

Chapin Information Services, Inc.

Federal Trade Commission Office of the Secretary
Room H-159 (Annex C)
600 Pennsylvania Ave NW
Washington DC 20580-0002

Date: Saturday, April 23, 2005

Subject: COPPA Rule Review 2005. P054505

Introduction

I am currently developing a new website, and learning about the COPPA Rule for the first time. It is exciting that the FTC is coincidentally seeking public comment at the height of my awareness of the issues involved. I will gladly share both the benefits and obstacles I experienced while implementing The Rule.

Summary

The COPPA Rule is creating a valuable improvement to the Internet experience. It is spreading awareness of privacy issues for people of all ages. At the same time, it is forcing technology experts to consider the effects of information collection from children and to respond creatively and responsibly to the challenges this creates.

The COPPA Rule is ambiguous on several points. In order for this law to remain beneficial, it must be updated with more specific regulations and exceptions. The Internet increasingly empowers average citizens to create websites and online services that collect personal information. It is therefore necessary to make the COPPA Rule easily understood by the average citizen.

General Practices

In the development and maintenance of a well-designed website, it is absolutely necessary to collect information about the website's visitors. There are two main reasons for this: Security requirements, and technological requirements.

It is absolutely necessary for a website operator to implement proactive security measures. For the purpose of my comments, I would like the audience to know that any given website is constantly at risk of attacks consisting of methods such as brute force password cracking, denial of service networking flooding, server-side and client-side script injection, session hijacking, spam, multiple account registration, inline hotlinking, chat bots, phishing, and intellectual property theft.

It is absolutely necessary for a website to collect a user agent's IP address simply to be a functional server on the Internet. It is also necessary to maintain session state

information for even the simplest non-static content to be available to that user agent after visiting the first page.

These security and technical concerns are always independent of the age of the end user. The COPPA Rule does not recognize this consistently as it is written. I will give specific examples below.

Availability

The ability of children to access information of their choosing is primarily subject to parental control. However, I was disappointed the COPPA Rule did not make a stronger statement against using it as a defense for age discrimination. Websites should be required to make their content available to children unless it is inappropriate for privacy or age rating reasons. As it stands, the COPPA Rule is too intimidating for some website operators to implement properly. I will make specific implementation recommendations below.

The availability of websites directed to children is equally important. I feel that the COPPA Rule does not intend to limit access to any website, but that it will do so increasingly in the future if it is not made more specific and easier to read and implement.

I also feel disturbed by the apparent ban on a child's protection under the First Amendment of the U.S. Constitution created by the COPPA Rule. (see my discussion of (b)(2)(A) below.) That a child should be allowed to speak, except on the Internet, seems extreme or unintentional. I cannot envision an Internet where children are passive participants.

Later in this comment I will also ask the FTC to seriously consider the use of online contact information maintained in a non-retrievable format, and how such information could be used to provide some of the other website functionality that is prohibited by the COPPA Rule. I feel this affects availability directly.

Ambiguity and Inconsistency

Sec. 1302. DEFINITIONS (8) PERSONAL INFORMATION

This definition fails to specify what information is not personal information. Further, it does not positively or negatively mention many pieces of information that are commonly collected by websites. These need to be addressed: an IP Address, an instant messaging identifier, a unique identifier assigned by the user agent itself (such as a media streaming client application's GUID), a username, a password, a date of birth, a physical description, and a photograph. Any and all of these could be stored in a retrievable format by the website operator and used to locate or contact a child. The fact that some of these may or may not also fall under Definition 12 is both confusing and misleading.

Sec. 1303. REGULATION... (b)(1)(A)

Because this paragraph makes no reference to Definition 12 or the phrase, "Online Contact Information," it is fair to assume that website operators are in no way required to provide notice on the website or to parents if the website collects online

contact information. Therefore, I would think it is reasonable to knowingly ask children under the age of 13 to provide their instant messaging screen names and chat room handles to carry on later conversations with the website operator.

Sec. 1303. REGULATION... (b)(1)(B)

The meaning of this paragraph becomes unintelligible after reading the exceptions of Regulation (b)(2). For example, if a website does not maintain collected personal information in a retrievable form, then does this paragraph apply? If not, it is terribly unclear. But if so, then this paragraph places an unreasonable burden on the website operators who most diligently implement the COPPA Rule. How could a website operator incapable of identifying a child be expected to comply with a parent's refusal to permit collections of that child's personal information? The problem lies not with the "use or maintenance in retrievable form", but with the "future online collection." This would seem to be a paradox.

The burden created by this paragraph is exacerbated by the possibility that a parent may have the right under Regulation (b)(1)(B)(iii) to inspect information that was collected under an exception of Regulation (b)(2) not requiring parental consent. In that case, the website operator has no reasonable means of identifying the child's parents. This is especially true when the child's collected information is maintained in a sufficiently anonymous form. How could a website operator be expected to disclose information collected about a child, when that information is not personally identifiable, and no information was collected about the child's parents, and no authenticating information was delivered to the parents, even though information subject to such a disclosure is being maintained?

Sec. 1303. REGULATION... (b)(2)(A)

It is extremely important for the COPPA Rule to establish guidelines regarding website user registration. My best interpretation of this paragraph is that websites are allowed to collect a child's e-mail address to create a user account, so long as that e-mail address is not available to anyone thereafter. However, this paragraph becomes muddled after reading the exceptions of Regulation (b)(2)(E). I will expand on this below and in my implementation recommendations.

The definition of "retrievable form" is missing. This is extremely important in determining the applicability of this paragraph. Online contact information that is not maintained in a retrievable form can later be used by a website operator to personally identify a child and other information that is retrievable. Because this point is missed by The Rule, it is impossible to know how it applies in that situation. I will discuss this further below, but part of the original intention of this paragraph remains unclear.

The definition of "recontact" is missing. This is extremely important in determining the applicability of this paragraph. Unfortunately, it would be reasonable to interpret this as a ban on public speech by children under 13. Consider any public forum or comment section on a news website. Users are usually asked to establish a username with their e-mail address, date of birth, and other information before carrying on conversations. Obviously, even if the personal information and online contact

information were not maintained in a retrievable form, the website operator would have the ability to “recontact” the child, as that would be the website’s intended purpose.

In a sense, the website itself is creating new online contact information. The child would not have the right to speak in this public forum because the operator is required to not maintain online contact information in retrievable form, or to seek consent of the child’s parent. For the sake of the average public forum or news comment section, it is reasonable to assume the website operator will not seek the consent of a parent.

Sec. 1303. REGULATION... (b)(2)(E)

I was so confused after reading the exceptions in this paragraph that I had to call the help line provided for COPPA Rule questions.

My best interpretation of this paragraph is that websites are allowed to maintain a child’s e-mail address for the sake of protecting the security and integrity of the website. This dangerously contradicts what I was told by an FTC representative on the telephone. In that conversation, I was informed that the security and integrity exceptions of this paragraph can only be applied in situations where there is a known and active security problem, and that it does not apply to any potential security risk whatsoever. I was shocked. “Pardon me?” I said. Maybe we should forego passwords and server logs altogether, because these are used only as proactive measures against potential security risks. In fact, by this FTC interpretation, Regulation (b)(2)(E) is in direct contradiction with Regulation (b)(1)(D), which requires the operator to establish reasonable protections.

As I pointed out earlier, proactive security measures are absolutely necessary and are often being implemented by average citizens. Any dilution of accepted security measures would be detrimental to the safety of children on the Internet. I strongly encourage the FTC to strike this entire paragraph, rewrite it, and include at least 20 specific examples of situations where the situation would or would not apply to the website.

Implementation

For me, the most confusing aspect of the COPPA Rule is the implementation of information collection procedures. The policy on use of information is clear. The policy on maintenance of information is clear. But, the legality of collecting a child’s e-mail address for one-time registration purposes is not clear. The legality of collecting information not defined as personal information is not clear. The legality of collecting content from a child in such a manner that it creates new online contact information or the opportunity to “recontact” the child through the website itself is not clear. The legality of collecting online contact information that is not maintained in retrievable form is not clear. I will recommend remedies to each of these issues in order.

The FTC should specify that registration of a user account is an acceptable use of online contact information under the exception of Regulation (b)(2)(A). Website operators who wish to avoid the liability of children announcing their age in a public

forum should ask for the user's age during this registration and disable the child's ability to speak on the website. (This recommendation assumes it is the FTC's intention to prohibit the speech of children when the website operator is aware of their age, as described above, with regard to the missing definition of "recontact".) Similarly, website operators should disable children's use of any sort of communications system, as this could be construed as maintaining online contact information.

The FTC should specify exactly which information is included in the definitions of the (currently disparate) key phrases "personal information" and "online contact information." The FTC should specify that a website operator may not collect and maintain in a retrievable form the online contact information of a child. Website operators should continue to collect users' IP addresses, session state information, usernames, passwords, and all other information that may be used to contact a child, but is necessary to proactively protect the security and integrity of the website, its users, and the personal information it maintains.

The FTC should specify whether or not it is allowable under the COPPA Rule to maintain information in a non-retrievable form. This would be in contrast to not maintaining information in a retrievable form. As I discussed earlier, this is a very important distinction. Website operators should use technologies such as a one-way encryption hash (such as MD5 or SHA) to maintain information such as children's e-mail addresses in a non-retrievable form. This allows the website operator to prevent children from registering multiple accounts while making it impossible for the operator to initiate contact with the child.

The COPPA Rule implicitly prevents a website operator from any "recontact" with a child. This means children will not be allowed to use features such as newsletters or password recovery. However, if a child specifically requests password recovery and provides the e-mail address for contact, it would be possible to verify the hash of that e-mail address against the hash being maintained by the website. This would provide beneficial functionality without directly exposing the child's online contact information. The FTC should seriously consider allowing such automated "recontact" under the COPPA Rule, so long as it is explicitly requested by the child each time.

Interestingly, several questions come to mind on either side of this debate. Does this mean that the child's account is personally identifiable? Absolutely. Yes. However, this could only be accomplished upon examination of the original e-mail address, which would have to be provided by the user or by a child's parent. Under no other circumstance would the website operator be able to identify the child's account using a hash of the e-mail address.

Therefore, the FTC should seriously consider whether Regulation (b)(1)(B) is applicable in a situation where the website operator is unable to identify the information maintained for an individual child's account unless the parent identifies the child to the operator. This applies not only to the use of e-mail addresses but also to usernames. A parent who wishes to exercise their right to examine the information collected about

“John Doe” would have to violate the anonymity of the collected information if the child’s name was not also collected. The FTC should seriously consider protecting information that is maintained in a non-retrievable form.

The FTC should also seriously consider protecting information collected under an exception of Regulation (b)(2) that does not require anything be sent to or received from the child’s parents, but could still be subject to Regulation (b)(1)(B)(iii) requiring the website operator to provide to a parent means to obtain that information. At least, the FTC should specify that this is not “reasonable under the circumstances.”

On the other hand, maintenance of information in non-retrievable form does create opportunity for abuse of the FTC’s policy of no “recontact”. Website operators will have to be diligent to abide by the FTC’s rule to allow or disallow automated password recovery by children.

Website operators should use new popular technologies in place of a more traditional e-mail newsletter system. An RSS news feed would allow a child to register an account on another website and use that other website’s services to anonymously consolidate favorite news feeds into one location or home page. In this way, children could receive updates about a website without being contacted by the website operator. I highly recommend that website operators do this, and I highly recommend that the FTC make this recommendation part of the COPPA Rule or its related privacy information websites.

Conclusion

While the COPPA Rule is beneficial to the legal advisors of major website operators, it is confusing and contradictory in the eyes of the average citizen who is more and more likely to have their own website complete with user-contributed information.

Consider a website that has a variety of content including forums, games, and static resources. In order to maintain a well-moderated and secure forum section, the website operator decides to install a forum software package that automatically collects user names, passwords, e-mail addresses, IP addresses, usage histories, session state cookies, and birthdates. The website operator knows that the forum section does not work securely (if at all) without amassing this information, but in reading the COPPA Rule finds very little guidance. May e-mail addresses be maintained in a non-retrievable form? Is the forum considered a means to “recontact” users under the age of 13? Is there any guidance about IP addresses and birthdates?

The COPPA Rule needs a moderate amount of revision and clarification to answer these questions.

Sincerely,

Robert Chapin
President