July 2020
MPT-2 Library

Fun4Kids Terms of Service Agreement

Excerpts from Children's Online Privacy Protection Act (COPPA)

15 U.S.C. § 6501 *et seq.*

§ 6501. Definitions

In this chapter:

(1) Child

The term "child" means an individual under the age of 13.

. . .

(4) Disclosure

The term "disclosure" means, with respect to personal information,

(A) the release of personal information collected from a child in identifiable form by [a website] operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and

(B) making personal information collected from a child by a website or online service directed to children, or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means . . . .

. . .

(7) Parent

The term "parent" includes a legal guardian.

(8) Personal information

The term "personal information" means individually identifiable information about an individual collected online, including

(A) a first and last name;

(B) a home or other physical address including street name and name of a city or town;

(C) an email address;

. . . or

(G) information concerning the child or the parents of that child that the website collects online from the child . . . .

(9) Verifiable parental consent

The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future

collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

. . .

§ 6502. Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet

(a) Acts prohibited

(1) In general

It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the [Federal Trade Commission] regulations [authorized by this Act] . . . .

Excerpts from Federal Trade Commission Regulations

16 C.F.R. §§ 312.3–312.7

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) 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 (§ 312.7); . . . .

§ 312.4 Notice.

(a) General principles of notice. It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) Direct notice to the parent. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) Content of the direct notice to the parent—

(1) Content of the direct notice to the parent . . . . This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) A hyperlink to the operator's online notice of its information practices . . .;

(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

. . .

§ 312.5 Parental consent.

(a) General requirements.

(1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) Methods for verifiable parental consent.

(1) An 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.

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via videoconference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete;

. . .

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

. . .

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning 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.

Excerpts from Franklin Civil Code § 200.1

§ 200.1 Disaffirmance of Contracts

(a) A contract made by a person after he or she has attained the age of 18 years may not be disaffirmed by himself or herself on the ground of infancy. A contract made by a person before he or she has attained the age of 18 years may be disaffirmed by that person's parent or guardian, except as provided in this section.

(b) [Exceptions omitted]

Excerpts from Franklin Children's Protection on the Internet Act (CPIA)

§ 18 Marketing and advertising

(a) An operator of an Internet website, online service, online application, or mobile application directed to minors shall not market or advertise a product or service described in subsection (h) on its Internet website, online service, online application, or mobile application directed to minors. A "minor" is an individual under the age of 18 years.

. . .

(h) The marketing and advertising restrictions described in subsection (a) shall apply to the following products and services as they are defined under state law:

(1) Alcoholic beverages

(2) Firearms, handguns, or ammunition

(3) Cigarettes or other tobacco products

(4) Dangerous fireworks

(5) Tickets or shares in a lottery game

(6) Permanent tattoos

(7) Drug paraphernalia

(8) Obscene matter

. . .

Sampson Scientific Foundation, Inc. v. Wessel
Franklin Court of Appeal (2017)

We are asked to determine if a particular type of online "terms of service" agreement is binding on the users of an Internet website. At the outset, we note that a contract is no less a contract simply because it is entered into via a computer. That is to say, agreements entered into via computer technology may be binding contracts, if the principles of contract law are followed.

The record shows that plaintiff Sampson Scientific Foundation conducts research and development in cutting-edge technologies. It operates a website, to which access is limited to individuals vetted by Sampson for their scientific and academic credentials. Basically, Sampson only allows those whom it trusts and who have "impeccable" reputations in the sciences and the academy to access its website. It takes this step in part because it deems much of the information it posts on its website to be confidential. Hence, it incorporates a "terms of service" agreement on the website, to which all who are given access to the website must agree.

It does so by employing a "clickwrap" agreement. Each time an individual who has been cleared to access Sampson's website logs on to it, a window appears asking the user to "Agree" or "Disagree" to the terms of service by clicking on an appropriate "button" indicator on the window; before making that choice, the user may access and review those terms (the full text of the agreement) by clicking a link that brings up the text. One term contained in the terms of service agreement specifies that the user will not disclose the substance of the information on the website to third parties.

Defendant Frederick Wessel is an associate professor of engineering at Franklin State University, whose academic specialty is rocket propulsion. He was granted access to the Sampson website in 2013, after being vetted and approved by Sampson. In 2014, Sampson posted some information on its website about research it was undertaking on new formulas for rocket fuels. Wessel accessed the website, printed out the information, and supplied it to Astrodyne Industries Inc., a commercial aerospace business, with whom Wessel had a paid consulting relationship. By means unimportant here, Sampson learned that Astrodyne had received the confidential information from Wessel. Sampson sued for breach of contract and sought significant damages. The trial court found for Sampson, and this appeal followed.

Wessel does not contest the facts as found by the trial court and as set forth above. Rather, he claims an error of law. Specifically, he argues that the "clickwrap" agreement is not a binding

agreement at all. He relies on our decision in *Hartson v. Hobart* (Fr. Ct. App. 2011). There, the validity of a "browsewrap" agreement for a commercial loan service was at issue. "Browsewrap" agreements typically have links to their terms of service, but the user's consent is deemed given by the mere use of the website, without the need to click an "Agree" or "Disagree" button. We held that such agreements are not necessarily binding, but rather depend on fact-specific questions. We said: "Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of a browsewrap contract depends on whether the user has actual or constructive knowledge of a website's terms and conditions. A court may be willing to overlook the utter absence of assent only when there are sufficient reasons to believe that the website user is aware of the website owner's terms." We concluded that there was no evidence that the user had actual knowledge of and hence assented to the agreement. We further noted that the overwhelming majority of users of the service were unsophisticated in the world of finance, let alone in the details of commercial loan agreements. Hence, in *Hartson,* we found that the "browsewrap" agreement was not binding.

Wessel's reliance on *Hartson* is misplaced, for a "clickwrap" agreement significantly differs from a "browsewrap" agreement. As the trial court here said, "the clickwrap agreement provided adequate notice to Wessel as a user of the website because it required clicking assent, an affirmative action on his part, and indeed on the part of any user, before access to the website was permitted." We find that the "clickwrap" agreement at issue is valid and binding. We note that many other courts across the nation have almost uniformly reached a similar conclusion.

Affirmed.