FLOOR INC
ATTORNEYS
Financial Services & ICT Law

Legal opinion on the parental consent requirement in section 25 of the Protection of Personal Information Bill

For

MXit Lifestyle (Pty) Ltd

19 September 2011

Stellenbosch

1 Introduction

1.1 This opinion has been compiled on behalf of MXit Lifestyle (Pty) Ltd in reaction to the amendments to section 25 in version 4 of the Protection of Personal Information Bill ("PPI Bill") and supplements our previous opinion on this matter dated 21 June 2010.

1.2 The essence of the proposed amendment of section 25 is that information about children remains classified as sensitive personal information, but instead of determining whether the child is subject to parental control (in general), the question in terms of the amended section 25 is whether a child is legally competent to act without the assistance of a competent person (in specific circumstances).

1.3 If the amendment stays and is adopted as such on our statute books, the question that responsible parties will face is not whether consent is required to process a child's information under the Protection of Personal Information Bill but rather whether that specific child can, in that specific instance and for that specific purpose act independent from his/her parents or guardian. The answer will always be found in another body of law, not in the Protection of Personal Information Bill.

1.4 MXit has often expressed their commitment to protect the best interests of children, who constitute a large portion of its user base, and will actively support measures aimed at improving the protection of children's interests. The following initiatives illustrate MXit's commitment to children's education: MXit offers a number of educational products and services on its platform specifically aimed at children, some of which are even endorsed by the Department of Education and includes a program to support the secondary school mathematics curriculum, the Drive Max initiative assists learner drivers in studying for their driving licence exams and MXit offers various counselling and health related services aimed at empowering and educating children who may not have easy access to health care services. Should MXit decide as a result of the provisions of section 25, as it currently reads, to decline new registrations by children then such children will be denied access to what is for them a valuable source of information.

1.5 MXit is also concerned that the requirement to obtain prior parental consent in its industry (as will be the case in related industries such as internet based service providers) will be difficult, if not impossible, to implement in practice. New users sign up for MXit using their cellular telephones and never visit a branch or meet any MXit representative on a face to face basis. The signing up process is fully automated and

requires no human intervention or any processing by hand. To obtain the parents' consent MXit would have to introduce special measures to record the parents' consent, which would include a special channel to record parental consent and human intervention to verify that the consenting parent is indeed the parent of the child in question. With between 40 000 and 50 000 new users joining MXit daily this will take substantial effort to implement correctly.

1.6 MXit further submits that prior consent is not recognised internationally as the one and only, or most effective, measure to manage the risks to which children are exposed when their personal information is processed. MXit feels there are more efficient measures available to improve the protection of children's personal information.

1.7 In this opinion we investigate whether: a) information about children is treated as sensitive personal information in other jurisdictions and international legal instruments dealing with data protection; b) the requirement for prior parental consent is widely adopted in other jurisdictions; and c) if there are any other measures, other than prior parental consent, to improve the protection of a child's personal information.

2 **Background**

2.1 The PPI Bill is currently under consideration by the *ad hoc* technical committee of the Portfolio Committee for Justice and Constitutional Affairs. The *ad hoc* technical committee has made amendments to the PPI Bill and the version under consideration is version 4 of 24 February 2011.

2.2 The intention of the *ad hoc* technical committee regarding the protection of children's information is, as I understand it, not to add any provisions to the PPI Bill that constitutes an outright prohibition on the processing of information about minors but to make sure that people can only process information about minors if it is lawful for them to engage with a specific child in terms of any other law. We respectfully submit at this stage that linking these two issues will not contribute to improving the protection of information of children. We will return to this issue later in the opinion.

2.3 The initial wording of section 25(a) of the PPI Bill reads

> "*a responsible person may not process personal information concerning a child who is subject to parental control in terms of the law*" (My paraphrasing)

and the wording of section 32(a) reads

> "*the prohibition on processing personal information, as referred to in section 25 does not apply if […] processing is carried out with prior parental consent where the data subject is a child and subject to parental control in terms of the law*" (My paraphrasing).

2.4 Under the revised wording as contained in the *ad hoc* technical committee's working draft 4 of 24 February 2011 section 25(1)(a) now reads

> "*a responsible party may, subject to section 25A, not process personal information concerning a child in those circumstances where that child is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning the child*" (My paraphrasing)

and the wording of section 25A reads

> "*the prohibition on processing personal information, as referred to in section 25, does not apply (a) if the processing is carried out with (i) prior consent of a competent person in respect of a child referred to in section 25(1)(a)*" (My paraphrasing)

2.5 Under the initial wording one had to ask whether a child is under parental control. The manner in which this was phrased meant you had to ask if a child is objectively, in other words generally, under parental control. If a child was not emancipated, you had to obtain prior parental consent for every instance in which someone may want to process the child's information. This wording did not take the specific circumstances of each and every processing relationship into consideration.

2.6 In terms of the new wording one must ask whether the child is *legally competent* to act in the particular circumstances and if the answer is positive then the responsible party may collect the information without first getting parental consent. If the child is not legally competent to act the consent of the parents are required.

2.7 The difficult question is now to determine whether the child is legally competent to enter into a use agreement with MXit. In paragraph 3 we will delve deeper into the question when a child can contract with MXit or not. If the answer is that the child may indeed contract with MXit, or with a bank for that matter, then such child will not enjoy any additional protection by the PPI Bill as it stands.

3 **Capacity to Contract**

3.1 It is not always clear under the South African law when a child is competent to act independent from parental guidance. While there are specific provisions in banking law for example, it is less clear in the context of concluding binding agreements when a child can act without the guidance of a parent. We therefore believe that by inserting a provision that prior parental consent is required for situations where a child requires parental guidance, the legislator forces responsible parties to investigate other areas of law to determine whether parental consent is required for purposes of the PPI Bill. We feel this is an unnecessary complication and urge the *ad hoc* committee to consider amending the Bill to the affect that it is clear from the wording of the Bill itself or its regulations, whether consent will be required.

3.2 The capacity of a child to conclude a binding agreement is set out by our common law. In Edelstein v Edelstein 1952 3 SA 1 (A) our courts stated that “a minor is considered immature throughout his minority and he is consequently not bound by his contracts”. According to the Edelstein case one should not label the contract with an unassisted minor as voided or voidable and the court rather states that the contract “limps”. A parent can later ratify the agreement.

3.3 There are exceptions to the common law rule, which include the Friendly Societies Act 25 of 1956 which allows a person who are 16 years or older to become a member, the Banks Act 94 of 1990 which allows a person who are 16 or older to enter into an agreement with a bank to make deposits as well as the Post Office Act 44 of 1958 which allows a person of 7 years or older to open an account with the Post Office and to make deposits and drawings from the account. None of these exceptions apply to MXit.

4 **Sensitive Information**

4.1 Information about children is not *per se* sensitive. Sensitive information is classified as such because of the intrinsic nature of the information itself and not the nature of the data subject. In other words, information is sensitive because it is information about the health status or race of a data subject. It should not be sensitive because the attributes of a data subject, like being under age.

4.2 A child also could have sensitive and non-sensitive information and the law must allow for it to be treated as such. It is therefore our opinion that it will be a conceptual error to treat all personal information relating to a child as sensitive information. This statement is supported by the survey below of the position in other jurisdictions and international instruments.

4.3 By classifying information about children as sensitive information, we will limit the processing of information about children only to instances where the guardian has given consent or where the guardian's consent is not required. If the guardian refuses consent, then no data processor, not even a government body, may process personal information about such a child.

4.4 We are further of the view that the current wording of section 25 *vis a* vis children does not contribute to the protection of children's information to the same extent as the measures listed in paragraph 13 can improve the protection.

5 **Consent**

5.1 The general position in the PPI Bill is that consent is not always required to process personal information. Section 10 of the PPI Bill provides that other grounds are perfectly acceptable to justify processing and such grounds should also be available to children. These grounds are sometimes referred to as gateways.

5.2 All instances where children require parental assistance are not equal in so far as the exposure of the child's privacy is concerned - in other words in certain situations a child may conclude a contract without parental consent but there could be a high level of risk for abuse of her personal information.

5.3 In other situations parental consent may be required but the risk from a privacy perspective may be very low. Or a child may be capable to fully understand the implications of the processing of his personal information.

5.4 When a child agrees to enter into a relationship where her information is processed, she enters into a continuous relationship with the data processor. A relationship that will last long after the parent has given prior consent. The fact that a parent has given consent does not in any way contribute to improving data processing practises.

5.5 To obtain prior parental consent before they can process information about children, poses challenges to responsible parties: the consent needs to be in a format that it can be recorded for evidentiary use when challenged at a later stage and it must be verifiable that it has been indeed the parent (or guardian) of that child who given the consent.

5.6 A further question is how to deal situations where guardians fail to act in the best interest of a child? A parent may consent but the child might not want his personal information shared with a retailer selling children's clothing.

5.7 Another aspect is that the capacity of a child to enter into a contract and the capacity to give consent to have information processed are not always linked and in our mind it serves little purpose to link the two.

5.8 Thus we recommend de-linking the capacity of the child to conclude agreements, which is regulated by the law of contract, from the capacity of a child to give consent to have his or her personal information processed. The measures protecting children from abuse of their personal information must stand alone and separate from the law that regulates other spheres of their lives.

6 **European Union**

6.1 As far as sensitive personal information in the European Union is concerned, Article 8 of the EU Data Protection Directive prohibits the processing of information about a data subject's race, political opinions, religion, trade union membership and/or health or sex life unless the data subject has given explicit consent. Article 8 does however list other gateways, other than explicit consent, to process sensitive personal information and these gateways include where the processing is necessary in the field of employment law, to protect the vital interest of the data subject, or where a NGO processes such information in the course of legitimate activities and with appropriate guarantees or where the data subject has made his special categories of data public. The EU Data Protection directive does not include information about children as a special category of data and contains no provisions requiring the consent of a child's guardian before

information about a child can be processed. The European Data Protection Directive makes no mention of minors or children, and makes no specific provision for processing information relating to children.

6.2 The European Commission and the Article 29 Working Party, which deals with policy issues surrounding privacy and data protection, have undertaken a number of studies to explore the protection of information relating to children and have made a number of recommendations to improve the protection of children's information. Three of these studies are discussed below.

6.3 The Article 29 Working Party issued Opinion 5 of 2009 on Privacy in Online Social Networking. Paragraph 3.4 of that opinion deals with sensitive data and lists the same type of information as being sensitive as listed in the EU data protection directive. Information relating to children is not treated as sensitive.

6.4 Paragraph 4 of Opinion 5 of 2009 deals with information relating to children and recommends a multi-pronged approach to protect children's information in social networks:

6.4.1 The social networks should raise awareness of privacy issues regarding children;

6.4.2 Encourage fair and lawful processing by not collecting sensitive personal information (see above for a list of sensitive personal information) relating to children, no direct marketing aimed at children, obtaining the prior written consent of parents before a child subscribes for this service and separating communities of children and adults;

6.4.3 Adopting privacy enhancing technologies, including privacy friendly default settings for children, pop up warning boxes and age verification software;

6.4.4 Encouraging industry self-regulation; and

6.4.5 Introducing laws to prevent certain unfair or deceptive practices that could occur in a social networking context.

6.5 The Article 29 Working Party also adopted Working Document 1 of 2008 on the Protection of Children's Personal Data (18 February 2008). In terms of this Working Document a number of principles are set out to guide the protection of children's rights to privacy.

6.6 Paragraph 6 of Working Document 1 of 2008 suggests that the consent requirement should depend on the maturity of the child. In the event of a less mature child, the parallel consent of both the child and the parent should be required while a more mature child should be able to give sole consent without a parent's assistance.

6.7 The Working Document 1 of 2008 also suggests in paragraph B(2)(a) that certain of the data protection principles need to be more strictly interpreted where the information of a child is concerned.

6.8 On pages 8 and 9 of Working Document 1 of 2008 the requirements for making the processing of information relating to a minor legitimate (with reference to article 7 of the EU data protection directive) are outlined and the document discusses how each requirement, including obtaining consent, should be interpreted when handling a child's information. But the Working Party does not put forward a suggestion that special permission by parents prior to the processing should be a legal requirement and also does not suggest that a child's information should be treated in the same manner as special or sensitive information.

6.9 When a parent has given consent to a data processor to process information about a child, such consent should again be obtained from the child once he or she reaches majority.

6.10 In another study, the same Article 29 Working Party raises the question on page 9 of its Opinion 2 of 2009 on the protection of children's personal data:

> "[…]*where the children who can in certain cases conclude legal acts without the consent of their legal representatives (in instances where they enjoy their partial rights), can also give valid consent to the processing of their data".*

6.11 The Article 29 Working Party suggests as a possible solution to protect the processing of children's information that data controllers must be permitted to collect personal information on the condition that parents do not object at a later stage (page 9 of Opinion 2 of 2009).

6.12 The Article 29 Working Party further recommends in Opinion 2 of 2009 that the EU Data Protection Directive of 1995 (1995/46/EC) is interpreted bearing in mind the principle of the child's best interest. Thus their recommendation is not to amend the directive but rather to interpret the law to serve the best interest of children.

7 **International Working Group and Data Protection in Telecommunications'**

7.1 The International Working Group on Data Protection in Telecommunications ("IWGDPT") also considered the issue of parental consent in its Working Paper "*Children's Privacy Online: The Role of Parental Consent*" dated 26/27 March 2002.

7.2 The Working Paper includes a brief discussion of the role that parental consent plays in protecting children's information in an online environment and concludes by recommending, *inter alia*:

7.2.1 Prior parental consent is only required for children under the age of 13;

7.2.2 Information collected about children may only be disclosed to third parties or made public if the parents have given written and verifiable consent;

7.2.3 Data processors should not collect information about other persons from children;

7.2.4 Children should not be enticed to divulge personal information with the prospect of a game or a winning a prize;

7.2.5 Reliance on parental consent should be limited.

8 **United Kingdom**

8.1 The UK Data Protection Act of 1998 does not include information about children in the definition of "sensitive personal data". Information included in the definition of sensitive personal includes information about race, political opinions, religion, trade union membership, physical or mental health, sexual life, or information about offenses committed by the data subject.

8.2 Since information about children is not treated as sensitive personal data in the UK the data controller may justify the processing of information about children on any of the gateways listed in the Schedule 2 of the UK Data Protection Act, which includes consent received from the data subject or any of the following:

a) The processing is necessary to perform a contract;
b) The processing is necessary to comply with legal obligation;
c) The processing is necessary to protect the interest of the data subject;
d) Or the processing is necessary to perform a public function.

8.3 The Information Commissioner's office of the UK released an Issues Paper "Protecting children's personal information" dated 22 November 2006. The Issues Paper is aimed at investigating the processing of information about children and whether current practices in the UK are adequate to protect the interest of children.

8.4 In the Issues Paper the Commissioner recognizes that Data Protection Laws, both in the United Kingdom and on a European level, do not draw any explicit distinction between data subjects that are adults and those who are children. This implies that children should, like adults, be able to exercise their rights in terms of the Data Protection Act, independently from their parents.

8.5 On page 7 of the Issues Paper the Commissioner states that consent may not always be the only way to ensure fair and lawful processing of information about children. The Commissioner continues by stating that it might in certain instances be safer for responsible persons to rely on another basis for processing, instead of consent, and further states that it is not the intention of the UK Data Protection Act to deprive children from protection where parents unreasonably refuse their consent.

8.6 The Issues Paper concludes by stating that the issue of consent is of such importance that the Commissioner will issue guidance notes to data processes on the need, or not to obtain consent from parents to process information about children. We were not able to source the guidance notes and believe it is still being drafted.

8.7 The Information Commissioners Office issued the "Personal Information Online: Code of Practice" dated July 2010. On page 15 of this Code the Information Commissioner acknowledges that it is difficult to determine whether consent should be obtained from children. In UK law there is not a simple definition of a child based on age. The Commissioner also remarked that children have different levels of maturity and understanding, and resourceful children could easily circumvent many mechanisms that are put in place for obtaining parental consent. The Code states that parental consent would normally be required before collecting personal data from children under the age of 12. The report continues by stating that parental consent may only be appropriate for children over 12 if there is a greater risk present.

8.8 The Issue Paper refers to the FIPR Report on Protecting Children's Information (2006). The FIPR Report discusses on pages 87 onwards the evaluation of consent given by children. On page 89 the Information Commissioner is quoted as saying that data

subjects who have reached sufficient maturity to understand their rights under the Data Protection Act should be approached to process their personal information. The Information Commissioner is quoted as stating that he believes children of 12 years and older have the maturity to understand their rights in terms of the Data Protection Act and are capable of giving informed consent.

9 **Netherlands**

9.1 Article 5 of the Dutch Data Protection Act ("*Wet van 6 Julie 2000, inzake bescherming van persoons gegevens*") provides that where permission is required in terms of the Act, such permission must be obtained from the guardians of children younger than 16 years. In other words, the consent of parents is only required where the data processor relies on consent as a gateway to justify the processing of personal information. It is not an absolute requirement for processing information about children and the data controller can rely on any of the other gateways.

9.2 Article 16 of the Dutch Data Protection Act regulates special personal information and, as is the case of the EU Data Protection Directive and the UK Data Protection Act, only treats information about religion, race, political affiliation, health and sexual orientation as special information. It does not treat information about children as a separate category of special information.

10 **United States of America**

10.1 The Children's Online Privacy Protection Act of 1998 ("COPPA") provides that websites that collect personal information about children under the age of 13 need to obtain parental consent before collecting such information. There is a lobby to increase this age limit to 18 years but as far as we could establish an amendment to that effect has not been implemented. COPPA further requires such websites to post a privacy policy outlining the way it processes information about children.

10.2 COPPA grants the right to parents to have access to their children's information and grant a right to opt out our future collection in use of personal information about their children.

10.3 COPPA prohibits websites to require a child to disclose more personal information that would reasonably be necessary to participate in any online game competition or other child orientated activity.

10.4 The United States adopts a sector specific approach, in other words there are different laws dealing with the protection of personal information in the financial services- and health industries. Because of this sectoral approach, the concept of sensitive personal information is not used in the United States.

11 **India**

11.1 India adopted the Privacy Rules on 11 April 2011 to implement the parts of the Information Technology (amendment) Act of 2008 dealing with protecting the privacy of personal information.

11.2 According to article 3 of the Privacy Rules sensitive personal information includes passwords, financial information, physical physiological and mental health information, sexual orientation, medical records and bio-metric information. Article 5 of the Privacy Rules requires prior written consent, either by letter, fax or email, giving consent for using the sensitive personal information for the stated purpose.

11.3 The Privacy Rules do not include information about children in the definition of sensitive personal information and does not contain any special provisions on dealing with children's information.

12 **Australia**

12.1 Australian Privacy Act 1988 does not specifically deal with children's information and information about children is not treated as sensitive personal information.

12.2 The Australian Privacy Act of 1988 defines in article 8 sensitive personal information as:

"(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information."

12.3 The Australian Law Review has recently conducted a review of the Australian privacy laws and this review also considered the processing of information relating to children.

12.4 Chapter 6 of the Office of the Privacy Commissioner's submission to the Australian Law Review Commission Review of Privacy Laws deals with consent by minors to process their information. The submission recommends that children of 15 and older should be deemed capable of giving permission for the processing of their own information. Children of 14 and younger should be assessed to determine whether they are capable of, amongst others, giving consent under the Privacy Act. If doing an assessment is not practical, then the consent by the child's parent should be obtained. This proposal, as far as we could determine, has not yet been implemented.

13 **Conclusion**

13.1 In each of the jurisdictions and instruments surveyed, the special categories of data treated as sensitive is treated as such because of the nature of the information and not because of the nature of the data subject. Sensitive personal information relates to different spheres of society where extra protection is required and not to members of society who are weak and require extra protection.

13.2 None of the jurisdictions or international instruments discussed in this opinion treats personal information relating to children as sensitive personal information. Our draft Protection of Personal Information Bill generally follows international precedent and would be out of kilter with such international precedent if we proceed to treat information of children as sensitive personal information.

13.3 None of the jurisdictions surveyed require parental consent for children between the ages of 13 and 18.

13.4 Only COPPA in the United States requires parental consent for children below 13. The Australian data protection regulator has made a recommendation that consent should be required for processing information about children younger than 15 but as far as we could establish this has not been implemented.

13.5 We are of the opinion, based on the various reports, guidance notes and other policy documents discussed in this report, that requiring consent on its own is not a sufficient instrument to improve the protection of personal information of children.

13.6 We therefore call on the Technical Committee to remove the information relating to children from the provisions in version 4 of the PPI Bill dealing with sensitive personal information and to consider any of the alternative measures listed below to bolster the protection of information about children.

13.7 Various measures to improve the protection of children's personal information are either in place in the countries discussed in this report, or are either considered or proposed. These measures can be adopted, either by Parliament or by the Information Protection Regulator to improve information protection for children and include:

a) Processing of information about children is permitted on the condition that parents may object at a later stage;
b) Responsible parties must implement special security measures when processing information about children;
c) Responsible parties must notify children on how their data will be used and such notices should be simple and easy for the child to understand. The provision should regulate the place and the time for such notices;
d) Restrict the collection of sensitive information (as per international best practice) about children;
e) Responsible parties must be obliged to raise awareness of privacy issues that may confront the children whose information they process;
f) Promote the adoption of privacy enhancing technologies;
g) Prohibit deceptive practices that may induce children to share their personal information;
h) Children must be allowed in certain instances to exercise their rights on their own, without their assistance or hindrance of their guardian;
i) Parental consent is required before information about children is shared with third parties or made public.

13.8 By adopting the approach suggested above, the uncertainty as to whether a particular child is legally competent or not (a child being any person below the age of 18 years) would be avoided and the information of children would be better protected without

placing an unnecessary and practically unattainable administrative burden on businesses to ensure that they have obtained verifiable prior parental consent in respect of all children they contract with and whose information they accordingly need to process to some degree in order to fulfil the contractual relationship. No business can practically conduct an individual assessment of each child it wishes to contract with - without even having any guarantee that a court would agree with such an assessment. It is not commercially feasible and we therefore request that the Technical Committee consider the aforementioned alternatives and amend the PPI Bill accordingly.

Opinion compiled by:

Jos Floor
Floor Inc Attorneys
021 880 1714 / 082 856 2233
jos.floor@floor-inc.co.za
19 September 2011