

July 2020
MPT 2
Representative Passing Answer

To: Tony Briotti

From: Examinee

Date: July 28, 2020

RE: Terms of Service Agreement for Fun4Kids

I have been tasked with writing a memo identifying the relevant issues related to writing terms of service for Fun4Kids, analyzing those issues, and making recommendations as to how to deal with those issues.

The first issue here is whether a browsewrap or a clickwrap agreement is a better solution.

I recommend using a clickwrap agreement for Fun4Kids. I do so because it has a substantially better chance of being upheld as a binding contract. In *Sampson Scientific Foundation, Inc. v. Wessel* (2019) ("Sampson"), the Franklin Court of Appeals considered whether a clickwrap agreement was binding upon its users. In that case, Sampson operated a highly technical website which contained confidential information available to its limited users, which are vetted and permitted to use the website. The website used a clickwrap agreement, which means that each time a user logs onto the website, it is prompted to agree or disagree with the terms of service by clicking a button indicating either choice. Before clicking, the user has the option to click a link and read the full terms of service (TOS) before agreeing or disagreeing. One particular term there was that users are not to disclose any information from the website to third parties not permitted to use the website. the defendant in that case, after agreeing to the TOS, thereafter disclosed information to a non-permitted third party. He argued that the clickwrap agreement was not binding. The Court of Appeals noted first that just because a contract is entered into on the internet, does not make it any less a contract; regular contracts may be entered into on the internet. The Defendant relied on *Harston v. Hobart* (Fr. Ct. Appl. 2011) to argue the clickwrap agreement was non-binding. However, in *Hobart*, the contract at issue was a browsewrap agreemet. this means that by merely using the website, a user consents to the TOS. This also means that there is no

popup or anything prompting users to agree or disagree with the TOS. The court there found that browsewraps are not necessarily binding, but rather depend on fact-specific questions. Because no affirmative action is required by users (such as clicking agree), the determination of validity of a browsewrap contract depends on whether the user has actual or constructive knowledge of a website's terms and conditions. A court will overlook the absence of assent only where there are sufficient reasons to believe that the user is aware of the website's terms. The court also noted that most of the users of the service in *Hobart* were unsophisticated in the world of finance (the website's use). The court then upheld the trial court's ruling against the defendant, finding the clickwrap to be binding. It also noted that most other courts in the nation find clickwrap agreements valid and binding. Additionally, Franklin law (§200.1) states that minors under 18 may have contracts they entered into while a minor disaffirmed by their parents.

As a result, here, for Fun4Kids, I recommend utilizing a clickwrap agreement. As noted, most courts in the nation uphold those as valid and binding. More importantly, for us, is the fact that browsewrap agreements are only upheld if the court can make a determination that the user has actual or constructive knowledge of the website's terms and conditions. Here, the audience is children ages 11-14. Per the Children's Online Privacy Protection Act (COPPA), a child means an individual under 13. That is the bulk of Fun4Kids' audience. It is very unlikely that a court would find that children have actual or constructive knowledge of the website's terms and conditions because children will likely not look into that sort of thing. It would be much safer to require the children to click "agree" on the website before each use, as that will have a better chance of being upheld. Further, per § 200.1, the children may have any contract disaffirmed by their parents, so we need to be very clear in our TOS, which will be addressed below.

Thus, my recommendation is to use a clickwrap agreement because it is much more likely to be upheld as a binding contract than a browsewrap due to its superior clarity and obtaining of consent.

The second issue here is whether the parents' consent is needed, and if so, how it should be obtained.

My recommendation, rather, the FTCs' requirement, is that a parents' permission is needed before an operator of a website directed at kids, or one who actually knows that it is collecting personal information from kids, must obtain verifiable parental consent to any

collection, use, and/or disclosure of personal information of children. I would recommend sending the parents a notice, and providing them with a form to sign or a number to call.

An operator is the person or entity that operates the website or mobile app. Per the FTC's regulations and COPPA, verifiable parental consent must be obtained before the operator of a website collects, uses, or discloses any personal information of children. Per COPPA, verifiable parental consent is any reasonable effort, including a request for authorization for future collection, use, and disclosure described in a notice*, to ensure a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices. Further, FTC regulation 312.5 provides that an operator is required to obtain verifiable consent before any collection or use or disclosure of children's information, and also consent for any changes to agreements parents previously consented to. Further, the parent must have the option of consenting to collection of the kids' information without disclosing his/her own info. Numerous methods of obtaining parental consent exist, such as: provide a consent form to be signed by the parent and returned to the operator, requiring a parent use a credit/debit card, have a parent call a toll-free number, have parent connect to trained personnel via videoconference, or check the parents' identity through a government database. The parent must also have the right to request and view all personal information provided by a child, including names, addresses, telephone numbers, and hobbies. Disclosure, as it relates to this, means any release of personal information for any purpose, other than to an internal operator for website support, and also means making personal information of children collected from a children's website, or by an operator with knowledge of collection, publicly available by any means. Personal information means names, addresses (both physical and email), or info concerning the child or parents collected by the website. Lastly, per FTC reg. 312.4, notice is required to be given to the parents, which must contain: the operator has collected parents' info from the kids, that parents' consent is needed for collection, use, or disclosure of such info and won't be done without consent, a hyperlink to operator's practices, the means by which a parent can provide verifiable consent, and if a parent doesn't consent within a reasonable time, operator will delete their info.

As such, I think providing the parents with notice of what the website will collect, info about that, info about how to review it, and procedures for consenting is appropriate. It may be easiest to simply provide the parents with a form they can sign and send in, or with a number they can call to consent to. We should also send the parents a notice any time the TOS change so they may re-consent. These methods will help protect against a kid pretending to be a parent online. Being clear with the parents is important because they may disaffirm contracts that kids enter into.

The third issue is whether credit cards may be used and what safeguards must be used to employ their use.

My recommendation is to require express consent from parents before charging for anything on the website or app. We could use some of the verifiable consent methods listed above. Further, we should give the parents the option to withdraw their consent.

Per the Persimmon Inc. case, FTC issued a Press Release providing that the above mentioned recommendations are what Persimmon Inc. must comply with going forward. In their case, they had a situation where parents entered a password and that finalized purchases and allowed for unlimited purchases for the next 15 minutes. Persimmon did not inform the parents of this.

To protect Fun4Kids, we should require express parental consent via writing in order to protect against unauthorized purchasing and lawsuits. This includes the website and the app. Plus, an option to take back consent.

The fourth issue is whether the website can collect the kids' information and if so, to what extent.

My recommendation would be that the website can collect kids' information, but limit it to the personal information necessary to participate in the games/activities on the website.

FTC Regulation; 16 CFR §312.3(d) provides that an operator must not condition a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. This is repeated in 312.7. As stated above, violation of this regulation is unlawful. As also stated above, "personal information" includes names, addresses, email addresses, and information concerning the child or parents of that child that the website collects online from the child.

Here, Jan stated that they wish to collect the child's name so that the game can interact with them and use their name in the activities. They wish to collect gender for the same reasons. I would advise that those are both reasonably necessary to the participation of the game, and thus can be collected. However, I would advise against collecting information about the children's or parents' addresses or email addresses. As Jan told us, that information is only for the advertisers and not necessary for the game itself. As such, it is not reasonably

necessary to collect that information to participate in the game, and the website cannot condition participation on disclosing such information.

Thus, I would advise that collecting names and genders is fine, but not to collect home or email addresses.

The fifth issue is whether the advertising to children complies with Franklin's statutes.

My recommendation for advertising would be that as long as the advertising on the website is "geared to kids on site," it will be fine.

Per Franklin Children's Protection on the Internet Act (CPIA), a minor is any individual under 18 years of age. An operator of any Internet website or mobile app shall not market or advertise a product on its website or app, if such marketing or advertising is of: alcohol, guns, cigarettes and other tobacco products, dangerous fireworks, tickets or shares in lottery games, permanent tattoos, drug paraphernalia, or obscene matters.

So, as long as the ads shown on the website are related to kids' interests and about things kids enjoy, it will be safe. Even though some kids may enjoy guns and fireworks (or other items prohibited), it will be a violation of CPIA to advertise such items.
