to five years.

The Conservatives have repeatedly used omnibus bills to impose regressive measures, burying cuts to unemployment benefits, the gutting of environmental regulations, and sweeping attacks on federal workers' pensions and rights to bargain and strike within massive budget bills.

The duplicitous manner in which the Conservatives are proceeding with their ostensible anti-cyberbullying legislation is entirely in keeping with its anti-democratic content.

Bill C-13 expands police powers in two distinct ways.

First, it introduces a lower threshold for the issuing of warrants authorizing the police to force telecommunications companies and Internet Service Providers (ISPs) to hand over personal information and data or force them to be retained for future police perusal.

Law enforcement agencies will only have to vow to the courts that they have a "reasonable suspicion" someone is complicit in a crime or intent on committing one to obtain a warrant. Traditionally, police have been held to a much more demanding standard than mere "suspicion"—the standard of "reasonable and probable grounds."

In lowering the threshold for police searches of Internet use, the Conservative government is flouting a recent Supreme Court decision that argued that to empower the police to conduct searches on the basis of "suspicion" would imperil citizens' privacy rights: "In most cases, the state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion."

Second and even more sinisterly, Bill C-13 will allow police and other law enforcement agencies to request telecom companies and ISPs to voluntarily disclose Canadians' online information and communications. And to do so even outside the scope of a criminal investigation. The Canadian Criminal Code currently forbids such requests.

Moreover, Bill C-13 will provide companies that fulfill such voluntary police requests with full immunity from criminal or civil penalties for complying. In other words, they are to be granted protection for participating in police fishing expeditions and spying.

Explains Ottawa criminal lawyer Michael Spratt, "In essence the police will be able to ask companies to turn over data on anyone, at any time, for any reason." Moreover, "the bill leaves no legal incentive for companies to be cautious in the dissemination of data—and no recourse for individuals whose privacy is compromised.

"This unregulated and expansive police power would result in more fishing expeditions … Given the recent allegations of government complicity in domestic spying," continues Spratt, "an expansion of police power to collect personal data under C-13 should be viewed with the utmost suspicion."

Canada's telecommunications industry, it need be added, is dominated by a handful of giant corporations whose owners and executives share the right-wing political outlook of

Canada's elite—an elite that is fearful of social discontent and, as such, has repeatedly supported attacks on democratic rights, whether it be the criminalization of strikes and social struggles or the overturning of basic democratic juridical principles like an accused's right to know the case against them.

However, were a company to balk at police requests for "voluntary" disclosures, especially from Canada's powerful and rapidly expanding national security apparatus, the state and government would have huge leverage to force compliance through the their tight legislative and regulatory control over the industry.

Willingness and the technical capacity to hand over client information and communications to law enforcement agencies have been a prerequisite for doing business in the Canadian telecommunications industry for nearly two decades. A report published in the *Globe and Mail* in September outlines the Solicitor General's Enforcement Standards (SGES), an accord that explicitly instructs mobile phone service companies to cooperate with law enforcement requests, including in the deciphering of encrypted communications. The SGES also mandates them to have the technical capacity to retrieve information about earlier communications of persons of interests to police and to transmit to police authorities almost instantaneously their current communications.

Until the *Globe* report, the SGES was entirely unknown to the Canadian public. Interviews with representatives of major telecommunications firms made clear that their only reservation with a proposed expansion of the SGES to include Internet communications was the increased costs that would be associated with it.

Bill C-13 resurrects the most egregious elements of Bill C-30, a previous Conservative attempt to expand police powers over the Internet and which was packaged as an instrument for combating child pornographers.

That bill would have amended the Criminal Code so as to empower the police to compel Internet companies to give them clients' personal data without a warrant. It was widely opposed by the general public as well as by civil liberties organizations and quietly withdrawn by the Conservatives last February.

Bill C-13 provides instead for voluntary disclosures from Internet companies, which, when combined with full legal immunity for those who comply, effectively resurrects the police power to obtain data without recourse to a warrant.

Because of the centrality of the Internet in people's lives, access to data about their Internet use would provide police agencies with vast information about their work, personal and social networks, finances and political beliefs and activities. This would enable the state to quickly assemble a detailed portrait of working-class and other dissident movements.

In the face of criticism of the new Conservative bill, Justice Minister MacKay has outright lied, asserting that the police "must still obtain a warrant. There is no warrantless access."

In making this claim, MacKay referred to the Personal Information and Electronic Documents Act (PIPEDA), a privacy law for the private-sector that entitles a company to voluntarily disclose client data to law enforcement agencies that possess "lawful authority" to make such requests. However, the "authority" cited in PIPEDA is not defined as a warrant, court order, or any legally-recognized court document, thus fully sanctioning warrantless data requests.

Lies and cover-ups are standard operating procedure for the Conservatives and indeed the entire political establishment, especially when it concerns the mass spying programs of government intelligence agencies.

When it was revealed last June that the Communications Security Establishment Canada (CSEC), the Canadian counterpart and partner of the US National Security Agency (NSA) was mining the metadata of Canadians electronic communications, MacKay, the Defence Minister at the time, repeatedly insisted that CSEC's activities were not directed at Canadians and did not violate core constitutional rights.

These statements were founded upon a spurious definition of what constitutes a constitutionally protected private communication. CSEC and Canada's government, under the Liberals who first authorized CSEC's metadata mining and now the Conservatives, maintain that metadata is not integral to Canadians' communications (merely the "envelope) and therefore "fair game" to be spied upon,

The opposition New Democratic Party (NDP) and Liberals have tabled a motion to split Bill C-13, separating the cyberbullying and surveillance clauses. At the same time, both of these big-business parties continue to remain all but totally silent on CSEC's activities—its role in the illegal activities being carried out by the NSA worldwide and its spying on Canadians electronic communications (phone calls, text messages, e-mail, Internet activity, etc.). Instead they have devoted months haranguing the Conservatives over the petty Senate expense-spending scandal.