

Corporate & Commercial

Cite as: Kristin Bryant, *Not Child's Play: Compliance with the Children's Online Privacy Protection Rule*, 1 *Shidler J. L. Com. & Tech.* 4 (July 1, 2004), at <<http://www.ictjournal.washington.edu/vol1/a004Bryant.html>>

NOT CHILD'S PLAY: COMPLIANCE WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE

By **Kristin Bryant**¹

© 2004 Kristin Bryant

ABSTRACT

The FTC regulates how Web site operators collect personal information from children based on the requirements of the Children's Online Privacy Protection Act (COPPA). The Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus has developed voluntary guidelines that businesses can use to assist them in achieving compliance with COPPA. Businesses that comply with the guidelines are deemed to be in compliance with COPPA and thus shielded from FTC sanctions. Costs of compliance may be high, so some Internet business models that target children may no longer be viable. Any business that does not target children but that collects birth date information from its customers must have a procedure for rejecting information from anyone under age thirteen.

TABLE OF CONTENTS

[Introduction: The Case of UMG](#)

[Requirements of the Children's Online Privacy Protection Act](#)

[The CARU Guidelines: A Safe Harbor Program](#)

[Other Safe Harbor Programs](#)

[Conclusion](#)

[Practice Pointers](#)

INTRODUCTION: THE CASE OF UMG

<1> In February 2004, the FTC settled claims that UMG Recordings, Inc., maintained multiple Web sites that violated the Children's Online Privacy Protection Act Rule ("the Rule").² UMG, a recording company, operates hundreds of general audience Web sites that promote its music labels and individual recording artists. The FTC concluded that at least one site, which promoted a thirteen-year-old pop star, specifically targeted children by including child-oriented games and activities. According to the FTC, UMG's general audience sites and the child-directed site collected personal information from

visitors even though it had actual knowledge that they were children, and it did not notify their parents or obtain parental consent. UMG agreed to pay civil penalties of \$400,000. Moreover, the settlement prohibits future violations, requires that UMG delete all information collected in violation of COPPA, and requires that UMG conform with specific record keeping requirements that allow the FTC to monitor compliance on an ongoing basis.

<2> This was the first time the FTC pursued COPPA enforcement action against general audience sites, asserting that because UMG collected birth dates it had actual knowledge that it was collecting private information from children in violation of COPPA. In this case the FTC has demonstrated a willingness to pursue enforcement action against general audience sites that do not directly target children. At the same time, the FTC expanded the scope of its enforcement to include online activities in connection with software products when it settled a COPPA enforcement action with Bonzi Software, which distributes children's software. These enforcement actions put anyone operating a general audience Web site and collecting birth date information from its customers on notice that they must avoid collecting information from anyone under age thirteen or risk liability for non-compliance with COPPA.

REQUIREMENTS OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

<3> In October 1998, Congress passed the Children's Online Privacy Protection Act of 1998 (COPPA or "the Act"), which protects children's privacy online by regulating how Web site operators collect information from children under thirteen.³ The FTC rule implementing the Act became effective on April 21, 2000.⁴ The Act recognizes the rights of parents to limit and control the personal information their children submit over the Internet and imposes sanctions on Web sites that collect personal information from children without first obtaining parental consent. COPPA's requirements include, but are not limited to:

- Posting a clear, understandable, and complete privacy policy online, including what information the Web site operator collects from children, how it uses this information, and its disclosure practices;
- Providing clear, understandable, and complete notice of its privacy policy, including specific disclosures, directly to parents when required by the Rule;
- Obtaining verifiable parental consent *before* collecting, using, or disclosing personal information from children;
- Giving parents the option to consent to collection and internal use of their children's personal information without consenting to its disclosure to third parties;
- Providing reasonable means for parents to review the

personal information collected about their children and to refuse to permit its continued use or maintenance;

- Not conditioning children's participation in any activity or game on disclosure of more information than is reasonably necessary to participate; and
- Establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.⁵

The regulations apply to commercial Web sites and online services "directed to children under 13 that collect personal information from children, and...general audience sites with *actual knowledge* that they are collecting information from children under 13" (emphasis added).⁶ In determining whether a Web site is targeted at children, the FTC will consider a variety of factors described in the Rule, including the characteristics of the site and evidence of the intended and actual audience.⁷

<4> Operators of Web sites that do not specifically target children but include content that is likely to attract children are subject to FTC sanctions if they know that they are collecting information about children.⁸ The FTC imposed sanctions on UMG's general audience Web sites that were attractive to children because the personal information collected included visitors' birth dates, giving UMG actual knowledge that children were visiting the site and submitting personal information.

<5> The Rule requires Web site operators to notify parents when children under thirteen submit personal information. Web sites must allow parents to change the information submitted or prevent the Web site from using the information.⁹ A Web site operator must make "reasonable efforts to obtain verifiable parental consent" before any collection, use, or disclosure of children's personal information.¹⁰ Web site operators can satisfy this requirement several ways, including:

- Providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile;
- Requiring a parent to use a credit card in connection with a transaction;
- Having a parent call a toll-free telephone number staffed by trained personnel;
- Using a digital certificate that uses public key technology; and
- Using e-mail accompanied by a PIN or password obtained through one of the previously listed methods.¹¹

Until April 21, 2005, acceptable methods of obtaining verifiable consent also include sending an e-mail to the parent and taking some additional step to ensure that the person responding to the e-mail and giving consent is in fact the parent.¹²

<6> It is not clear how effective the suggested methods are. Using postal mail, fax, or a telephone hotline are not Internet solutions, and seem to miss the point of using the Internet; a telephone hotline is also expensive to maintain. Using a credit card is likely to be ineffective because payment cards are not designed to validate age, and a parent can give a child a card to use without being personally involved. Both the digital certificate and password/pin suggestions do not provide sufficient guidance to allow effective implementation. In addition, it is not clear where Web sites will find the infrastructure to support the password/pin method.

<7> The Rule allows the creation of "Safe Harbor" programs by trade associations and other groups.¹³ The Safe Harbor provisions promote industry self-regulation so that the Rule can be implemented in a way that addresses industry concerns and new technologies.¹⁴ Self-regulatory guidelines may be officially approved by the FTC if they require operators to "implement substantially similar requirements that provide the same or greater protections for children as those contained" in the Rule.¹⁵ Web site operators who show that they are in full compliance with an FTC-approved Safe Harbor Program will be deemed in compliance with the Rule and are not subject to FTC enforcement action under COPPA.¹⁶ The CARU guidelines were the first Safe Harbor guidelines, approved in January 2001.¹⁷ Two additional Safe Harbor programs have since been approved, the Entertainment Software Ratings Board (ESRB) Privacy Online Children's Program in April 2001¹⁸ and TRUSTe in May 2001.¹⁹

<8> The FTC specifically "retains discretion to pursue enforcement under the Rule if approval" of the guidelines of the Safe Harbor program "was based upon incomplete or inaccurate factual representations, or if there has been substantial change in circumstances, such as the failure of an industry group to obtain approval for a material modification to its guidelines."²⁰ Thus, the protection provided by a Safe Harbor program is dependent on the accuracy, credibility, and reliability of its sponsoring organization.

<9> Meeting the requirements of a valid Safe Harbor program protects Web site operators from FTC sanctions under COPPA, including civil penalties. COPPA allows the FTC to seek civil penalties of up to \$11,000 per violation of the Rule.²¹ Taking into account the volume of traffic and amount of information that may be collected by a popular Web site, this provision theoretically allows for staggering civil penalties. To date, the largest penalty imposed was \$400,000 in the settlement with UMG Recordings. The settlement

with UMG, combined with recent penalties of \$75,000 to \$100,000, represents a significant increase from earlier settlements of \$30,000 to \$35,000, possibly indicating a trend toward higher penalties for COPPA violations.²²

<10> Businesses that operate Web sites regulated by COPPA may comply with the Rule in different ways. They may change the Web site so that it targets general audiences and does not collect personal information from visitors under thirteen, limiting the applicability of COPPA provisions. If they choose to continue to target children, they may either (a) refrain from collecting any personal information from visitors or (b) create the parental notification devices required by the Rule. Businesses that continue to collect personal information from children may protect themselves from FTC enforcement actions by participating in an approved Safe Harbor program.

THE CARU GUIDELINES: A SAFE HARBOR PROGRAM

<11> The CARU guidelines were the first Safe Harbor program approved by the FTC. CARU was established in 1974 by the National Advertising Review Council (NARC) as a division of the Council of Better Business Bureaus to promote responsible children's advertising and respond to public concern.²³ CARU's most prominent feature is its self-regulatory program, which encourages children's advertisers to adhere voluntarily to standards that promote children's welfare. CARU assists both advertisers seeking to comply with voluntary guidelines and federal regulations, and government agencies seeking to enforce federal guidelines.²⁴

<12> Web site operators who receive communication from CARU alleging that the sites violate COPPA should take note of the relationship between CARU and the FTC. CARU brought UMG to the FTC's attention, resulting in FTC enforcement action against UMG.²⁵ The FTC also investigated and initiated a COPPA lawsuit against Lisa Frank, Inc. based on CARU's determination that: 1) the company's Web site violated the Rule, and 2) it refused to make the changes CARU recommended to bring the Web site into compliance with the Rule.²⁶

<13> The CARU guidelines include a section focused on interactive media, such as the Internet and e-mail. The guidelines regarding the collection of personal information from children over the Internet and through e-mail conform to the requirements of the Act. They "apply to online activities which are intentionally targeted to children under 13, or where the Web site knows the visitor is a child," and provide direction for "[w]ebsites where there is a reasonable expectation that a significant number of children will be visiting."²⁷ As with all sections of the CARU guidelines, this section should be interpreted in light of the guidelines' general principles, which focus on the special needs, developmental capacity, and characteristics of children.

<14> Web sites that comply with the CARU guidelines are deemed to be in compliance with COPPA and are shielded from FTC enforcement action. CARU has developed a procedure for certifying Web sites that comply with the guidelines.²⁸ The certification procedure includes:

- Self-assessment by the Web site operator;
- Initial review by CARU staff; and
- Ongoing monitoring by CARU staff.

All information must be updated annually.

OTHER SAFE HARBOR PROGRAMS

<15> The FTC approved the ESRB Privacy Online Children's Program as a Safe Harbor program in April 2001. ESRB is a "self-regulatory body for the interactive entertainment software industry established in 1994 by the Entertainment Software Association."²⁹ ESRB "independently applies and enforces ratings, advertising guidelines, and online privacy principles adopted by the computer and video game industry."³⁰ The ESRB Safe Harbor program is used primarily by Web sites that offer online games for children.

<16> Web sites may be certified by the ESRB Privacy Online Children's Program if they:

- Register with ESRB Online;
- Submit their privacy policies for review;
- Receive confirmation that ESRB Online has reviewed the policy and determined that it complies with the guidelines;
- Pay an annual license fee;
- Sign a licensing agreement; and
- Receive final certification.

After receiving final certification, the Web site may begin to display the ESRB Privacy Online Certification Seal.³¹

<17> TRUSTe was approved as a COPPA Safe Harbor program in May 2001. TRUSTe was founded in 1996 by the Electronic Frontier Foundation as a "third-party oversight 'seal' program that alleviates users' concerns about online privacy, while meeting the specific business needs of each of [its] licensed Web sites."³² Web sites that comply with TRUSTe's general privacy provisions may contract with TRUSTe to display a special seal on the Web site. TRUSTe certifies Web sites that comply with the COPPA guidelines separately, and grants them a license to display a special "Children's Privacy Seal." Web sites can be certified by TRUSTe if:

- TRUSTe approves the Web site's:
- Privacy statement,
- Parental notices, and
- Privacy practices; and
- The Web site operator:
- Signs a license agreement,
- Submits a self-assessment form, and
- Pays an annual license fees.³³

Additionally, applications by PrivacyBot.com and Privo, Inc. to serve as Safe Harbor programs are currently pending.³⁴

CONCLUSION

<18> Businesses that operate Web sites whose visitors include children must consider the effect COPPA has on their business models. This includes not only sites that target children but also general audience sites that collect birth date information from their visitors. If they collect personal information from children, they must comply with the requirements of the Rule or risk FTC enforcement action, including increasingly large civil penalties and increased FTC monitoring. Businesses can effectively shield themselves from enforcement action by participating in one of the FTC approved Safe Harbor programs. Alternately, businesses may change their Web sites so that the costly parental notification provisions of the Rule do not apply to them.³⁵ General audience sites need procedures to ensure that whenever a visitor provides a date of birth showing he or she is under thirteen, no personal information is collected from that visitor.

PRACTICE POINTERS

- Businesses that operate Web sites targeted at children may avoid possible FTC enforcement action under COPPA by complying with the requirements of the Act, including costly parental notification, or they may change their Web sites so that the COPPA notification procedures do not apply to them.
- Businesses that operate general audience Web sites that collect personal information must determine whether the COPPA provisions apply to them. In doing so, they should consider:
 - Does the Web site ask for the age or birth date of the users?

- If yes, what happens if someone enters an age that is under thirteen?
- If yes, what happens if someone leaves the age blank?

Web site operators must not collect any personal information if the user enters an age or date showing that he or she is under thirteen. If the user leaves the age blank, the operator must determine whether to continue collecting personal information, a potentially risky strategy, or take a safer course and assume that the user is under thirteen.

- If Web site operators choose to continue to collect personal information from children, they must create mechanisms for parental notice, as required by the Rule. Implementing a system that ensures verifiable parental consent may significantly increase the cost of operating the Web site. Each business must determine whether the information gained is sufficiently valuable to justify the cost of obtaining parental consent. Businesses that choose this route should consider participating in a Safe Harbor Program, as doing so ensures that the business is not subject to FTC sanctions under COPPA

[<< Top](#)

FOOTNOTES

1. Kristin Bryant, University of Washington School of Law, Class of 2005. Thanks to Nick Allard and Andrew Konstantaris for feedback on a draft of this article.
2. Press Release, Federal Trade Commission, UMG Recordings, Inc. to Pay \$400,000, Bonzi Software, Inc. to Pay \$75,000 to Settle COPPA Civil Penalty Charges (Feb. 18, 2004) (FTC press release), *at* <http://www.ftc.gov/opa/2004/02/bonziumpg.htm> (last visited Mar. 7, 2004).
3. Pub. L. No. 105-277, Div C, Title XIII, § 1302, 112 Stat. 2681-728 (codified as 15 U.S.C. §§ 6501-6505 (2004)).
4. 16 C.F.R. § 312.1.
5. Complaint for Civil Penalties, Injunctive, and Other Relief at 7, U.S. v. UMG Recordings, Inc., No. CV-04-1050 (C.D. Cal. W.D.), *available at* <http://www.ftc.gov/os/caselist/umgrecordings/040217cagumgrecordings.p>
6. Federal Trade Commission, Frequently Asked Questions about the Children's Online Privacy Protection Rule, *at* <http://www.ftc.gov/privacy/coppafaqs.htm> (last visited Feb. 29, 2004); *see also* 16 C.F.R. §§ 312.2-3.

7. 16 C.F.R. § 312.2.
8. § 312.3.
9. *Id.*
10. § 312.5(a)(2).
11. § 312.5(b)(2).
12. *Id.*
13. § 312.10.
14. Children's Online Privacy Protection Rule, 64 Fed. Reg. 212,59888, 212,59906 (Nov. 3, 1999).
15. 16 C.F.R. § 312.10(b)(1).
16. § 312.10(a)
17. Letter from Benjamin Berman, Acting Secretary, Federal Trade Commission, to Elizabeth Lacroux, Vice-President and Director, Children's Advertising Review Unit (Jan. 26, 2001), at <http://www.ftc.gov/os/2001/02/caruletter.pdf> (last viewed Feb. 29, 2004).
18. Letter from Donald Clark, Secretary, Federal Trade Commission to Marc E. Szafran, General Counsel, ESRB (Apr. 21, 2001), at <http://www.ftc.gov/privacy/safeharbor/esrbapprovalltr.htm> (last viewed Feb. 29, 2004).
19. Letter from Donald Clark, Secretary, Federal Trade Commission, to Rebecca Richards, Director of Compliance and Policy, TRUSTe (May 21, 2001), at <http://www.ftc.gov/privacy/safeharbor/trusteapprovalltr.htm> (last viewed Feb. 29, 2004).
20. Children's Online Privacy Protection Rule, 64 Fed. Reg. at 212,59906.
21. 16 C.F.R. § 312.9, (*citing* 15 U.S.C. §57a(a)(1)(B) (2004), *citing* 15 U.S.C. §45(m)(1)(A) (2004)), *modified* by 16 C.F.R. §1.98(d) (2004).
22. For a complete list of FTC enforcement actions under COPPA and settlements reached, see http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.
23. Children's Advertising Review Unit Self-Regulatory Guidelines: Introduction.
24. *Id.*
25. Press Release, Federal Trade Commission, UMG

- Recordings, Inc. to Pay \$400,000, Bonzi Software, Inc. to Pay \$75,000 to Settle COPPA Civil Penalty Charges (Feb. 18, 2004) (FTC press release), at <http://www.ftc.gov/opa/2004/02/bonziung.htm> (last visited Mar. 7, 2004).
26. Press Release, Federal Trade Commission, Web site Targeting Girls Settles FTC Privacy Charges (Oct. 21, 2001), at <http://www.ftc.gov/opa/2001/10/lisafrank.htm> (last viewed Feb. 29, 2004).
 27. Children's Advertising Review Unit Self-Regulatory Guidelines: Interactive Electronic Media.
 28. Information about how to receive CARU certification is available at <http://www.caru.org/program/index.asp>.
 29. Entertainment Software Rating Board, *About ESRB: What is the Entertainment Software Rating Board*, at <http://www.esrb.org/about.asp> (last viewed Feb. 29, 2004).
 30. *Id.*
 31. Entertainment Software Rating Board, *ESRB Privacy Online*, at http://www.esrb.org/privacy_wp_join.asp (last viewed Feb. 29, 2004).
 32. TRUSTe, *About TRUSTe*, at <http://www.truste.com/about/truste/index.html> (last viewed Feb. 29, 2004).
 33. Truste, *Seal Programs: How to Join the Children's Privacy Seal Program*, at http://www.truste.com/programs/pub_child_join.html (last viewed Feb. 29, 2004).
 34. For further information about all Safe Harbor programs, see <http://www.ftc.gov/privacy/safeharbor/shp.htm>.
 35. Joseph Turow, *Privacy Policies on Children's Websites: Do They Play by the Rules?* 11-12 (2001), available at <http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf> (study of 162 children's websites found that 32 did not post privacy policy or collect personal information, and 24 posted a privacy policy but did not collect personal information).