CIPS Response RE: Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act

CIPS, Canada's association of IT professionals applauds the Government of Canada's support of bullying awareness and cyber safety initiatives.

While not opposed to the sections of Bill C-13 that address cyberbullying, we believe cyberbullying is a social issue, best addressed through education and by setting good examples.

CIPS is committed to positive initiatives, as well as to the modernization of legislation to deal with emerging technologies. However, the effects of Bill C-13 on Information Technology, the Canadian Telecommunications industry, as well as Canadian business in general far outweigh its positive aspects.

CIPS is very concerned about certain measures in the proposed Bill, "An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act".

As computer technology professionals, we appreciate the need to modernize legal terminology to include all forms of telecommunications. In the process of doing so, the proposed legislation significantly lowers the evidentiary threshold for law enforcement surveillance of all forms of communication and introduces new civil and criminal immunity provisions. It will have applicability far beyond the relatively small number of cases that involve the distribution of intimate images.

We are also familiar with the technical aspects of collecting and storing information. While this legislation does not contain the ill-considered warrantless access to subscriber information and telecommunication infrastructure modification provisions of the predecessor Bill C-30, ("The Protecting Children from Internet Predators Act,") the proposed legislation may, in our view, still provide for warrantless access to information as well as a reduced threshold for warrants.

> CIPS is concerned about the new investigative powers, (including preservation orders) proposed by the Bill C-13 and the thresholds for their use, including voluntary disclosure of Canadians' online information.
>
> CIPS is concerned about the use of investigative powers by a peace officer or public officer without a warrant.
>
> CIPS is also concerned about the reduced threshold for warrants from "reasonable grounds to believe" to "reasonable grounds to suspect" for specific production orders such as tracking data or transmission data.

Removal of the words "*enforcing or administering this or any other Act of Parliament "* in section 487.014(1) of the *Criminal Code of Canada* dangerously broadens the applicability of this section to allow voluntary requests for any reason. Immunity from civil or criminal prosecution proposed in Section 487.0195 (1) and (2) provides a powerful business-case incentive for Internet Service Providers (ISPs) to routinely comply with requests. This may lead to an overly reliant relationship between ISPs and "peace officers and public officers."

Except for universities and similar entities, ISPs are, in general, for-profit businesses that will seek to accomplish what is required of them with the least cost possible. From an information technology point of view, this may easily lead to "de facto" compliance with law enforcement requests. It may lead to gratuitous retention of data "just in case it's requested." Immunity from civil or criminal liability will, from a business standpoint, make it more effective to acquiesce to requests rather than pay legal staff to scrutinize each one on its merits.

CIPS believes the proper channel for production and preservation requests from Internet Service Providers is through a judicial warrant, issued with an appropriate legal and evidentiary threshold.

> CIPS is also concerned about a lack of accountability and the immunity of data providers in preserving and disclosing personal information without a warrant.

Under the CIPS Code of Ethics, CIPS members must:

> *- treat all client business information as confidential, and respect copyrights, trade secrets, privacy and terms of license or other applicable agreements;*
>
> *- understand and comply with any obligations that may be imposed on them under applicable privacy legislation, including The Personal Information Protection and Electronic Documents Act, and any amendments to or successor legislation; …*

It is our position a CIPS member has, in most cases, two prohibitions on sharing a client's confidential information: 1) the ethical obligation as noted above; 2) a very likely contractual obligation. In both cases, legal compulsion is generally a defense; in other words, permits disclosure.

In neither case however, does the ethical obligation nor the likely legal obligation permit voluntary sharing of confidential information without consequences to the CIPS member. Breach of confidentiality penalties can be severe. It is also possible an ethics complaint will be filed with CIPS and thus the member may be disciplined accordingly.

Bill C-13, as it stands, could suggest a CIPS member contravene the CIPS Code of Ethics, if requested by an authority to 'voluntarily' disclose 'private' information.