OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
*for British Columbia*

Protecting privacy. Promoting transparency.

February 27, 2012

Kevin Sorenson, MP
Chair
Standing Committee on Public Safety and National Security
Sixth Floor, 131 Queen Street
House of Commons
Ottawa, ON K1A 0A6

Dear Mr. Sorenson:

**Bill C-30 – An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and Other Acts––OIPC File No. F12-48383**

I would like to take this opportunity to make some initial comments about Bill C-30 that focus on the parts of the Bill that relate to warrantless access to individual personal information.

There is little question that Bill C-30 has touched a deep nerve among Canadians. The public wishes to ensure that law enforcement can do its job of protecting public safety. It is equally evident Canadians care deeply about their privacy rights.

I believe it is possible for Bill C-30, if carefully constructed, to achieve both of these goals. Previous versions of what is now Bill C-30 fell short of achieving this balance. In drafting Bill C-30 I believe government has moved to address some of the shortcomings expressed about the previous proposals.

The number of data elements that were previously subject to warrantless access requests by law enforcement, for example, has been reduced from 11 to 6. Provisions concerning the reporting out of the use of warrantless powers to the responsible Minister are no longer left to the subjective judgement of law enforcement officers. These reports or audits must be conveyed to the Minister responsible with a copy to offices such as mine, measures that will, to a degree, increase the transparency of powers exercised under Bill C-30.

I appreciate these changes attempt to improve the legislation. However, they remain premised on, and leave unaltered, the Bill's fundamental flaw; that law enforcement can obtain an array of personal information about citizens, including real names, home address, unlisted numbers, email addresses and IP addresses from internet service providers, without a warrant. That Canadians view this information as sensitive, and

have an expectation of privacy with respect to it, can be judged by their reaction to Bill C-30.

This point is critical because while privacy rights are by no means absolute, any action by the state that would restrict or infringe them should only be taken where it is necessary to do so and only to the least extent possible.

The significance of the privacy rights of citizens in a free and democratic society was eloquently stated by Mr. Justice La Forest,

> [Privacy] is at the heart of liberty in a modern state. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[1]

Bill C-30 gives government, through the arm of law enforcement, the authority to obtain an individual's private personal information. This kind of information is far from inconsequential as some would suggest. As one commentator on privacy matters has noted:

> It's more insidious than a wiretap. It allows police to massively monitor the net and build associations with the subscriber information they have on you and from there determine whether they have a case against you or not.[2]

The only restriction on this power is that any request for the information be related to the duty or function of that official. This broad power is not limited to reasonable grounds to suspect criminal activity or to a criminal investigation and could affect any law-abiding citizen.

Why does law enforcement require such authority from the state? Where is the evidence that these enhanced powers are necessary? These are the questions that I and my colleagues have asked on behalf of citizens on numerous occasions and to date have yet to be addressed with a compelling answer.

It has been widely reported that internet service providers have, in up to 95% of cases, already voluntarily provided law enforcement with the information sought. I also note Bill C-30 contains a provision that excuses ISP's from civil or criminal liability for voluntary disclosure or preservation of information to law enforcement. One would expect this would further open this method of information gathering to law enforcement.

---

[1] *R. v. Dyment* (1988), 45 C.C.C. 93d, 244 (S.C.C.), at para. 17.

[2] Chris Parsons is a doctoral candidate at the University of Victoria studying digital surveillance.

Moreover, in the remaining 5% of cases where information was not provided voluntarily I am not aware that the need to obtain a warrant to gather information posed any kind of obstacle to law enforcement undertaking its role effectively. If an issue exists about whether law enforcement is able to acquire necessary information in a timely way, let us examine that matter and study where the heart of the problem lies. If the problem resides with the efficiency of the justice system, for example, the availability of judicial authorities to hear warrant applications, let us work to rectify these matters. The answer, however, is not to infringe the privacy rights of citizens without any or minimal oversight.

It is my view that effective law enforcement and the protection of citizens' right to privacy are not mutually exclusive. It is therefore imperative that Bill C-30 be amended so that law enforcement officials are required to demonstrate to a judicial authority the need to acquire an individual's personal information. Such a measure will ensure that law enforcement can undertake its critical work while ensuring citizens' rights are safeguarded.

Yours sincerely,

**ORIGINAL SIGNED BY**

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

pc: Committee Members of the
Standing Committee on Public Safety and National Security (SECU)