Canada’s telecoms aid state surveillance by handing over personal data

Ed Patrick
5 August 2014

As part of a vast expansion of the Canadian surveillance state, federal government police agencies are requesting personal subscriber information from the country’s telecommunications companies (such as Rogers, Bell, TELUS, and Quebecor’s Vidéotron) at staggering rates—with well over a million such requests per year.

Internal documents from Public Safety Canada and others tabled by the country’s privacy commissioner in the House of Commons indicate that the vast majority of these requests are made without a warrant. Yet the telecoms almost invariably provide the requested information.

The Public Safety Canada documents show that between 2006 and 2008, authorities made on average 1.13 million requests per year for “basic subscriber information.” These figures are in keeping with those collected by the Office of the Privacy Commissioner, which showed at least 1.2 million such requests in 2011.

According to interim privacy commissioner Chantal Bernier, the country’s telecom companies are refusing to provide her office with any new information on the scope of their collaboration with federal government police and security agencies like the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service. In particular, the telecoms have declined to disclose the number of times they have handed over personal customer information to the state in the absence of a warrant.

A Conservative appointee, Bernier was quite willing to give the police a wide berth, advancing the authoritarian notion that “there are times when there is no time to get a warrant—life is in danger.” Yet even she was forced to voice dismay over the telecoms’ refusal to provide information on how many warrantless requests they have fulfilled. “We have tried many times,” said Bernier. “They’ve given us very general comments.”

Only once and in respect to a single year, 2011, did some of the telecoms offer up information about their collaboration with state agencies. Even then, only nine out of the country’s several dozen telecoms participated in a joint response, collected in an aggregate form by the Canadian Wireless Telecommunications Association (CWTA). Issued via a law firm, the CWTA report provides no company specific information. The report, again drawing on responses from just nine companies, revealed that a massive 1,193,630 requests were lodged by federal agencies in 2011 alone.

The telecoms do not inform their customers when a request has been made or fulfilled, so Canadians have no way of knowing when or if their information is being scrutinized by the authorities.

The providers were selective in their responses, but based on just three of the nine companies, in that same year, 784,756 users and accounts were accessed by government agencies. Given the small sample size and the fact that the figures do not include requests from local or provincial police forces, the actual number must be much higher. Furthermore, the information collected by Public Safety Canada demonstrated that some forces, such as the RCMP, were not even tracking warrantless requests, some of which were apparently verbal.

Both Rogers and the smaller TekSavvy have released what they turn “transparency reports” that reveal little beyond the massive number of state requests for information. Rogers alone received 175,000 requests last year, though the company declined to admit the number of times it provided the desired information.

In 2010, the RCMP admitted that in 94 percent of cases customer name and address information was provided without a warrant. Given the sheer volume of requests per year—which would amount to about one request every 30 seconds—there is essentially no chance that any but a tiny fraction of the requests could be sanctioned by a warrant.

Canadian law permits telecoms to refuse to provide this information unless a warrant is produced. That they rarely

do so is both because the government encourages their cooperation through carrots and sticks and because the telecoms are, apart from a handful of bit players, themselves giant corporations that fully support the assault on the working class, the revival of Canadian militarism, and the associated erosion and dismantling of democratic rights.

The telecoms are able to seek compensation from the authorities for fulfilling police requests, and the data from the 2011 report shows that the companies nearly always seek such compensation. According to the CWTA report, one company even created a system by which a "mirror" of user data was automatically sent to the police, to be mined at their own pleasure.

Moreover, the federal government has made it a condition of obtaining a wireless license that carriers must agree to allow Canadian security agencies and police access to their networks in order to spy on suspects and must have or procure the technical means to retain data for police investigations.

The exposure of the close relationship between the telecoms and the state comes in the wake of a series of revelations, many of them coming from Edward Snowden, concerning the Communications Security Establishment Canada (CSEC), the Canadian partner of the US National Security Agency (NSA). CSEC is an integral partner in the NSA's illegal global spying operations, which target literally everyone from the heads of government of US allies to ordinary citizens, including Americans.

When it was first revealed that since 2005 CSEC has been mining the metadata of Canadian electronic communications, which includes telephone and cell phone calls, as well as e-mails and text-messages, the Conservative government brazenly lied, claiming that CSEC never spies on Canadians. However, some eight months later, it baldly asserted the right to collect and scrutinize the metadata from Canadians' communications, saying such information was innocuous (see: "CSEC and Harper government assert right to spy on Canadians").

Similarly, the government is now claiming that the voluntary disclosure of information to the state by the telecom industry is much ado about nothing, comparing it to the type of information found in a telephone book.

That claim, however, was exposed as baseless in June, when the Supreme Court of Canada issued its decision on the R. v. Spencer case, which revolved around the legal status of the current practice of telecoms voluntarily disclosing basic subscriber information to federal agencies and law enforcement without court orders (i.e., warrants). The country's highest court ruled the practice unconstitutional.

Though the court maintained the original conviction in the case, saying the police could not have known what they were doing was illegal, it said that the warrantless disclosure of the information constituted an illegal search.

"The disclosure of [subscriber] information," said the court, "will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search."

Stephen Harper's Conservative government has indicated that it intends to find a way to circumvent the court ruling so as to perpetuate a situation where police, with the complicity of the telecoms, can access private information and carry out what the country's highest court has deemed to be illegal searches at will.

Although the new Privacy Commissioner has urged the government to reconsider two bills now before parliament in light of the court decision, the Conservatives have vowed to press forward with their adoption without amendment.

Bill C-13, which is being shamelessly touted as an anti-cyber-bullying bill, would grant telecoms complete legal immunity from any civil or criminal liability for disclosing data to authorities—giving further incentive for the already willing corporations to collaborate with the government. The bill would cover not only subscriber data, but more sensitive information such as tracking and transmission data.

Bill S-4, meanwhile, would expand the number of entities that can request subscriber information to include private organizations engaged in the investigation of any kind of crime or breach of contract whether actual or simply possible.