

## “Lawful Access” in Canada: Government’s power to monitor citizens’ electronic communications

---

### **Canadian government introduces legislation to increase Internet snooping powers**

**FIPA and other rights groups have united to oppose a radical new  
surveillance regime for cell phones and the Internet**

Updated November 2, 2011

---

For the latest update, see the [STOP ONLINE SPYING CAMPAIGN](#).

The federal government is about to introduce legislation which will vastly increase police surveillance of Canadians’ Internet and telecom communications. Since 2001, privacy watchdog groups, including FIPA, have squared off against successive Liberal and Conservative governments on similar “lawful access” legislation. We are quickly gearing up to oppose it again.

On May 9, Public Safety Minister Vic Toews [re-affirmed](#) the government’s commitment to passing lawful access legislation which will

- require mandated surveillance capabilities at Canadian Internet Service Providers (ISPs)
- force ISPs to disclose subscriber information such as name and address with out a warrant, and
- grant the police broad new powers to obtain transmission data and force ISPs to preserve data.

According to Internet law expert [Michael Geist](#), “The package is benignly nicknamed “lawful access,” but isn’t benign. If the Conservatives move forward with it, it would feature a three-pronged approach focused on information disclosure, mandated surveillance technologies, and new police powers.” See also Online surveillance law could erode Canadian freedoms, says Canada’s Privacy Commissioner: <http://fipa.bc.ca/home/news/295>

The new legislation is being portrayed by the government and police groups as necessary to enable law enforcement agencies to catch up to the new technologies being used by criminals.

But Privacy Commissioner Jennifer Stoddart and her Provincial counterparts say that such measures go much further than that, giving police powers they did not have in the past and should not have today. See <http://www.thewirereport.ca/reports/content/12409-privacy-commissioners-concerned-about-lawful-access>

**We await the new version of the legislation, but it will be similar to two bills the government has introduced in 2009:**

- the *Investigative Powers for the 21st Century (IP21C) Act*, and
- the *Technical Assistance for Law Enforcement in the 21st Century Act*.

**Government backgrounders:**

- Backgrounder: Public Safety Canada, [Technical Assistance for Law Enforcement in the 21st Century Act](#)
- Media Release: Public Safety Canada, [Government Of Canada Introduces Legislation To Fight Crime In The 21st Century](#)
- Backgrounder: Department of Justice, [Investigative Powers for the 21st Century \(IP21C\) Act](#)

## **How much surveillance is too much?**

The debate over extending lawful access is a question of balance – of where to draw the line on infringing on personal privacy and other civil liberties in order to improve security or prevent crime.

FIPA and the Department of Justice co-hosted one of three consultation sessions that were held across Canada in 2005 to air the lawful access proposals. Of the 30 groups that participated in Vancouver, not one had a positive view of the federal plan. Rather, it was heavily criticized as an excessive and unwarranted assault on the privacy rights of Canadians.

Now FIPA and other privacy and civil liberties groups across Canada are gearing up to alert Canadians to this imminent threat to their privacy and publicly oppose the federal legislation.

**Our view in a nutshell is simple:**

***We have no objection if police and security forces have the same ability to intercept and monitor email and wireless communication that they currently have to intercept and monitor letter mail and conventional telephone communication. But the lawful access proposals go far beyond this to propose much greater license to intercept and monitor, and with a lower standard of judicial supervision.***

FIPA and other rights groups across Canada are preparing a national alert and action plan, and we are urging Canadians who value their privacy rights to take part. We will be working with the Canadian Internet Policy and Public Interest Clinic (CIPPIC), the BC Civil Liberties Association, the Public Interest Advocacy Centre and others.

Do you think law enforcement agencies should have more power to place our electronic communications under surveillance? Watch this page for suggested actions you can take to have your say and make an impact on this important issue!

## What you can do about this:

- Check out the **Stop Online Spying** Campaign: <http://StopSpying.ca>
- If you have concerns about the Canadian government's Lawful Access proposals, [contact your Member of Parliament](#) and let him or her know. MPs will be voting on these proposals sometime in the near future.
- You can also write to:

Prime Minister Rt. Hon. Stephen Harper: [pm@pm.gc.ca](mailto:pm@pm.gc.ca)

Hon. Rob Nicholson, Minister of Justice and Attorney General of Canada:  
[Nicholson, Rob \(Hon.\)](#)

Hon. Vic Toews, Minister of Public Safety:  
<http://www.publicsafety.gc.ca/abt/contact-eng.aspx>

- Join CIPPIC's "Lawful Access" activist network, and CIPPIC will send you email bulletins informing you of important news on this initiative, and letting you know when urgent action is needed. To sign up, email [cippic@uottawa.ca](mailto:cippic@uottawa.ca), putting "Subscribe to Lawful Access Network" in the subject line.

## MORE INFORMATION AND RESOURCES

Prof. Michael Geist, the founder of CIPPIC and one of Canada's leading experts on Internet and e-commerce law, states that the federal plan creates ***"A real surveillance network... It envisions a dramatically new Internet, new kinds of surveillance powers for network providers and requirements for providers to disclose information about Canadian Internet users, often with little or no judicial oversight."***

Most striking among these is the power to compel the production of consumer information without a warrant, removing the crucial safeguard of judicial oversight.

Under the lawful access plan, Internet and telecommunication service providers (TSPs) will be required to install high-tech equipment that is "intercept capable". This will give police and the Canadian Security Intelligence Service (CSIS) the ability to intercept and monitor the email, web surfing, telephone and cell phone communications of thousands of people simultaneously. The enormous cost of this new technology will be borne by the TSPs, who will pass it along to consumers.

Combined with new technologies that permit the interception and instant analysis of vast troves of data, the proposed legislation would give police the power to instantly summon information about the private lives of individual Canadians.

## Resources

### The Stop Online Spying Campaign

The Stop Online Spying campaign is spearheaded by [Open Media](#) and supported by a large coalition of public interest and civil liberties organizations, businesses and concerned academics.

We have come together to create public awareness and debate about Bill C1 and encourage Canadians to oppose it. The government must explain why the invasive, excessive and costly increase of surveillance powers in the bill is justified.

**Campaign Website:** <http://StopSpying.ca>

*Comments on the Lawful Access Consultation Document*, Information and Privacy Commissioner of BC, Dec. 16, 2002: [Click Here](#)

Terrorism, Trade, and Internet Privacy – Martin R. Dowding, University of British Columbia: [Click Here](#)

### FROM FIPA:

Comments on the Lawful Access Proposals (March 2005): [Click Here](#)

The Lawful Access Proposals: Why Canadians Should Say “No” to Expanded Electronic Surveillance by Police – FIPA, Feb. 13, 2003: [Click Here](#)

Comments on the Government of Canada’s Lawful Access Consultation Document – Submission to Department of Justice by BC Freedom of Information and Privacy Association (FIPA), Dec. 16, 2002: [Click Here](#)

\* \* \*