Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	**)**	
	)	
AssertID, Inc. Application for Approval of	**)**	
Parental Consent Mechanism	**)**	**P-135415**

COMMENTS OF CENTER FOR DIGITAL DEMOCRACY

The Center for Digital Democracy ("CDD") respectfully submits these comments in response to the *AssertID Application for Parental Consent Method, Project No. P–135415*, filed with the Federal Trade Commission ("FTC" or "the agency").[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 Commission only approves verifiable parental consent methods that fully comply with the FTC's rules and with the underlying purpose of the Children's Online Privacy Protection Act ("COPPA"), *i.e.* to prohibit the collection of personal information from children without the verifiable informed consent of their parents.

Introduction

The FTC should reject AssertID's application for a verifiable parental consent ("VPC") mechanism for the following reasons: the mechanism is not reasonably calculated, in light of available technology, to ensure the person providing consent is the child's parent; and the mechanism also harms the public because it requires parents to disclose a substantial amount of information without explanation, it allows for Operators to disclose only minimal information regarding information collection practices, and the application contains many ambiguities and

[1] 78 Fed. Reg. 51677 (Aug. 21, 2013) ("Parental Consent Method Notice").

omissions. AssertID's plan to use the information it gathers from parents to target them with particular advertisements is one example of information omitted from the application that must be explained more fully to the FTC.

I. Overview of AssertID Mechanism

AssertID's application for a verifiable parental consent mechanism is the first application for what the FTC calls a "common consent mechanism."[2] As such, the AssertID application includes processes and goals that facilitate VPC en masse by many Operators and parents, and purports to provide on-going support for parents' consent needs. The application includes processes for the following six functions: (1) parental notification of consent-request; (2) presentment of consent-request direct notices to parents; (3) recording and reporting a parent's response to a consent-request to the Operator; (4) recording and reporting a parent's request to revoke consent previously granted and to have their child's personal information deleted; (5) verification of the parent-child relationship; and (6) ensuring only the parent of a child for whom consent is being requested can access and respond to such requests.[3] Despite the seeming complexity of this scheme, the goal of the program is to provide simplicity for Operators and ease-of-use for parents.[4]

Based on the information included in the AssertID application, the following is a detailed description of how a parent would interact with the AssertID Portal.

When a child expresses interest in a website or application by either using it or downloading it, the Operator will use AssertID technology to facilitate VPC. The parent of that child will receive an email from the Operator—the parent's email address and the first name of

[2] Common consent mechanisms hold "potential for the efficient administration of notice and consent for multiple operators." 78 Fed. Reg. 3972, 3989 (Jan. 17, 2013).
[3] App. at 1.
[4] App. at 5-6.

the child are provided by the child.[5] The email will tell the parent to either (1) log into his or her already-existing AssertID account (if the parent previous created one), or (2) follow a link to the AssertID website to sign up for an account.[6]

To create an account, the AssertID Portal will request the following information: the parent's photo, full name, gender, age, and location. "For user convenience," however, this data can be taken from the user's Facebook profile if the parent allows.[7] If the parent does not allow, the information must be input manually.[8]

Once completed, the AssertID Portal will automatically create a "ConsentID," a separate attribute that represents the relationship between the parent and the child.[9] At this point, the parent is given the opportunity to supply information on the child as well: gender, age, and a photo.[10]

Even though this information has been divulged up-front, the parent still is not yet able to view the COPPA disclosures and privacy policies of the websites of interest to his or her child. Before the AssertID Portal will allow a parent to consent to their child using a website or app (in other words, before the Portal becomes functional), all attributes of the parent, as well as the ConsentID (parent-child relationship), must achieve a "trust score" of 7 out of 10.[11]

The trust score is based on a "web of trust" that is created from the parent's social network on Facebook.[12] After the parent fills in the parent and child information as described

---

[5] App. at 19. Once signed up, the parent may choose from other notification options, including Facebook notification or text-message notification. App. at 20.
[6] App. at 21.
[7] App. at 21.
[8] App. at 21.
[9] App. at 21.
[10] App. at 21-22.
[11] App. at 22, 32.
[12] App. at 28.

above, the parent must then go to his or her Facebook account to choose family members and friends (that also have Facebook accounts) to "verify" the information that has been provided to the AssertID program. Those family members and friends must then use the AssertID Portal to verify that information by answering "Yes," "No," or "I Don't Know" to a series of questions.[13] Behind the scenes, AssertID will now have access to the parent's complete friends list (first and last name, profile picture), as well as any information on the parent that is available under the "basic" authorization settings in Facebook.[14] AssertID uses the parent's friend list to analyze "an individual's social-graph" or "web of trust" as a second step to verification in establishing a "trust score."[15]

During the pendency of the verification process, parents might be able to use the already-approved credit-card method to allow their child immediate access to the website or app.[16] The credit-card method also is available for those parents without Facebook accounts.[17] The AssertID website, however, indicates that this option is only available on websites or apps where the Operator has opted to purchase the "Premium" package.[18] As a result, a parent without a Facebook account may be barred from allowing their child to access some or all websites and apps that use the AssertID mechanism. Even if the parent attempts to create a new Facebook account to allow use of the mechanism, it may take a long time to achieve the required trust

[13] App. at 29-31.
[14] App. at 28. "Basic" authorization includes name, profile pictures and cover photos, networks, gender, and username/user ID. It also includes anything the user has chosen to make public. Information We Receive About You, Facebook, https://www.facebook.com/about/privacy/your-info#public-info (last visited Sept. 18, 2013).
[15] App. at 5, 51.
[16] App. at 32.
[17] App. at 28. If chosen, a new credit card verification must occur for every consent request.
[18] AssertID, ConsentID™ Service Pricing, http://www.assertid.com/consentid/pricing (last visited Sept. 19, 2013)

score to allow the parent to consent.[19] Further, parents should bear in mind that if they change *any* verified attribute such as uploading a new photo, the trust score for that attribute is set to zero and the verifiers must re-verify that attribute.[20]

If and when the parent does reach the requisite trust score, *only then* does the parent see information on the website or app the child was seeking to visit or use, and the attendant COPPA-compliant disclosures. These disclosures contain basic information about the website or app, and its privacy policy or policies. Operators, as part of the process to sign-up for AssertID, will have already disclosed data collection information to AssertID in the following four categories: what data is collected, how the data is collected, how the data is used, and who the data is shared with.[21]

For each category, the Operator chooses, from an array of check-boxes, the types of information collected and how it is used and shared. For example, under what data is collected, the Operator can choose, among other things, "Websites visited," "Device identifier," and "Other behavioral data," along with name, address, contact information, geolocation data, and others. Under how the information is gathered, the Operator can choose "directly from the child," "from party databases," "from other sources," and others. The information could be used, for example, "to contact the child," "to personalize the child's user experience," "to perform behavioral analysis," and others. Finally, Operators can note that they share the data with "the child's network of friends," "3rd [party] marketers and advertisers," and "other 3rd parties." Operators may also write a short summary of what they collect and why, which is viewable by parents.[22]

[19] This could also look suspiciously like a child attempting to get around the system.
[20] App. at 31.
[21] App. at 11.
[22] App. at 10-17.

Once the parent has reviewed this information, he or she can either grant or deny access.[23] The Portal retains this information, and allows a parent to access previously granted consents. If a parent changes his or her mind, the Portal allows the parent to revoke access at any time. When that happens, the website is notified, the information that was collected on the child is deleted, and the website will close the child's account.[24] There is no opportunity for the parent to review the data collected on the child through this mechanism or to tell an operator to stop collecting certain information without denying the child future access to the service.

Once parents have an account and have achieved the 7 out of 10 trust score on all individual attributes and the existence of the parent-child relationship, the parents are allowed to consent to websites and apps the child visits or uses, and also can pre-approve other services that use the same AssertID mechanism. Parents will likely learn about these other services through advertisements on the AssertID Portal, which is one way the company plans to monetize its users.[25] The application does not discuss what happens if the trust score dips below 7 after

[23] App. at 9.
[24] App. at 25-27.
[25] *See* AssertID, ConsentID™ Service Pricing, http://www.assertid.com/consentid/pricing (last visited Sept. 9, 2013) ("ConsentID™ Marketplace listing (future) - Operators will have a range of 'application promotion' options designed to improve app-discovery *through targeted placements based upon the ages and application preferences of a parent's children*.") (emphasis added); Angel Launch Bay Area, Keith Dennis, http://www.meetup.com/AngelLaunch/members/12170639 (last visited Sept. 9, 2013) ("I am president of AssertID . . . . Integrated with our ConsentID solution is a '*Application Marketplace*' which will address the two greatest challenges mobile-app publishers face (after COPPA compliance); *app-discovery and monetization*") (emphasis added); Angel List: AssertID, Slide 4, https://angel.co/assertid/deck#1 (last visited Sept. 9, 2013) ("The same parental-portal (ConsentID) where parents can grant consent for their children is an ideal marketplace for mobile-app discovery and monitization"). The fact that this use of VPC-generated verified information is going to be used in a way that is never mentioned in the company's application suggests that the company has not considered the privacy implications of this undisclosed use.

consents have been granted, other than implying parents lose control of their consent/declines on the portal.

II. Analysis

The FTC has recognized the potential benefits of common consent mechanisms. They can be beneficial because they offer parents a centralized consent platform. Because of their central nature, common consent mechanism should be robust and there should be no doubt that they comply with COPPA. In addition, this application is the first common consent mechanism application. For these reasons, the FTC should pay particular attention and subject the application to rigorous scrutiny to prevent subsequent applications from containing the same shortcomings.

These comments will address the following questions: (1) Whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent?; and (2) Does this proposed method pose a risk to consumers' personal information?

a. Whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent?

Any interested party that seeks approval of a parental consent method must "provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1)."[26] Section 312.5(b)(1) states that

> [a]n operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

[26] 16 CFR 312.12(a).

First, the "analysis" provided by AssertID is inadequate. It covers two pages, most of which references previous sections of the application that merely explain *how* the mechanism works, rather than *why* the consent mechanism is reasonable in light of available technology.

The application claims that it "uses" available technology to gain consent,[27] but does not discuss how the use of that technology is "reasonably calculated, in light of available technology" as required by COPPA. In describing the parent-child relationship verification, the "analysis" merely reiterates how the mechanism works.[28] It offers no discussion of other available technologies, whether those technologies are superior, or why AssertID chose to use this particular method rather than some other method and some other technology. A discussion about available technology must necessarily *mention and discuss* other technologies that are available.

AssertID recognizes that its mechanism is susceptible to fraud, as all methods would be.[29] It also recognizes that there are trade-offs between ease-of-use and fraud. AssertID's explanation of how it achieves this "balance" is cryptic: "AssertID achieves this balance through our implementation of configurable 'contexts' which allow us to adjust the veracity of our verifications to meet the specific needs of the application."[30] AssertID further states it has "tuned the weights applied to specific verification coefficients and variables within our proprietary *trust score* algorithm."[31] To the lay reader (and even an experienced reader), this explanation is confusing and unhelpful. How have the weights been "tuned"? What does AssertID mean by "configurable 'contexts'"? To what "context" does the application refer? This kind of "analysis"

[27] App. at 31.
[28] App. at 32.
[29] App. at 32.
[30] App. at 32.
[31] App. at 32.

should not be sufficient for any consent mechanism, much less a common consent mechanism. Surely, the FTC will require more than blanket statements and convoluted technical language by an applicant to satisfy § 312.5(b)(1).

Second, the public lacks the technical expertise and knowledge to discern, for itself, whether this mechanism is "reasonably calculated, in light of available technology." AssertID's application does not adequately explain how the mechanism works in a public-friendly way. For example, the explanation of how the trust score is calculated is amorphous; the extent to which Facebook information will be tied to the AssertID portal is unexplained; and AssertID does not explain how it will overcome potential fraud and abuse of the system.[32]

AssertID has kept secret many aspects of the mechanism. Multiple pages are redacted, including pages that seem to further explain helpful topics such as "Verification Process" and "Trust Score."[33] There are even some inconsistencies between the application and the website: the application states that parents without Facebook accounts will be allowed to use the credit-card verification process approved by the FTC, but the website states that credit card functionality will only be available to parents when Operators pay for the fee-based "Premium" service.[34] Thus, the availability of credit card verification is the Operator's decision, not the

[32] To the extent this information is included in the patent application, it is unreasonable to expect the public to read a highly technical, jargon-filled, and extremely lengthy patent application. It is the applicant's responsibility to "provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1)." 16 CFR 312.12(a).
[33] Exhibit A, AssertID Verification Technology, AssertID Application.
[34] *Compare* App. at 28 *with* AssertID, ConsentID™ Service Pricing, http://www.assertid.com/consentid/pricing (last visited Sept. 19, 2013) ("Premium Services . . . Alternate Verification Methods - An operator has the option to select our alternate verification methods option. This option offers payment card verifications and government ID verification as alternate verification methods. If enabled, parents may select one of the alternate verification methods to complete the consent response.").

parent's. These redactions and inconsistencies make it even more difficult for a member of the public to understand the AssertID mechanism.

Because of AssertID's lack of analysis, and the inability of the public to determine, on its own, the reasonableness of this mechanism, the FTC should find that the mechanism is not reasonable in light of available technology, and should reject the application.

b. Does this proposed method pose a risk to consumers' personal information?

The FTC public notice asks "Does this proposed method pose a risk to consumers' personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this using this method?" There are three primary ways in which this common consent mechanism, if approved, would pose a risk to consumers' personal information and harm the public generally. First, it requires parents to divulge a substantial amount of information without an accompanying explanation as to why so much information must be shared. Second, it allows Operators to explain, at too high of a level of abstraction, the type of data it collects, how it is used, and with whom it is shared. Third, there are many ambiguities in the application that must be explained before the public could understand how key aspects of the mechanism work.

i. Information Shared by Parents and Others

The AssertID Portal requires parents to divulge substantial personal information on both the parent and the child. As discussed above, the parent must provide information such as full name, gender, age, and a photo, to simply create an account to use the mechanism. That information, in turn, is highly likely to be disclosed to third parties in order for the app/website market on the platform to be successful.

Despite claims to the contrary, the information collected is intrusive. The application states "AssertID's verification process does not require that a parent divulge sensitive personal or financial information such as SS#, address, bank account # or government ID and is therefore

less intrusive to the parent."[35] In lieu of collecting financial information, the mechanism collects name, gender, age, and photos from Facebook. It also collects anything viewable under the "Basic" authorization in Facebook (which includes *all* of the parent's friends, profile photos, and cover photos). Further, it collects information about the parent's child. This information is collected far in advance of the parent being able to use the Portal for its intended purpose, because it takes time (it is unclear how *much* time) to reach a score of 7 on all individual attributes and the parent-child relationship. The disclosures should come first so the parent can decide whether he or she wants to provide all this information. If the parent is going to reject the permission anyway, it is needless to require him or her to provide so much personal information.

AssertID has not demonstrated why this amount of information collection is necessary. The public knows nothing about the algorithm and very little about the program in general except for high-level information. Perhaps this information is required for the algorithm to work. But even if that is true, AssertID should also have to show why the algorithm could not be altered to reduce the amount of information that needs to be collected. If the reason the information is being collected is because AssertID needs to advertise operators to individual users, then that should be disclosed and AssertID should explain that. If this is truly the reason, the FTC should scrutinize very seriously the idea that this common consent mechanism is essentially forcing parents to share personal information about themselves and their children well in advance of receiving COPPA-compliant disclosures, all for the sake of advertisers.

The use of AssertID's mechanism is not the parent's decision initially. The Operators sign up for AssertID and invoke AssertID's technology to seek consent from parents. When parents receive their first AssertID email, they *must* sign up for an account before moving

[35] App. at 27.

forward with the consent. It is unlikely that an Operator would use more than one VPC mechanism and the AssertID Terms of Service seem to forbid this;[36] thus, the parent is left with the Hobson's choice of signing up (embarking on the burdensome process described above), or not, which results in the child's inability to access any website or app whose Operator uses AssertID.

ii. Operators' Lack of Specificity

Under the COPPA rule 312.4(a), notice is required to be "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials."[37] While COPPA does not explicitly require a VPC mechanism to comply with § 312.4, it should apply here because AssertID is seeking approval of a "*common* consent mechanism," that would provide a one-stop-shop for parents and all their consent needs. Because the AssertID mechanism is intended as a substitute for direct notice from the Operator itself, the FTC must ensure that the notices to parents meet the requirements of 312.4(a).

The disclosures made by Operators in AssertID in the application are neither clearly and understandably written nor are they complete. For example, an Operator states they are collecting "Websites visited" and are disclosing that to "3rd [party] marketers and advertisers" for the sake of "customiz[ing] advertisements."[38] Given the complexity and ever changing nature of online and digital advertising, it is not reasonable to assume that the average parent will understand what this language means.

[36] "Operators are required to accept the *ConsentID™* terms-of-service ("TOS"), and in so doing agree to be legally bound by these TOS and to process all notifications, status changes and requests issued to them though the *ConsentID™* API in accordance with these TOS." App. at 9.
[37] 16 CFR 312.4(a).
[38] This example could occur, given the prompts in the Portal. App. at 13-15.

In addition, the information is not complete because it fails to provide any specific information about who the third party marketers and advertiser are and what will be advertised that may be important to a parent in deciding whether to let their child utilize the service. Moreover, merely telling parents that "we collect geolocation data" does not provide parents with the information they need to provide informed consent. Does that mean the tracker is on all the time, even when the app is not active, or when the app is on in the background, as well? When an Operator claims it is collecting "Other behavior data," what does that mean? If an Operator claims it is disclosing information to the "child's network of friends," how is that network defined? Is it Facebook? Is it some other platform? Perhaps the "network" itself is collected from the child directly. Thus, the AssertID mechanism fails to supply complete and understandable notice to parents as required by COPPA.

iii. Ambiguities and Omissions in the Application

AssertID's application also contains many ambiguities and omissions. These comments will briefly discuss two ambiguities and then two omissions that are particularly problematic.

AssertID does not make clear how it interacts with the separate Facebook "verifiers." For instance, it does not explain whether the Portal requires the verifiers to sign up, which would require disclosure of verifiers' name, age, gender, and photo as well. If the Portal collects information from those users in some other way, such as through cookies, the application does not make this clear.

The application points out that the trust score is "dynamic,"[39] but the application does not discuss what happens if the trust score goes above 7 and then later goes below 7. If the parent has

[39] App. at 5.

previously granted consent, those consents either could be frozen or automatically revoked. AssertID does not indicate what would happen in this instance. Depending on how the algorithm is calibrated, a simple change in profile picture or other verifiable attribute could automatically freeze the account because all attributes must have a trust score of 7 or above.

There are two primary omissions in the application for the common consent mechanism: there is no explanation of how a parent can review information that an operator has collected about his or her child, and there is no explanation of how parents will review changes in privacy policies.

First, the Portal allows parents to grant or deny consent and allows a parent to revoke a previously-granted consent. There is no provision in the application, however, that discusses how parents can ask the Operator to tell the parent what information the Operator has collected from the child. This is a requirement under § 312.6(a). While COPPA does not explicitly require a VPC mechanism to comply with § 312.6(a), this application is for a "*common* consent mechanism," and is intended is a one-stop-shop for parents and all their consent needs. Moreover, in this case, the AssertID mechanism is being offered as a substitute for the Operator's obligation to allow parents to view information collected about their child. Thus, the FTC should make clear that any such common consent mechanism must also meet the requirements of 312.6(a).

On its website, AssertID indicates that it might provide this service in the future, for Operators purchasing "Premium" services.[40] This function, however, is very important for

[40] AssertID, ConsentID™ Service Pricing, http://www.assertid.com/consentid/pricing (last visited Sept. 19, 2013)

parents and should be launched with the release of the mechanism itself, and not delayed to an indefinite future time.

Second, the application does not discuss how parents can review changes in an Operator's privacy policies. AssertID knows changes will happen: its website boasts that "you can modify your policies at any time."[41] AssertID should not leave this unexplained. There should be at least some discussion of how that situation will be resolved. For instance, will AssertID automatically revoke consent until the parent logs in to grant consent? Will AssertID assume that a parent agrees unless he or she opts out? These are two very distinct options that are not discussed in the application.

The FTC should find that this mechanism will harm consumers because it will require parents (and potentially others) to divulge a substantial amount of information without explanation, it only requires Operators to divulge high-level and vague information, and it leaves unexplained material portions of the process.

Conclusion

For the foregoing reasons, CDD asks the FTC to reject this VPC mechanism application.

[41] AssertID, ConsentID™ - Operator Quick-start Guide, http://www.assertid.com/consentid/getting-started/ (last visited Sept. 18, 2013).

Of Counsel:

/s/
Eric G. Null
Angela J. Campbell
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Ave., NW
Suite 312
Washington, DC 20001
(202) 662-9535

/s/
Hudson B. Kingston
Legal Director
Center for Digital Democracy
1621 Connecticut Ave., NW
Suite 550
Washington, DC 20009
(202) 986-2220

Signatories:

/s/
David Jacobs
Consumer Protection Counsel
Electronic Privacy Information Center
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
(202) 483-1140

September 20, 2013