Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	**)**	
	)	
iKeepSafe Application for Safe Harbor	**)**	P-145402

COMMENTS OF CENTER FOR DIGITAL DEMOCRACY

INTRODUCTION

The Center for Digital Democracy (CDD) respectfully submits these comments in response the Federal Trade Commission's (FTC) *Children's Online Privacy Protection Rule Safe Harbor Proposed Self-Regulatory Guidelines; iKeepSafe COPPA Safe Harbor Program Application*.[1] CDD is a national nonprofit, nonpartisan organization dedicated to promoting responsible use of new digital communications technologies, especially on behalf of children and their families. CDD has a strong interest in ensuring that the FTC only approves self-regulatory guidelines that fully comply with the agency's rules and with the underlying purpose of the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule.

ANALYSIS

In this submission, CDD responds to questions two and six posed by the Commission in the *Safe Harbor Notice*.[2] However, we begin with question six because it raises our most significant concerns.

[1] 79 Fed. Reg. 15271 (Mar. 19, 2014).
[2] *Id.* at 15272

Question 6: Does iKeepSafe have the capability to run an effective safe harbor program? Specifically, can iKeepSafe effectively conduct initial and continuing assessments of operators' fitness for membership in its program in light of its business model and technological capabilities and mechanisms?

Based on its application, iKeepSafe cannot run an effective safe harbor program. Safe harbor applicants must submit "a detailed explanation of [their] business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program."[3] It is the applicant's burden to prove it has the "capability to run an effective safe harbor program."[4] The FTC must find that the safe harbor program meets that requirement.[5] Through these rules, the FTC seeks to ensure that safe harbors are reliable and sustainable.[6]

Reproduced below are the pertinent parts of iKeepSafe's discussion of its technological capabilities and mechanisms:

> The iKeepSafe Safe Harbor program intends to use a combination of manual and technical assessments to determine fitness of Member Companies to participate in and maintain good standing in the program.
>
> Member Company products will be assessed and the guidelines enforced by PlayWell, LLC. . . . PlayWell will have access to the full support and resources of iKeepSafe, including administrative support, database and filing resources, and office support.[7]

The application briefly discusses PlayWell and its President and apparently sole employee, Linnette Attai.[8] Playwell is responsible for at least the following tasks with regard to each

---

[3] 16 CFR § 312.11(c)(1).

[4] *Children's Online Privacy Protection Rule, Statement of Basis and Purpose*, 78 Fed. Reg. 3972, 3996 (Jan. 17, 2013) [hereinafter *Statement of Basis and Purpose*].

[5] 16 CFR § 312.11(b)(2).

[6] *Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking*, 76 Fed. Reg. 59804, 59823 (Sept. 27, 2011).

[7] iKeepSafe app. at 6. The third paragraph says that iKeepSafe (not PlayWell) will help Member Companies determine what information is being sent to third parties on their site if the company cannot make that determination on its own.

[8] iKeepSafe app. at 2-3. iKeepSafe's application mentions no other PlayWell employees. *See*

member website: conduct initial assessments, technical and manual assessments, on-going assessments (three per year), yearly reassessment for renewal of membership; review and develop privacy policies; provide enforcement guidance; and report yearly to the FTC.[9]

iKeepSafe does not provide a "detailed explanation of . . . the technological capabilities and mechanisms" to be used by the program. The application spends a mere three (short) paragraphs discussing the technical capabilities of the companies.[10] In those paragraphs, iKeepSafe says that PlayWell will assess and enforce the guidelines against all Member Companies. This places a substantial burden on PlayWell. The application, however, fails to show that either iKeepSafe or Playwell have *any* technological capabilities or mechanisms to accomplish its extensive tasks. Beyond the (redacted) pricing model, it appears neither company has invested time in planning how to ensure it is an effective safe harbor program.

What little information the application does provide about PlayWell shows that it cannot effectively enforce the safe harbor. First, the application clearly shows PlayWell is not properly staffed to handle its assessment and enforcement responsibilities. PlayWell's responsibilities are extensive, as discussed above. PlayWell seems to have only one employee. It may have access to iKeepSafe's eight staff members, but that is not enough: those eight include five high-ranking iKeepSafe officials.[11] Further, Ms. Attai has responsibilities outside of iKeepSafe's safe harbor program, including serving on iKeepSafe's advisory board and being an adjunct professor at Fordham Business School.[12] These multiple competing obligations exacerbate the problem: Ms. Attai is unlikely to have the time to assess, review, and enforce all Member Companies'

---

also About, PlayWell, http://playwell-llc.com/about-us (last viewed Mar. 31, 2014) (PlayWell's website does not mention any employees besides Ms. Attai. Her email is also listed as PlayWell's primary contact.)

[9] *Id.* at 4–6;

[10] *See supra* note 7 and accompanying text.

[11] iKeepSafe app. at 3.

[12] iKeepSafe app. at 3.

practices on her own, nor to manage many newly hired, and potentially untrained, employees. iKeepSafe's staff of eight each have their own independent responsibilities as well. These companies are essentially creating an entire COPPA safe harbor program with one person. The safe harbor's success is highly implausible given these circumstances. Neither company is properly staffed to do its job.

Second, the application focuses on Ms. Attai's privacy accolades, but does little to support these accolades. The application makes numerous vague claims regarding Ms. Attai "working with major media organizations" and being considered "an expert in the implementation of COPPA."[13] Ms. Attai also has a "keen interest in societal issues impacting children" and has provided pro bono support for iKeepSafe.[14] The only evidence presented, however, of Ms. Attai's experience with COPPA consists of twelve speaking engagements in 2013 on "managing compliance," and authoring or co-authoring three papers with minimal relevance to COPPA.[15] The FTC should not rely on unsupported claims of experience and expertise.

Thus, iKeepSafe has failed to demonstrate the capability to run an effective safe harbor program. iKeepSafe plans to pawn off the responsibility for assessing operators' privacy practices and enforcing the guidelines to a third party, Playwell. Yet, the application provides no

---

[13] *Id*. at 2.

[14] *Id*. at 2-3.

[15] For example, one paper contains a mere one-paragraph summary of the COPPA Rule's consent requirement in relation to schools. *Data Privacy and Schools*, iKeepSafe, http://storage.googleapis.com/ikeepsafe/Data_Privacy_And_Schools.pdf (last viewed April 3, 2014). *See also iKeepSafe and Data Security*, iKeepSafe, http://storage.googleapis.com/ikeepsafe/Data_Security_General_Overview_and_Positioning_Paper.pdf (last visited Apr. 7, 2014) (containing a one-paragraph summary of COPPA's data security requirement); *see also BYOD in Schools: Building Success for Educators*, iKeepSafe, http://storage.googleapis.com/ikeepsafe/BYOD_Building_Success_For_Educators.pdf (last visited Apr. 7, 2014) (out of the document's twelve pages, COPPA is mentioned only four times and each time without substantive analysis) .

basis to conclude that either company has the technological capabilities and mechanisms necessary for the initial and continuing assessment of operators' compliance with the safe harbor program.

Question 2: Do the provisions of the proposed guidelines governing operators' information practices provide ''the same or greater protections for children'' as those contained in Sections 312.2–312.10 of the Rule?

iKeepSafe's proposed guidelines fail to provide "the same or greater protections for children as those contained" in sections 312.2 through 312.10 of the COPPA Rule.[16] First, iKeepSafe's proposed guidelines use permissive standards when the COPPA Rule imposes mandatory requirements. Section 312.6 of the Rule states, "Upon request of a parent . . . the operator of that Web site or online service is *required* to provide to that parent" various opportunities to control personal information provided by their children.[17] The Rule also provides that operators "*must* ensure that the requestor is a parent of that child, taking into account available technology."[18]

In sharp contrast to the Rule's distinctly mandatory language, several provisions in iKeepSafe's application are purely aspirational. For instance, iKeepSafe writes that "[p]arents *should* remain in control of data collected from their child," and "providing parents with notice, choice and consent over [the operator's data practices] should be maintained at all times while the operator intends to collect data."[19] It also writes "Member Companies *should* have a process in place that takes into account available technology to provide for verification that the person requesting to review the data is the parent."[20] By proposing merely permissive standards,

[16] 16 CFR § 312.11(b)(1).
[17] *Id.* § 312.6(a) (including a description of the specific types or categories of data collected from their child, the opportunity to refuse further collection or use of their child's data, the opportunity to direct the operator to delete that data, and a means of reviewing the data.)
[18] *Id.* § 312.6(a)(3) (emphasis added).
[19] iKeepSafe app. at 12 (emphasis added).
[20] *Id.*

iKeepSafe's guidelines fail to provide the same protection contained in § 312.6 of the COPPA Rule.

Second, iKeepSafe's definition of child-directed sites is ambiguous. Under the COPPA Rule, a site that is directed to children—determined by looking to the totality of the circumstances—must presume that all users are children and apply COPPA Rule protections accordingly.[21] If the site is child-directed under the totality of circumstances test, but does not target children as its primary audience, then it is permitted to use an age-screen to differentiate users and apply the COPPA Rule's protections only to those users who self-identify as under age 13.[22] At the moment a user self-identifies as under age 13, the operator has actual knowledge that the user is a child under the COPPA Rule.[23] If the site chooses not to age-screen its users, it remains a child-directed site and must continue to presume that all users are children.[24] Thus, age-screening is an option only for some operators who want to add this feature in order to differentiate among users, but otherwise those sites must assume all users are children.

Under the heading "Children as a Secondary Target," iKeepSafe's application states "[i]f a website or online service is directed to children under 13, but children are not the primary audience, the Member Company may ask users for their age via use of a neutral age-screening mechanism prior to the collection of personal information."[25] This language is unclear because it fails to communicate to operators that if they do not age-screen, they must continue to presume that all users are children. It seems to suggest that age-screening is a good idea, but it does not communicate that it is *required* by the COPPA Rule for operators who assert that "children are not the primary audience" of their child-directed website or mobile application. Even the

[21] 16 CFR § 312.2.
[22] *Statement of Basis and Purpose*, 78 Fed. Reg. at 3984.
[23] *Id.*
[24] *Id*.
[25] iKeepSafe app. at 8.

language in the next paragraph, "Personal information may not be collected prior to requesting the user's age," is not sufficient. This could still apply only to sites that use an age-screening mechanism, and leaves open the possibility that websites with children as secondary targets could collect and use data without age-screening because the guidelines make the age-screen look like an optional best practice rather than a regulatory requirement. While this ambiguity could, in some cases, be sufficient under the COPPA Rule, the lack of clarity in the language could allow operators to avoid compliance with the COPPA Rule by making their services appear slightly less child-directed and then opting not to screen users' ages.

These provisions do not provide the same protection contained in § 312.2.

CONCLUSION

For the reasons stated above the FTC should reject iKeepSafe's application, or require amendments and clarifying submissions from the company.

Respectfully submitted,

/s/

Eric G. Null
Angela J. Campbell
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9535

Of counsel:

John Tran
Georgetown Law Student

/s/

Hudson B. Kingston
Legal Director
Center for Digital Democracy
1621 Connecticut Ave., NW, Suite 550

Date: April 21, 2014