THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

September 15, 2009

Michael D. Chong, P.C., M.P.
Chair
House of Commons Committee on Industry, Science and Technology
Sixth Floor,
131 Queen Street
Ottawa, ON K1A 0A6

Dear Mr. Chong:

Re: Bill C-27, *Electronic Commerce Protection Act* (ECPA)

INTRODUCTION

The Canadian Bar Association welcomes this opportunity to comments on Bill C-27, the *Electronic Commerce Protection Act* (ECPA). The CBA is a national association representing 37,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice. This submission was prepared by the National Competition Law Section and the National Privacy and Access Law Section (the CBA Sections). The CBA Sections comprise over 2900 lawyers who have in-depth knowledge in the areas of competition and antitrust law as well as privacy matters and access to information. The CBA Sections have been active in providing commentary on developments in competition and privacy and access law and policy.

The CBA Sections fully support the government's efforts to combat unsolicited commercial email messages as well as fraudulent and deceptive electronic communications practices that collectively can be considered "abusive communications". We believe that there is consensus among most stakeholders on what types of conduct constitute abusive communications and can be considered harmful or problematic, or, to put it in terms of the purpose of the ECPA, "conduct that discourages the use of electronic means to carry out commercial activities".

CONCERNS WITH THE PROPOSED LEGISLATION

a) Overbroad approach risks unintended consequences

In our view, the ECPA approaches the problem of abusive communications too broadly. Essentially, the ECPA has adopted a "ban all, subject to exceptions approach" to all types of electronic commercial messages (except voice and fax) as well as installations of computer

programs on electronic devices. This approach raises some significant concerns about unintended negative consequences.

The ECPA outlaws most forms of commercial speech that use electronic communications technology and uses exceptions to define permitted communications. While these exceptions may be clarified or expanded upon in regulations, we believe that the preferred approach is for the statutory language to be clear and comprehensive.

A key principle of the Canadian legal system is that persons subject to or benefitting from a law, whether individuals or businesses, must be able to understand the law so that they can conduct themselves accordingly. The exceptions in the ECPA are sufficiently vague that many forms of otherwise acceptable commercial electronic communications are potentially made unlawful or subject to additional regulatory requirements. This vagueness means that consumers, businesses and other organizations alike may not be able to adequately determine what they need to do to lawfully conduct electronic communications in the 21st century. Certainty in the law is particularly important where, as in the case of the ECPA, a violation of the law includes the potential for significant administrative monetary penalties (AMPs), statutory damages and a private right of action (PRA).

Consistent with our view that the ECPA approaches the problem of abusive communications too broadly, we are concerned that the ECPA may not withstand a *Charter* challenge. Any regulation of speech, including commercial speech, implicates the freedom of expression rights under the *Canadian Charter of Rights and Freedoms*. Any infringement must be justified under section 1, which requires that the right be infringed as little as possible while still meeting the legislation's overall objective. The ECPA goes beyond prohibiting unsolicited commercial email messages and fraudulent messages to capture other forms of communications, some of which prohibitions may be unintended. The preferred approach would be for the statute to address explicitly those communications that are problematic with possible loopholes being addressed in additional regulations.

Parliament should reconsider its general legislative approach in the ECPA by directly targeting only that conduct that results in abusive communications rather than introduce an entirely new regulatory regime for electronic communications.

b) Overlapping and potentially inconsistent regulatory regimes

Canadian organizations that communicate electronically are already required to comply with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and more recently the National Do Not Call List (DNCL). The ECPA would add another layer of regulation leading to three overlapping and potentially inconsistent regulatory regimes that are not necessarily mutually complementary.

We identify the following two specific concerns:

i) Consent

For almost a decade, the concept of consent has been a cornerstone of private sector privacy legislation in Canada under PIPEDA and substantially similar provincial legislation. ECPA's use of the term "consent" departs from the common understanding developed over the course of nearly a decade, and proposes to treat certain commercial online activity differently and more

restrictively than other commercial activity currently subject to privacy laws. Most Canadian organizations and foreign organizations doing business in Canada have conformed their approach to electronic communications to accord with that legislation. The proposed approach under ECPA would unnecessarily require those organizations to revisit the compliance framework of their communications and likely require substantial work to adjust that framework to meet ECPA's requirements.

ii) Existing business relationship (EBR)

The definition of EBR in the ECPA is not consistent with its use in the context of the DNCL and this will likely result in confusion for businesses and consumers alike. The difference between the definitions of EBR appears arbitrary. We are not aware of any rationale that would support the adoption of different meanings of EBR in the context of electronic communications (ECPA) versus voice communications (DNCL).

While PIPEDA has regulated for almost a decade the collection, use and disclosure of personal information in the context of all commercial activity, including an EBR, ECPA now proposes to target a subset of that commercial activity, i.e. commercial electronic messages, and attach specifically defined rules for consent and withdrawl of that consent, as well as rules around the form of communication.

These are two of the CBA Section's specific concerns about the ECPA's terms that will impact existing regulatory regimes including a well-established Canadian privacy regime. We have other specific concerns, which we propose to address in our in-person presentation before the Committee.

c) Proposed Competition Act amendments

We see no justification for omitting the materiality condition from both proposed subs. 52.01(1) and (3) and proposed subs. 74.11(1) and (3). We urge, therefore, that the phrase "in a material respect" be added to the text of each of these subsections.

Furthermore, we believe that there is no demonstrated need to alter the threshold for a temporary order to be issued by a court in respect of alleged reviewable conduct contained in subs. 74.11(1). We urge, therefore, that subs. 74.11(1) not be amended as proposed.

APPROACHES TO ADDRESSING THE CONCERNS

To assist the Committee in considering how the legislation should deal appropriately with abusive electronic communications, we put forward the following options for consideration.

a) Target conduct that results in abusive communications

Rather than ban all electronic communications and rely on exceptions and regulations to allow certain specific behaviour, ECPA could explicitly prohibit certain behaviour or conduct that results in abusive electronic communications and allow for additional flexibility to target additional behaviour via regulations. In this way, the law is not always trying to play catch-up on exceptions for legitimate activities by those who use electronic means for communications purposes. It would be easier to use regulations to close loopholes for spammers and those engaged in harmful activity than to keep pace with an indefinable and potentially unlimited range

of non-objectionable and otherwise legally compliant messages that might be sent and that are already subject to Canada's broad private sector privacy regime.

b) Target computer programs that can do harm

The legislation could target only computer programs that do harm, *i.e.* target "malware" which is a general term to capture hostile software (such as viruses, worms, Trojan horses, botnets, spyware, or key loggers). These programs can typically do the following:

- modify settings or other programs, such as default browser settings
- collect personal or financial information of a computer's owner
- activate keystroke logging software to collect personal information
- prevent a user from removing a spyware program

The consent requirements in ECPA work and make sense if targeted to malware, but become potentially problematic if applied to installation of all computer programs. Many such activities are already generally covered by existing consumer protection legislation and contract law, so there is likely no need for new legislation for this aspect of the marketplace.

c) Consider ways to reduce overlapping and conflicting regulatory regimes

While it makes sense to have the Competition Bureau and the CRTC responsible for pursuing the more serious activities that result in abusive electronic communications, the Office of the Privacy Commissioner (OPC) and existing privacy legislation are well positioned to deal with everyday commercial practices. For example, the OPC has already issued two findings regarding unsolicited commercial email that resulted in organizations changing their practices as part of everyday compliance under a broad privacy framework.

We believe that consent-based requirements for commercial activity including electronic communications should continue to be subject to PIPEDA, which has proven successful in regulating the conduct of Canadian businesses when communicating with their customers or prospective customers. This approach leverages existing privacy legislation with a track record relating to legitimate commercial communications. It also recognizes that the general nature of abusive communications does not rely solely on the lack of consent but rather on other fraudulent and deceptive conduct. Following this approach, the proposed amendments to PIPEDA in section 78 of the ECPA would not be necessary. To the extent any conduct related to the collection of electronic addresses or access to a computer system to collect personal information is not already covered by PIPEDA and may result in abusive communications, it should be targeted in legislative amendments outside of PIPEDA, such as would be provided in substantive provisions under ECPA.

If the approach reflected in the ECPA is maintained, the Committee may wish to consider ways to broaden the consent provisions (for both express and implied consent). Examples of how this could be achieved include: not limiting the type or nature of the relationship when defining consent; and including consent that can be inferred from conduct and other business relationships without limiting the circumstances in which such consents can exist.

d) Exceptions

Exceptions (e.g. existing business relationship) could be more broadly worded to allow flexibility in their interpretation instead of having to rely on regulations to remedy unintended problems.

e) Remedies

If the intent behind ECPA is to have stiff penalties to target abusive communications and to serve as a deterrent to such harmful conduct, we believe the Committee should consider limiting the application of AMPs/PRA/statutory damages to only the more serious violations or conduct that do real harm to consumers, business and the marketplace generally.

CONCLUSION

We appreciate the opportunity to provide our initial comments on the ECPA and look forward to appearing before the Committee to explain these concerns and possible options.

Yours very truly,

(Original signed by Tamra L. Thomson for David Fraser)

David Fraser
Chair, National Privacy and Access to Information Law Section

(Original signed by Paul Collins)

Paul J. Collins
Chair, National Competition Law Section