August 15, 2011

By Electronic Filing

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Aristotle Application for safe harbor, Project No. P-114509

Dear Secretary Clark:

As an FTC approved safe harbor under the Children's Online Privacy Protection Act (COPPA) Privo appreciates the opportunity to provide brief comments to the FTC as it undertakes a review of the Aristotle application to become a safe harbor.

The process of applying for safe harbor allows for each new applicant to leverage the previous applications submitted to the FTC. What the application does not do is provide an easy way to evaluate the applying organizations intent, skill set or demonstrated ability to administer a children's privacy protection and certification program. The applicants opening paragraph states that Aristotle "offers companies an integrated privacy program that is dedicated to the protection of personal information from children online." However, there is no such integrated privacy program in the market place that can be readily evaluated. The company states that the Integrity division established in 1999 in part to "enable companies to create rewarding relationships with children online while meeting the expectations and concerns of parents and governmental regulators". That would imply that Aristotle has been in the business of providing for parental consent to enable companies to comply. However, there is no such service currently available by Aristotle. The company states that it is a leader in age and identity verification and that it intends to build on its "knowledge of COPPA". However, since the inception of the Integrity division in 1999 there is no evidence that Aristotle has made any attempt to take place in the ongoing dialogue surrounding COPPA over the last ten years. The elephant in the room is that Aristotle is a twenty+ year old data aggregator. The value of the company is derived by the amount of data that they can amass and then provide others access to. The company states it has the ability to verify parents data against its "own extensive databases without the need to send data out to third parties for verification." Assuming that is true then how will they possibly separate the new parent data and the related child accounts and their activities from the extensive data base that is the company's current bread and butter? As an example, Aristotle's home page at www.aristotle.com clearly shows that they can "provide high quality voter data for political organizations, campaigns and government agencies". If approved as a safe harbor the data base of Aristotle will have even richer data. Based on the description of the Integrity System this data aggregator will have new personally identifiable information about parents and their children. The individual consumer data that currently lives within the extensive database is not under the end consumer's control. Control is a foundation concept under COPPA. A parent may not realize that their political leanings are now going to be combined with their children's' data. How will the FTC assure the public that the parent profile

collected by Integrity System is not going to be combined with other extensive information owned by Aristotle's marketing division?

There are a few areas of real concern:

1) Throughout the application there is an inconsistency as it relates to access of information. In some areas the parent is given the right to "update the child's information". The requirement if for the parent to have access to review the information collected and to be able to refuse to permit further collection or use. Providing a parent with the right to "update the child's information" could pose a serious problem in that the information provided by the child may indeed be a work of art or expression of a child's opinion for example. It should not be encouraged to have parent's under COPPA be given the ability to alter such information. If they do not approve then they can ask to have it removed but not edited at will.

2) The discussion around exceptions to verifiable parental consent includes a section called "Required Parental Consent". It is not at all clear what the applicant is trying to say. It does not seem to call out the collection of the parents online contact information so it is not clear how this process is supposed to work or what the consent relates to. It states that if the consent is not received in a reasonable time that the information must be deleted. However, it does not state how long is reasonable nor does it discuss how the consent would be provided. If this is an attempt to allow for email+ then it is clear the applicant does not understand how and when it would be applied, that the information collected can ONLY be certain data and that confirmation of the consent would need to take place.

3) The application calls out 14 methods that would qualify for verifiable parental consent. It is clear that email+, as it is currently understood by industry, is not an acceptable method under this proposed program. That is the prerogative of the safe harbor as the guidelines are intended to be as good as or better than the Rule requires. However, it is also evident that the concept of the sliding scale for internal use versus public disclosure and sharing has been flattened and therefore, it appears as if the 14 methods that are listed are all intended to provide a level of verifiable parental consent that would be required "under most situations"… "with few exceptions". The applicant specifically calls out social networks as a group that will benefit from the integrated solution offered by Aristotle. However, at least two of the methods that would allow for a print form to be signed and then emailed or electronically uploaded would not provide for a level of consent that is as good as mail or fax. The FTC has given industry guidance that a print form cannot be signed then emailed or scanned in. In another method the system would allow for a parent (or child) to photo copy the parent government ID or driver's license to then email in to be stored by a 3rd party. This is not privacy enhancing. At least verification data can be deleted and or 1-way hashed/encrypted to protect it. The most alarming method is that it is the intent of this program to allow for a name, address and date of birth alone to be qualify as verifiable parental consent. The applicant references the placement of tobacco orders online coupled with this low level of person verification. In order to place a tobacco order online I assume that a financial transaction is taking place and the person verification is a supplemental verification. This method would not meet the standards that have been set under COPPA. Most children will certainly know their parents basic details.

4) The Integrity System as described in the application would allow for a child to provide personal information in advance of parental consent by forcing a *parent with me* path described in the application as "upon entering information that indicates the child is under 13, the child is directed to contact a parent" at which point the "parent begins the verification process". This mistake was made clear in the Hershey settlement. COPPA is very strict about how an organization must go about obtaining parental consent and in what order data can be collected from a child. It is unreasonable to think that a child will not attempt to enter the parent data themselves especially when they never have to leave the browser session that they initiated registration in.

The current safe harbors have worked very hard to educate the market place about how and why to comply with COPPA. They have all been in the trenches for six to 10 years working on the very complex issues that surround marketing to kid's and the privacy protections that need to be in place. To approve another provider, especially one that comes from the data aggregation industry and is just arriving on the scene as a privacy expert, would have the potential to further confuse the market place about what and how to comply with COPPA.

Thank you for your consideration.

Regards,

Denise Tayloe | CEO | **Privo**
office: 703-932-4979
dtayloe@privo.com