MOSTERT
OPPERMAN
INCORPORATED

Attorneys
Office: 021 913 3113
Fax: **086** 673 2403
www.mostert.co.za

1st floor Chardonnay House
The Vineyards Office Estate
99 Jip de Jager rd
Tygervalley, Cape Town

Suite 157
Private Bag X7
Tygervalley 7536
VAT Reg. No. 401 021 5301

7 October 2009

Mr V Ramaano

Portfolio Committee on Justice and Constitutional Development

vramaano@parliament.gov.za

Dear Mr Ramaano

SUBMISSION ON THE PROTECTION OF PERSONAL INFORMATION BILL ("PPI BILL")

1 INTRODUCTION

We submit these comments on behalf of our firm and, where indicated, on behalf of certain SABS committees.

Kindly afford us the opportunity to make oral submissions.

2 COMMON LAW

2.1 The submissions in this paragraph are made on behalf of our firm.

2.2 Will the common law on privacy still apply to the protection of personal information in conjunction with this Bill?

2.3 If so:

2.3.1 will an aggrieved party have two causes of action: one in common law and the other under this statute?

2.3.2 must the courts develop the common law to give effect to the provisions of the Bill? If so, should this be expressly provided for in this Bill?

2.4 If not, should the common law be excluded? If so, this must be expressly provided for in this Bill.

3 JURISTIC ENTITIES

3.1 The submissions in this paragraph are made on behalf of our firm.

3.2 We believe the issue of whether the PPI Bill should apply to juristic entities will be well traversed during the public comment phase. We do not necessarily object to the application of the Bill to juristic entities. What this part of our submission

wishes to achieve is to suggest a compromise between those in favour vs those opposed to their inclusion.

3.3 It is suggested that a mechanism be provided for whereby the Bill initially applies to natural persons.

3.4 The Minister must then be entitled to specify by notice in the Gazette whether certain or all parts of the Bill afford protection to personal information of juristic entities or juristic entities with an annual turnover of less than a certain amount. Such a notice may take effect on the date of proclamation or another date as stipulated in the Minister's notice.

3.5 It must be remembered that juristic entities still have the common law to rely on in respect of protection of personal information.

4 RECOGNITION FOR PRO-ACTIVE RETENTION OF RECORDS FOR EVIDENTIARY PURPOSES (CLAUSE 14)

4.1 The submissions in this paragraph are made on behalf of our firm.

4.2 We believe that this subclause does not provide adequately for the normal, pro-active retention of records for evidentiary purposes by responsible parties where such evidentiary matter may include personal information.

4.3 It is reasonable to assume that the exceptions stipulated in paragraphs (a) to (d) will be interpreted restrictively.

4.4 The use of the terms "by law" in paragraph (a) would, in terms of the Interpretation Act, refer to formal statutory legal instruments such as "any law, proclamation, ordinance, Act of Parliament or other enactment having the force of law".

4.5 In this regard it cannot be said that records collected pro-actively for their evidentiary value would as per paragraph (b) be required for lawful purposes related to the "functions and activities" of a responsible party. In our view the functions and activities of a responsible party would relate to the furthering of its business or official functions and activities and would not go as far as including the pro-active collection and preservation of evidentiary records.

4.6 Paragraphs (c) and (d) would also not in our view make sufficient provision for the legitimate, pro-active collection of records for future evidentiary purposes.

4.7 In this regard we would suggest that paragraph 14(1)(b) be broadened to read as follows:

> (b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities or <u>for the protection of its legal rights</u>;

5 DESTRUCTION OR DELETION OF RECORDS (CLAUSE 14)

5.1 The submissions in this paragraph are made on behalf of our firm.

5.2 In properly structured, best-practice based information or records systems massive amounts of data are often backed up at various intervals. It is not uncommon for large organisations to have daily, weekly, monthly and annual back-ups of all the data in their operational systems. Because of the voluminous nature of such back-ups they are often done on unstructured sequential media (e.g. magnetic tapes) which are not search- or edit-friendly. They are used for

disaster recovery purposes to restore systems following catastrophic events and would not be seen as normal record repositories. While one may be able to readily delete or destroy the personal records of an individual stored in the structured operational records systems of a responsible party the same cannot be said for such expungement from backup media. This may lead to scenarios where organisations may properly comply with subclauses 14(4) and (5) as far as personal data in their operational systems are concerned while they may inadvertently infringe such requirements because of the existence of the same information in their backup environments. This problem is not unique to South Africa but these subclauses represent the first mandatory destruction provisions of its kind in South Africa, which is the reason why this issue was not prevalent before.

5.3 In this regard we would suggest that the retention of information for purposes of disaster recovery in backup systems be excluded from the working of subclauses 14(4) and (5). This would of course be subject to such further requirements regarding the necessary safeguarding of such backup data in line with the provisions of clause 18 of the Bill.

6 STATUS OF GENERALLY ACCEPTED PRACTICES IN REGARD TO INFORMATION SECURITY (CLAUSE 18)

6.1 The submissions in this paragraph are made on behalf of our firm.

6.2 While subclause 18(3) seems to place a regulatory burden on responsible parties to have due regard to generally accepted practices in relation to information security, which is commendable, the words “which may apply to it generally” is in our view problematic. It is not entirely clear whether the requirement to have due regard to such practices would stem from:

6.2.1 the mere fact that such practices are generally accepted for the sector or type of organisation; or

6.2.2 whether some other mandatory connection to such practices is required (i.e. they are required by a law to be followed).

6.3 An example would be where SABS standards which deal with issues of information security would in general be applicable and indeed useful to many organisations such applicability would not under normal circumstances be a mandatory requirement.

6.4 Dictionary.com, among others, defines this verb as “to be pertinent, suitable, or relevant” to a matter.

6.5 We suggest that it should be made clear whether subclause 18(3) requires organisations to have due regard to generally accepted information security practices only where they are made mandatory by some other decree, rule or regulation. If the intention is to limit the application of this subclause to scenarios where there is such mandatory requirement, we would argue that the whole of subclause 18(3) is superfluous as such other decree, rule or regulation would then in any event make the application of the generally accepted practices mandatory. If the idea is to forthwith establish a higher level of diligence in regard to

information security in responsible parties it would be helpful if this is made clear in the wording of the subsection.

7 RECORDS MANAGEMENT AND THE PRESERVATION OF THE INTEGRITY OF INFORMATION (CLAUSE 18)

7.1 The submissions in this paragraph are made on behalf of the South African Bureau of Standards (SABS) Technical and Subcommittees *TC171 (Document Management Applications)* and *TC46 (Information and Documentation)- Subcommittee 46D (Archives and Records Management)*.

7.2 We would argue that similar recognition to that afforded to generally accepted standards in regard to information security (see the discussion on subsection 18(3) above) should be given to generally accepted standards in regard to records management. The standards in this field, among others, provide guidance on the preservation of the integrity of records over time and should therefore be extremely relevant not just for clause 14 of the Bill when dealing with the preservation, management and destruction of records but also in order to satisfy the requirements for the preservation of the integrity of personal information set by subclauses 18(1) and (2) of the Bill.

7.3 Examples of useful standards in this field are SANS 15489 and SANS 15801 prepared by SABS Technical Committee 46 Subcommittee 46D and SABS Technical Committee 171 respectively.

8 ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT ("ECT Act")

8.1 The submissions in this paragraph are made on behalf of our firm.

8.2 The removal of s 50 and 51 of the ECT Act is welcomed.

8.3 The amendment of the definition of personal information in the ECT Act is unnecessary and should be removed. Once s 50 and 51 are removed, the definition only occurs in s 43(1)(p), which in our view does not justify a separate definition:

> ***43. Information to be provided***
> (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered:
> …
> (p) the security procedures and privacy policy of that supplier in respect of payment, payment information and <u>personal information</u>;

8.4 If the definition is retained it will have to be amended each time the definition in the PPI Act is amended. Should it be decided to retain the definition (which we submit is unnecessary), it should merely refer to the definition as per the PPI Bill.

8.5 Likewise, the definitions of "data subject" and "data controller" in s 1 of the ECT Act should also be removed as they only appear in s 50 and 51, which are to be removed.

9 UNSOLICITED ELECTRONIC COMMUNICATIONS (CLAUSE 66)

9.1 The submissions in this paragraph are made on behalf of our firm.

9.2 The removal of s 45 of the ECT Act is welcomed.

9.3 The provisions of clause 66 of the PPI Bill appear to overlap with Chapter 4 Part C of the National Credit Act ("NCA") and Chapter 2 Part B of the Consumer Protection Act ("CPA").

9.4 While overlap with the NCA seems unavoidable, as the latter is now entrenched, it is prudent to ensure there is not overlap between the PPI Bill and the CPA.

9.5 While the PPI Bill is restricted to electronic communications, the CPA is technology neutral and deals with any form of unsolicited communications. The CPA is *prima facie* the more appropriate statutory instrument to regulate unsolicited electronic communications.

9.6 If, however, clause 66 of the PPI Bill is removed, large corporate entities may be prejudiced as they would not qualify for protection under the CPA (the CPA would not apply to juristic entities with an annual turnover above an amount to be prescribed).

9.7 To bridge this impasse, one of the following options may be considered: [1]

9.7.1 amending the CPA by means of an addendum to the PPI Bill to afford the Chapter 2 Part B protection to all juristic entities, irrespective of the turnover threshold; or

9.7.2 the threshold notice to be issued by the minister under the CPA may exclude the provisions of Chapter 2 Part B of the CPA from the threshold.

10 AUTOMATED DECISION MAKING (CLAUSE 68)

10.1 The submissions in this paragraph are made on behalf of our firm.

10.2 The PPI Bill should remain true to its objective to protect personal information and one should take care not to use the Bill as a vehicle to extend into the realm of consumer protection, however laudable the protection.

10.3 We submit that the processing of personal information for the purpose of making a decision is a matter of commerce, contract and trade and not *per se* a matter of protection of personal information.

10.4 In our view the subject matter dealt with in clause 68 is not a matter to be dealt with under the PPI Bill but rather under the CPA, if at all.

10.5 Accordingly, we lobby for the removal of clause 68 in its entirety.

Yours faithfully

Wim Mostert

[Transmitted electronically and deemed signed]

[1] The State Law Advisor must advise whether this is legally competent to do so.