NOTE

Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online

Dorothy A. Hertzel*

* B.A., University of Illinois, 1995; Candidate for J.D., Indiana University School of Law—Bloomington, 2000.

I. INTRODUCTION

Statistics reveal that approximately sixty-four million adults in the United States use the Internet.[1] Studies also indicate that nearly two-thirds of children have used the Internet.[2] In addition to being a valuable tool to those who use it, the Internet has created unique concerns for users, Internet providers, and lawmakers. Protecting a user's privacy while online is one such concern. A practice that implicates this concern is the collection, storage, and sale of an online user's personal information without that user's knowledge or consent. Such a practice is commonplace in the Internet world. A Federal Trade Commission (FTC) investigation of 1402 Web sites in 1998 revealed that ninety-two percent of those Web sites collected personal information from their users, yet only a fraction notified the user on how that information would be used.[3] The relative ease with which Web sites collect personal information from online users is disconcerting. In fact, the Internet is said to have the "capacity to be the most effective data-collector in existence."[4] The practice of collecting and releasing or selling an online user's information becomes particularly troublesome when the user is not an adult but rather a child. Unfortunately, studies indicate that the solicitation of a child's personal information is dangerously common.[5]

Given that children are signing onto the World Wide Web (Web) in increasing numbers, how to protect a child's privacy online is at the forefront of the "privacy" discussion. As a result, both the Internet industry and lawmakers focused their recent efforts to curb the widespread practice. The Internet industry has made conscious efforts aimed at protecting a child's privacy online.[6] These efforts include requiring that Web site operators post a privacy policy. Recently, big players in the Internet industry have created an informational Web site to alert parents about the

1. *See Almost 65 Million Americans Online* (visited Jan. 29, 2000) <http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_150971,00.html>.

2. *See Parents Lack Skills to Supervise Children Online* (visited Jan. 29, 2000) <http://cyberatlas.internet.com/big_picture/demographics/article/0,1323,5901_164711,00.html>.

3. *See* FTC, *Privacy Online: A Report to Congress* at 19 (visited Jan. 29, 2000) <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> [hereinafter *Report to Congress*].

4. Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1164 (1997).

5. *See* FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure* at IV.A. (visited Jan. 29, 2000) <http://www.ftc.gov/reports/privacy/privacy1.htm> [hereinafter *Staff Report*].

6. *See* Greg Miller, *Firms to Set Standards for Online Privacy*, L.A. TIMES, June 20, 1999, at D1; *Internet Privacy Alliance Recommends New Guidelines*, COMM. DAILY, June 20, 1999, at 4.

dangers of their children roaming the Internet without supervision.[7] In November 1998, Congress enacted the Child Online Privacy Protection Act (COPPA), which governs online information collection from children under thirteen years of age.[8] Pursuant to COPPA, the FTC issued a rule implementing the requirements of the legislation.[9] The rule will become effective in April 2000.[10] In addition to legislation and industry efforts, technological tools are currently available that block the transfer of personally identifiable information from the user to the computer.

Attempts to address the matter of a child's privacy online raise the question: Who is in the best position to properly and effectively protect a child's privacy online? This Note attempts to answer this question. Part II discusses the privacy concerns raised by both adults and children online. Part III discusses the recently enacted COPPA and the FTC's Rule implementing the legislation and whether such legislation will prove effective in protecting children online. Part IV discusses the role of the Internet industry in protecting children online and the value of technological tools available to protect against the unwanted solicitation of a child's personal information. After concluding that neither the government nor the Internet industry are in a sound position to secure children's privacy online, Part V proposes the necessary element to ensure that children can enjoy the benefits of the Internet safely.

II. PRIVACY CONCERNS

A. Information Collection

The Internet is unique among other communications mediums in the "variety and depth of personal information generated by its use."[11] The majority of personal information collected online is gathered by Web sites in one of two ways. First, a Web sites collect the user's personal information without the user's knowledge.[12] A user browsing the Web provides the Web site with certain personal information each time that person visits a site.[13] By leaving an "electronic marker" at each site or page that they visit, the user unknowingly provides information to the Web site

7. *See GetNetWise* (visited Jan. 29, 2000) <http://www.getnetwise.org>.
8. *See* 15 U.S.C.A. § 6501 (1998).
9. *See* 16 C.F.R. §§ 312.1-312.12 (1999).
10. *See id.*
11. *Staff Report*, *supra* note 5, at II.A.
12. *See id.*
13. *See* Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 859 (1998).

that can be stored and reused.[14] Unbeknownst to the user, a Web site can then "'know' [a] users' e-mail addresses, the names of their browsers, the type of computer they are using, and the universal resource locator (URL), or Internet address, of the site from which they linked to the current site."[15]

Second, sometimes a user voluntarily discloses personal information to a Web site. For example, various Web sites require users to register in order to gain access or provide certain information in order to complete a purchase.[16] Web site may also provide incentives to the user to provide personal information.[17] Many users provide this information rather freely.[18] A survey conducted by Dr. Alan F. Westin revealed that 92% of online users were "concerned" and 67% of online users were "very concerned" about the possible misuse of their personal information online.[19] Despite express concerns, however, surveys reveal that users do not refuse to provide personal information to requesting Web sites and rarely do they provide false information. For example, a study conducted by the Boston Consulting Group revealed that only 42% of online consumers refuse to provide information to requesting Web sites and only 27% provide false information to those sites.[20]

There are other ways to track a user's online activities. New methods demonstrate the ease with which technology can be used to facilitate the collection of personal information. In 1999, Intel released its new Pentium chip labeled with a unique identifying number that could be used to track an online user's activity.[21] Additionally, it was discovered that certain Microsoft operating systems attached the computer's serial number to documents or spreadsheets created by the user.[22]

The dangers and concerns do not arise with the mere collection of personal information. Instead, the concerns surround how this information is later used. Information, whether it is collected by the voluntary of unknowing online user, is often resold to marketers,[23] accessible to public

14. *See Staff Report*, *supra* note 5, at II.A.

15. *Id.* (footnote omitted).

16. *See* Budnitz, *supra* note 13, at 859.

17. *See id.*

18. *See id.* at 850.

19. *See* Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, PRIVACY & AM. BUS., Nov. 1999, at 7.

20. *See* Budnitz, *supra* note 13, at 850.

21. *See* Richard Raysman & Peter Brown, *Update on On-Line [sic] Privacy*, N.Y. L. J., Nov. 9, 1999, at 3.

22. *See id.*

23. *See* Gindin, *supra* note 4, at 1157; Budnitz, *supra* note 13, at 853.

online users,[24] or stored by Web sites for future use or sale.[25] The majority of online participants are unaware of these practices. A survey revealed that eighty-one percent of consumers "believe [that] [W]eb sites do not have the right to resell information about them to third parties."[26] What online users do not recognize is the value of their personal information to online marketers. A user's personal information enables an online marketer to personalize and tailor advertising to a particular individual. Because studies indicate that such advertising receives a more positive response than random ads sent to the online user, companies have a financial incentive to collect users' personal information.[27]

To aggravate the situation, a majority of Web sites fail to provide notice to users about how their personal information will be used.[28] In 1998, the FTC conducted a thorough examination of over fourteen hundred Web sites.[29] The investigation disclosed that nine out of ten Web sites collected personal information,[30] while only a fraction of those Web sites provided the user with notice on how their personal information would be used.[31] More recently, a Georgetown study revealed that while the vast majority of Web sites collect personal information from consumers, about sixty-six percent of commercial Web sites posted a privacy policy.[32]

Despite marked concerns about privacy online, there is currently no legislation restricting the practice of collecting information from online users. In its 1998 report to Congress, the FTC stated that, as for adults, industry efforts looked promising and legislation was unnecessary.[33] However, in the same report, the FTC expressed concerns about children's privacy online.[34]

B. Children's Privacy Online

Studies reveal that the Web sites' practice of soliciting personal

24. *See* Budnitz, *supra* note 13, at 859.

25. *See id.*

26. Budnitz, *supra* note 13, at 850.

27. A majority of Internet users indicated that they would be positive toward receiving ads tailored to their personal interests. *See* Westin, *supra* note 19, at 8.

28. *See Report to Congress*, *supra* note 3, at iii.

29. *See id.* at ii.

30. *See id.* at iii.

31. *See id.*

32. *See Georgetown Internet Privacy Policy Study* (visited Jan. 29, 2000) <http://www.msb.edu/faculty/culnanm/gippshome.html>; Jeffrey D. Osterman, *Consumer Privacy and the Internet*, 570 PRACT. L. INST. 1113, 1118 (1999).

33. *See Report to Congress*, *supra* note 3, at iii.

34. *See id.* at i-ii.

information from children is commonplace.[35] Unlike adults, the solicitation of personally identifiable information from children triggers special privacy concerns. There are several reasons to consider children more susceptible to this kind of invasion of privacy.[36] First, children are a group that socially and legally have always been given special protections because they are considered less capable of protecting themselves. Second, children "lack the cognitive ability to recognize and appreciate privacy concerns"[37] and are more trusting than adults. Third, children "may not understand the nature of the information being sought, nor its intended uses."[38] Finally, the mode of solicitation is often too appealing for a young child to resist.[39] In addition to these factors, the lack of supervision while online exacerbates a child's vulnerability to online violations of privacy.[40] A 1998 survey revealed that thirty-six percent of parents admitted that they never supervised their child's use of or access to the Internet.[41]

The availability of a child's personal information online has several implications. First, the information is valuable to marketers who wish to target an eager audience. As a result, the Web sites that collect this information are likely to store or sell the information to turn a profit. In addition to invading that child's privacy, a child or that child's parent is subsequently bombarded with advertisements after the information has been sold to a third-party marketer. Furthermore, it is not clear whether a Web site monitors to whom it provides the user's personal information. For example, in May 1996, a reporter, posing as Richard Allen Davis, a man convicted of kidnapping and murdering a twelve-year-old child, obtained a list of five thousand children living in various neighborhoods.[42]

Second, and equally alarming, are the dangers that arise when a child posts personal information on a bulletin board or provides information to

35. *See id.*

36. The interest in protecting children did not arise with concerns regarding the Internet. There are restrictions aimed at protecting children from the dangers of other mediums. For example, there are special regulations concerning television advertising directed at children. *See* Angela J. Campbell, *Ads2Kids.com: Should Government Regulate Advertising to Children on the World Wide Web?*, 33 GONZ. L. REV. 311, 313 (1997).

37. Nicholas W. Allard, *Privacy On-Line [sic]: Washington Report*, 20 HASTINGS COMM/ENT L.J. 511, 529 (1998).

38. Jerry S. Birenz, *Caching World Wide Web Sites*, 516 PRACT. L. INST. 475, 516 (1998).

39. *See* Campbell, *supra* note 36, at 320.

40. *See* Anne R. Carey & Web Bryant, *USA Snapshots: Who's Watching Kids Online?* USA TODAY, Sept. 24, 1998, at 1A.

41. *See id.*

42. *See* Gary Chapman, *The Cutting Edge Cybernews Protecting Children Online Is Society's Herculean*, L.A. TIMES, June 24, 1996, at D14.

gain access to a chat room. The unsuspecting child not only makes his or her personal information accessible to the public but also makes him or herself available for anyone to address online. An investigation conducted by the Federal Bureau of Investigation and Department of Justice concluded that the Internet is being utilized by predators of children.[43]

In 1996, the FTC conducted a workshop to probe privacy issues posed by children online.[44] Here, the FTC recognized that children "represent a large and powerful segment" of online consumers who are actively targeted by commercial Web sites.[45] The FTC concluded that: "(1) children are a special audience; (2) information collection from children raises special concerns; (3) there is a need for some degree of notice to parents of Web sites' information practices; and (4) parents need to have some level of control over the collection of their children's information."[46]

Also in 1996, the FTC staff identified and surveyed 272 sites from several lists of children links.[47] The FTC disclosed the results of this survey in the *Staff Report*, which followed the workshop.[48] The *Staff Report* revealed that Web sites employ a variety of methods to obtain a child's personal information. These methods include requiring a child to provide personal information when seeking to correspond with fictitious characters, register in a contest or drawing, obtain access to a chat room or certain site, or register to play a game.[49]

While most sites operating at the time of the survey simply requested the child's e-mail and mailing address, other sites requested more personal information. For example, Disney.com required its visitors to register in order to participate in contests and demanded a child's full name, birth date, and mailing address in order to receive "free updates."[50] Freezone.com held a short story contest online.[51] To submit an entry in the contest, the site required that a child provide his or her name, age, address, and phone number.[52] Cyberjaques.com required that its visitors register by providing their name, date of birth, gender, full street address, parents' full name, and e-mail address.[53] While all participants at the workshop agreed

43. *See Staff Report*, *supra* note 5, at I.
44. *See id.*
45. *Id.* at IV.
46. *Id.* at IV.B.2.
47. *See id.* at VI, app. e, A.
48. *See id.* at II.C.2.
49. *See id.* at VI, app. e, B.
50. *See id.* at IV, app. e, C.
51. *See id.*
52. *See id.*
53. *See id.*

that a child's privacy interests are unduly jeopardized while that child is online, a majority of the participants disagreed as how or who should protect a child's privacy online.[54]

In July 1997, the FTC investigated and reprimanded for the first time a children's Web site for its "deceptive" practices.[55] The Center for Media Education's (CME) allegations of deceptive practices in the operation of Kids.com prompted the investigation.[56] Using the authority granted to them under the FTC Act,[57] the FTC's investigation found that practices engaged in by Kids.com violated Section 5 of the FTCA.[58] Although the FTC did not recommend enforcement measures, it took the position that:

> [I]t is a deceptive practice to represent that a Web site is collecting personal identifiable information from a child for a particular purpose . . . , when the information will also be used for another purpose which parents would find material, . . ., in the absence of a clear and prominent disclosure to that effect.[59]

In June 1998, the FTC released *Privacy Online: A Report to Congress*.[60] The FTC notified Congress that industry self-regulation was not effective and legislation was necessary to protect children's online privacy.[61] The FTC reached this conclusion after reviewing the results of a survey of over fourteen hundred Web sites, including 212 children's Web sites, conducted in March 1998.[62] The vast majority of these Web sites collected personal information from children, yet only a fraction warned the users of that fact.[63] Moreover, very few had a "comprehensive privacy policy."[64]

The results of the survey of children's' sites did not reveal a significant change from the survey taken in 1996. Eighty-eight percent of Web sites directed at children collected personal identifying information from children.[65] Only 54% disclosed for what purposes the information

54. *See id.* at IV.B.2.

55. *See* Birenz, *supra* note 38, at 487; *see also* Information Technology Practice Group for Cooley Godward, LLP, *Privacy Limits on Collecting Personal Information via the Internet*, 15 COMPUTER L. 17, 18 (1998).

56. *See* Birenz, *supra* note 38, at 489.

57. *See* 15 U.S.C. § 41 (1994).

58. *See* § 45 (1994) (prohibiting unfair and deceptive practices that are in or affecting commerce).

59. Birenz, *supra* note 38, at 490.

60. *See Report to Congress*, *supra* note 3, at 1; *see also* Campbell, *supra* note 36, at 335.

61. *See Report to Congress*, *supra* note 3, 41-42.

62. *See id.* at 19.

63. *See id.* at 23, 27; Campbell, *supra* note 36, at 335.

64. Campbell, *supra* note 36, at 335.

65. *See Report to Congress*, *supra* note 3, at 31.

would be used, while only 24% posted a privacy policy.[66] Less than 10% of the surveyed sites provided for some level of parental control and only 23% of the sites suggested that the child online user consult with their parents before providing the requested information.[67] Based on these findings, the FTC recommended "that Congress develop legislation placing parents in control of the online collection and use of personal information from their children."[68]

In September 1998, FTC Chairman Robert Pitofsky testified before Congress and asked lawmakers to enact children's online privacy legislation.[69] Al Gore suggested legislation that "gives parents the right to say yes or no before information can be collected from children under age [thirteen]."[70] In October 1998, pursuant to the FTC's suggestion, legislators passed the COPPA.[71] Passage of this legislation reflects the view that the government, not the industry is in the best position to protect a child's privacy interests.

III. THE CHILD ONLINE PRIVACY PROTECTION ACT

While adult users currently surf the Net, their personal information unguarded, children's privacy is now protected by the COPPA.[72] Congress designed the COPPA to enhance parental involvement in a child's activities online, protect the safety of a child while participating in online locations such as chat rooms, secure a child's personally identifiable information collected online, and limit information collection from a child absent parental consent.[73] To accomplish these goals, the COPPA places certain restrictions on the practice of soliciting personal information from children online.[74]

A. Provisions of COPPA

Generally, the COPPA requires that the operator of a children's Web site that collects personal information must provide notice on the site of what information is collected and how the information is used.[75] Second,

66. *See id.* at 34-35.
67. *See id.* at 37.
68. *Id.* at 42.
69. *See* Richard Raysman & Peter Brown, *Regulating Internet Content, Privacy; Taxes*, N.Y.L.J., Nov. 10, 1998, at 3.
70. *Gore Endorses Privacy Regulation by Industry*, COMM. DAILY, Aug. 3, 1998, at 4.
71. *See* 15 U.S.C.A. § 6501 (1998).
72. *See id.*
73. *See* 144 CONG. REC. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan).
74. *See id.*
75. *See* 15 U.S.C.A. § 6502(b)(1)(A)(i) (1998).

the Web site operator must obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.[76]

The COPPA protects children under the age of thirteen.[77] Congress imposed compliance with the requirements of the COPPA on "any person who operates a website [sic] located on the Internet or an online service and who collects or maintains personal information from or about the users . . . where such website [sic] or online service is operated for commercial purposes."[78] The COPPA specifically targets those "website [sic] or online service directed to children."[79] However, a Web site operator who has *actual knowledge* the site is collecting personal information from a child must comply with the COPPA's parameters.[80] The COPPA does not apply to third parties that were not involved in the collection of personal information.

COPPA defines "personal information" broadly. Personal information means:

> [I]ndividually 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 e-mail address;
>
> (D) a telephone number;
>
> (E) a Social Security number;
>
> (F) any other identifier that the [FTC] determines permits the physical or online contacting of a specific individual; or
>
> (G) information concerning the child or the parents of that child that the website [sic] collects online from the child and combines with an identifier described in this paragraph.[81]

The COPPA requires that a Web site obtain "verifiable parental consent" before collecting information from a child.[82] To obtain verifiable parental consent, a Web site operator must make:

> [A]ny 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

76. *See id.* § 6502(b)(1)(A)(ii) (1998).

77. *See id.* § 6501(1) (1998).

78. *Id.* § 6501(2)(A) (1998).

79. *Id.* § 6502(a)(1) (1998). A Web site is directed to children if it is a "commercial website [sic] or online service that is targeted to children; or that portion of a commercial website [sic] or online service that is targeted to children." *Id.* § 6501(10)(A).

80. *See id.* § 6502(a)(1).

81. *Id.* § 6501(8) (1998).

82. *Id.* § 6502(b)(1)(A)(ii) (1998).

> 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.[83]

The parental consent requirement is subject to certain exceptions. For example, parental consent is not required when the operator collects personal information to "respond directly on a one-time basis to a specific request from the child and is not used to re-contact [sic] the child" or when the request for personal information is needed "for the sole purpose of obtaining parental consent."[84]

The COPPA also mandates that Web operators remedy situations where a child's information has already been disclosed to the operator.[85] Upon request of a parent, a Web operator must provide a description of the type of personal information collected from the child.[86] The Web provider must also allow a parent an opportunity at any time to refuse to permit further use or future online collection of personal information from that child.[87] In addition, the Web provider must create a "means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child."[88]

The COPPA also restricts the practice of enticing children to disclose personal information through contests or by offering prizes.[89] The COPPA bars "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity."[90]

The COPPA does not provide parents or children with a private right of action and protects Web sites from liability in the event of a good faith effort to remedy the disclosure of a child's personal information.[91] The COPPA mandated that the FTC enforce the legislation and enact rules governing the online collection of personal information from children under the age of thirteen.

83. *Id.* § 6501(9) (1998).
84. *Id.* § 6502(b)(2)(B) (1998).
85. *See id.* § 6502(b)(1)(B) (1998).
86. *See id.* § 6502(b)(1)(B)(i).
87. *See id.* § 6502(b)(1)(B)(ii).
88. *Id.* § 6502(b)(1)(B)(iii).
89. *See id.* § 6502(b)(1)(C) (1998).
90. *Id.*
91. *See id.* § 6502(b)(D) (1998).

B. FTC's Child Online Privacy Protection Rule

In April 1999, the FTC published its *Notice of Proposed Rulemaking* and requested public comments.[92] The FTC received 147 comments from a variety of concerned parties.[93] Additionally, in July 1999, the FTC sponsored a public workshop to acquire additional information from representatives of various groups, including Internet businesses and privacy groups, on how to obtain verifiable parental consent.[94] The FTC held the workshop in response to concerns represented in the comments about how to effectively and practically obtain verifiable parental consent in compliance with the COPPA. In October 1999, the FTC released the Child Online Privacy Protection Rule (Rule).[95] April 2000 is the effective date of the Rule. The Rule offers Web site operates guidelines on how to comply with the requirements set out in the COPPA.[96]

First, the Rule addresses the COPPA's statutory definitions. While most of the Rule's definitions are consistent with the COPPA, the Rule supplemented some definitions. The Rule asserts that the COPPA's protections extend both to the direct and passive gathering of any personal information from a child.[97] While the Rule retained the definitions "child" and "verifiable parental consent," it extended the COPPA's definition of "Internet" to include "the myriad of computer and telecommunications facilities, including equipment, and operating software, which comprise the interconnected world-wide network that employ the Transmission Control Protocol/Internet Protocol, or any *predecessor or successor* protocols."[98] Because the "technology used to provide access to the Internet will evolve over time, it is imperative that the Rule not limit itself to current access mechanisms."[99] The Rule also explains that a screen name that is associated with individually identifiable information will be considered "personal information."[100]

The COPPA requires that Web operators notify users of what information is being collected. The Rule offers specific instructions

92. *See* Notice of Proposed Rulemaking, 64 Fed. Reg. 22,750 (1999).

93. *See Public Comments Received*, <http://www.ftc.gov/privacy/comments/index.html>.

94. *See Children's Online Privacy Protection Rule Public Workshop* (visited Jan. 21, 2000) <http://www.ftc.gov/privacy/chonlpritranscript.pdf> [hereinafter *Children's Online Workshop*].

95. *See* 16 C.F.R. § 312.1 (1999).

96. *See id.*

97. *See id.*

98. *Id.* § 312.2 (1999).

99. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 (1999).

100. *Id.*

regarding where to locate the notice.[101] According to the Rule, notice must be placed "at each area on the website [sic] or online service where children directly provide, or are asked to provide, personal information and in close proximity to the requests for information in each such area."[102] Also, if a general audience site links to a children's area, then notice must be provided on the home page of the children's site.[103] The notice must contain certain details.[104] Such details include the "types of personal information collected from children and whether the information is collected directly or passively;"[105] whether the personal information would be disclosed to third parties [and] the types of business in which such third parties are engaged;"[106] and "[t]hat the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[107]

The COPPA requires that an operator "obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented."[108] The public workshop held in July 1999, the FTC and others discussed and reviewed the problems surrounding this provision.[109] The concerns that were raised focused on how to effectively obtain a parent's consent. As expressed at the workshop, obtaining "verifiable parental consent" is costly.[110] One estimate of the cost related to obtaining parental consent was two dollars a child or fifty to sixty thousand dollars a year.[111] This cost is nominal to large Internet service providers but concerns were expressed that such a cost would effectively wipe out small to medium-size Web providers. Another concern raised at the workshop was how to obtain verifiable parental consent.[112] The Web providers discussed the current mechanisms available to obtain parental consent: e-mail, faxing, toll-free numbers, credit card verification, or digital

101. *See* 16 C.F.R. § 312.4(b)(1) (1999).
102. *Id.* § 312.4(b)(1)(iii).
103. *See id.* § 312.4(b)(1)(i).
104. *See id.* § 312.4(b)(2).
105. *Id.* § 312.4(b)(2)(ii).
106. *Id.* § 312.4(b)(2)(iv).
107. *Id.* § 312.4(b)(2)(v).
108. *Id.* § 312.5(a)(i) (1999).
109. *See Children's Online Workshop*, *supra* note 94.
110. *Id.* at 15 (statement of Ms. Aftab).
111. *See id.* at 16.
112. *See id.*

signatures.[113] E-mail was regarded as the least costly, however, arguably it is the easiest for a child to manipulate.[114] Another mechanism would require that the child print out a consent form for the parent to sign and return by fax to the company. Though this method proves costly, it is "least subject to falsification."[115] The use of credit cards may prove effective although some parents may not have or be willing to use a credit card online.[116] The use of digital signatures received overwhelming support, however, this technology has only recently become available.[117]

In drafting the Rule, the FTC had to balance the competing interests of a child's privacy and the financial capacity of Internet providers. The end result was the adoption of a sliding scale.[118] The sliding scale allows an operator to use varying consent mechanisms depending upon how the information collected will be used. For example, the scale allows a Web site that collects personal information from a child to verify consent via e-mail only if the information is used for internal purposes.[119] However, the Web operator must take additional steps to substantiate the parent's identity.[120] For instance, the Web site operator may phone or send a letter to the parent confirming his or her identity.[121]

For a Web site operator that plans to disclose collected information to a third party or post the collected information in general areas such as chat rooms or bulleting boards, the operator must use more rigorous means to obtain consent, such as requiring credit card verification. The FTC approved the following methods: requiring that the parent print, sign, and return a consent form; asking that the parent call a toll-free telephone number staffed by personnel for the Web site; requiring that the parent provide a credit card number; or asking that the parent provide a digital signature or an e-mail accompanied by a personal identification number (PIN) or a password.[122] The Rule retained the five exceptions to obtaining verifiable parental consent proposed in the language of the COPPA.[123]

The Rule also gives parents access to personal information that has

113. *See Children's Online Workshop*, *supra* note 94, at 15.

114. *See id.* at 39.

115. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,899 (1999).

116. *See* 16 C.F.R. § 312.5(b)(2) (1999); *see also Children's Online Workshop*, *supra* note 94, at 43 (statement of Ms. Sehgal-Kolbet).

117. *See* 16 C.F.R. § 312.5(b)(2).

118. *See id.* § 312.5.

119. *See id.*

120. *See id.* § 312.5(b)(2).

121. *See id.*

122. *See id.*

123. *See id.* § 312.5(c).

been previously collected by a child.[124] First, the Rule requires that the Web operator confirm that the person requesting the information is the child's parent or guardian.[125] Methods used to obtain parental consent can be used to confirm the requesting parent's identity.[126] An inadvertent disclosure of a child's information to someone other than the child's parent will not expose a Web site operator to liability under the COPPA provided that the disclosure was made in good faith.[127]

C. The COPPA's Shortcomings

When released in October 1999, both the Internet industry and privacy advocates applauded the FTC's Rule. However, one should ask whether the COPPA provides for the complete safety of children in the Internet world. Despite the thoughtful drafting by the FTC, the COPPA is not a panacea to the problem of a child's privacy online.

The COPPA protects children under the age of thirteen, leaving in the hands of industry self-regulation those children older than thirteen. This requirement varies from the Child Online Protection Act, which protects all children under the age of seventeen.[128] Many teenagers who access the Internet go unprotected by legislation even though teenagers actively participate in e-commerce and their use more frequently goes unsupervised.[129]

A second shortage of the COPPA is that it does not provide a private right of action to a victimized parent or child. The COPPA provides for fines imposed by the FTC and for action taken by the state. However, it is argued that any legislation directed at protecting an individual's privacy should provide for an avenue of action on behalf of or by the victim of such an invasion.[130]

Third, general audience Web sites do not have to comply with the COPPA, unless they have *actual knowledge* that the online user is a child under the age of thirteen.[131] Many general audience sites do not request the user's age for access to the site. As a result, when a child wanders away from children's sites, the COPPA' protection disappears.

---

124. *See id.* § 312.6 (1999).

125. *See id.* § 312.6(a)(3).

126. *See id.*

127. *See id.* § 312.6(b).

128. *See* 47 U.S.C.A. § 231 (1998).

129. *See US Teens Increase Online Shopping*, (visited Jan. 29, 2000) <http://cyberatlas.internet.com/big_picture/demographics/article/0,1323,5901_205961,00.html>.

130. *See* Allard, *supra* note 37, at 528; Gindin, *supra* note 4, at 1178.

131. *See* 16 C.F.R. § 312.3 (1999).

Last, how will detection of COPPA violators be conducted? Practically, detection will be costly and difficult. The Internet world is immense and constantly evolving. Web operators have access to the technology that will keep them one step ahead of any FTC action. In July, 1999, the CME conducted a brief survey of Web sites' practices directed at children.[132] After reviewing 155 sites, the CME found that "a disturbingly large number of children's sites are still collecting personal information from children without providing notification of their privacy policies or obtaining parental consent."[133] Of the total sites reviewed, eighty sites were regarded as the most popular children's sites.[134] The survey revealed that eighty-eight percent of those sites collected personally identifiable information, while less than twenty-six percent of the sites attempted to get any kind of parental permission.[135] Though CME conducted the survey before the enactment of the FTC's rule, the results highlight the industry's failure to carry out the requirements of the COPPA. This questions the effectiveness of the COPPA, and, if COPPA does not change the state of affairs, then what or how can children's privacy interests be protected from intrusion by Web sites. In the "privacy" discussion, two other solutions exist: internet self-regulation and filtering tools.

IV. ALTERNATIVES TO LEGISLATION TO PROTECT A CHILD'S PRIVACY ONLINE

A. Self-regulation and Industry Efforts Directed at Children's Privacy Concerns

In response to consumer demands and in order to thwart legislation directed at the Internet, the Internet industry has taken several measures towards protecting children online. In June 1998, the Online Privacy Alliance (OPA), a coalition of Internet industry groups, was created to deal directly with online privacy issues.[136] The OPA includes key players from the Internet world, such as American Online and Microsoft Corporation.[137] The OPA proposed Online Privacy Guidelines directed at the collection of

132. *See* Center for Media Education, *CME Assessment of Data Collection Practices of Children's Web Sites*, (visited Jan. 29, 2000) <http://www.cme.org/ministudy.html>.

133. *Id.*

134. *See id.*

135. *See id.*

136. *See Industry Privacy Alliance Recommends New Guidelines*, COMM. DAILY, June 22, 1998, at 4.

137. *See* Online Privacy Alliance, *Online Privacy Alliance Members* (visited Jan. 30, 2000) <http:www.privacyalliance.org/who>. By the end of 1998, more than 50 companies had joined the Privacy Alliance.

personally identifiable information.[138] These policies set forth by the OPA went "much further than any previous industry attempt to establish guidelines for the ways that companies collect and use private information."[139]

OPA also issued guidelines directed at dealing with children online users.[140] The OPA, while recognizing the "tremendous opportunities that the Internet provides for children," noted that the Internet presents "unique challenges for protecting the privacy of young children."[141] To meet this unique challenge, the OPA adopted several principles directed at protecting a child's privacy. Though these principles resemble COPPA's measures, they are more restrictive. For example, the Alliance's principles recommend a complete moratorium on offering free gifts in exchange for information.[142]

TRUSTe, a nonprofit organization, administers a seal program that regulates Web sites' collection of personal information.[143] The program requires that members or licensees disclose to users their information collection practices in exchange for the right to display a privacy seal on their Web site.[144] A TRUSTe member must disclose what information is collected, how the information will be used, and with whom the information will be shared.[145] TRUSTe requires that sites directed at children adhere to additional guidelines. TRUSTe prohibits a children's Web site from collecting, distributing, or permitting a child to post personally identifiable information "without prior verifiable parental consent."[146] TRUSTe currently has more than five hundred members.[147] The voluntary program involves third party monitoring and periodic reviews of a member site's privacy policies and practices.[148]

The Better Business Bureau Online (BBB*OnLine*), a subsidiary of the

138. *See* Online Privacy Alliance, *Online Privacy Alliance Members* (visited Jan. 30, 2000) <http://www.privacyalliance.org/about/privacypolicy.shtml>.

139. Miller, *supra* note 6, at D3.

140. *See* Online Privacy Alliance, *Principles for Children's Online Activities* (Jan. 30, 2000) <http://www.privacyalliance.org/kidsprivacy/>. The Alliance standard is leaps and bounds ahead of its peers.

141. *Id.*

142. *See id.*

143. *See Web Site Group Endorses TRUSTe Program to Protect Privacy of Internet Consumers*, 10 J. PROPRIETARY RTS. 17, 17 (July 1998).

144. *See* TRUSTe, *The TRUSTe Program: How It Protects Your Privacy*, (visited Jan. 26, 2000) <http://www.truste.org/users/users_how.html>.

145. *See id.*

146. *Id.*

147. *See id.*

148. *See id.*

Council of Better Business Bureaus, also maintains a privacy seal program.[149] In addition to requiring requires businesses that display the BBB*OnLine* privacy seal to notify users of their collection practices, BBB*OnLine* businesses must provide adequate data security, consent to periodic monitoring, and "use encryption for the receipt and transfer of sensitive information."[150] BBB*OnLine* members must also agree to participate in a consumer dispute resolution system.[151] Noncompliance with these policies result in the public reporting of decisions, suspension, or revocation of privacy seals.

The Children's Advertising Review Unit of Council of Better Business Bureaus (CARU)[152] analyzed Web sites' policies and practices and released new guidelines to address online advertising.[153] Most of the changes concern the collection of data from children. The guidelines for data collection state that advertisers should (1) notify children to ask permission; (2) disclose why information is being requested and whether it will be shared with a third party; (3) make reasonable efforts to offer parents opportunity to exercise choice; (4) disclose the past collection of information; and (5) when collecting identifiable information, make reasonable efforts for parental permission.[154]

Recently, informational Web sites have been created to educate users about privacy concerns. For example, Internet industry corporations introduced GetNetWise.[155] GetNetWise is a service that was created to provide information to help parents protect their online kids.[156] The Web site provides a parent with several resources, including an index of available online filtering programs and links to those sites that have privacy policies and include filtering software.[157]

149. *See* BBBOnLine, *How the Privacy Program Works*, (visited Jan. 26, 2000) <http://bbbonline.com/businesses/privacy/self-regulation.html>; BBBOnLine, *BBBOnLine Privacy Seals*, (visited Jan. 26, 2000) <http://bbbonline.com/about/about_seals.htm> [hereinafter *BBBOnLine Privacy Seal*].

150. *BBBOnLine Privacy Seals*, *supra* note 149.

151. *See id.*

152. The National Advertising Review Council established the CARU in 1974.

153. *See* Birenz, *supra* note 38, at 487.

154. *See* Better Business Bureau Advertising Review Programs, *Self-Regulatory Guidelines for Children's Advertising* (visited Jan. 30, 2000) <http://www.bbb.org/advertising/ caruguid.html>; *see also* Campbell, *supra* note 36, at 341, n.188.

155. *See GetNetWise*, *supra* note 7.

156. *See id.*

157. *See id.*

B. Adequacy of Internet Self-regulation

Industry efforts demonstrate that Internet businesses are taking action in response to consumer concerns about privacy protection. Through further efforts such as those already taken by the OPA and the providers of GetNetWise, arguably the Internet will become a safer place for children. With regard to adult users, industry self-regulation has been cited as the "least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[158] However, critics of self-regulation point out that there is no assurance that Web operators will comply with their own privacy standards. Though the incentive to protect a user's privacy exists, industry efforts, such as seal programs, currently fail to provide an effective means of enforcement to guarantee compliance with their guidelines.[159] Only a small majority of Web providers participate in seal programs.[160] Seemingly, the results of the recent survey conducted by the CME prove that the Internet industry is behind in ensuring the safety of young users online. Though the industry is the current overseer of an adult's privacy online, due to the vulnerability of children online users and the incredible incentive to collect personal information from children, the Internet industry should not be relied upon as the sole defender of a child's privacy.

C. Filtering Software

In response to the concerns of a child's access to objectionable content on the Internet, many software developers designed filtering software to provide supervising adults with control of a child online user's access to certain content on the Internet. Recently, and in response to concerns of children's privacy online, filtering software has been adapted to protect an individual user's privacy.[161]

Filtering software aimed at protecting the user's privacy screens both incoming and outgoing text. The use of specific terms, such as names, addresses, birth dates, and credit card numbers, triggers the outgoing screening.[162] The software prevents the information from being sent to the provider.

There are numerous programs that are currently available to prevent a child from providing personal information to a Web site. For example,

158. *Report to Congress*, *supra* note 3, at 6.
159. *See* Allard, *supra* note 37, at 528.
160. *See Report to Congress*, *supra* note 3, at 12.
161. *See Staff Report*, *supra* note 5, at IV.C.1.
162. *See id.*

Cybersitter, NetNanny, CyberPatrol, and Specs for Kids offer privacy preferences.[163] Also, some have additional features. For example, Cybersitter provides an option to filter access to chat rooms, e-mail, and games.[164] The software screens both incoming and outgoing information. The software can prevent the transfer of personal information such as a credit card number. Net Nanny offers the same features as CyberSitter and provides complete control to a supervising adult.[165]

D. Adequacy of Filtering Software

Filtering software can be an effective and useful tool to prevent the unsolicited collection of a child's personal information.[166] Filtering software empowers the parents of the child to regulate a child's experience online. Because parents are in the best position to determine to what extent their children should be allowed to participate in certain online activities, filtering software is arguably more attractive than legislation that dictates age restrictions. Furthermore, filtering software provides parental control without requiring that the parent release any personal information about themselves or their child. Filtering software protects the unsupervised child online.

The avid online child user can easily manipulate some filtering programs. For example, depending on how the information is entered, it is possible that the software would permit certain information to pass. Blocking software also might restrict a child's access to only a few sites, thereby hampering what could be a valuable online experience. Given the nature of technology and how quickly it changes, manufacturers must continuously update filtering software to keep up pace with information collection technology.

V. NECESSARY PARTICIPANTS TO THE PROTECTION OF A CHILD'S PRIVACY ONLINE

Thus far, the discussion has demonstrated that the methods recognized as potential solutions to the problem of the unsolicited collection of a child's personally identifiable information suffer from shortcomings. Because COPPA violations are difficult to detect, the goals of the COPPA may never be fully achieved. Furthermore, the Internet industry has demonstrated its reluctance to abide by COPPA standards even as of late last year. Filtering software offers sufficient protection,

163. *See id.*
164. *See id.*
165. *See id.*
166. *See* ACLU v. Reno, 942 F. Supp. 824, 842 (1996).

however, only for those parents who know of its value and existence. Given these shortfalls, children remain unprotected while exploring the world of the Internet. Regardless of the existence and sufficiency of the COPPA or industry guidelines and coalitions, this Note proposes that the one group in the best position to protect a child's information online has been excluded from the "privacy" discussion: parents.

While the Internet progresses toward respecting its young users' privacy, the FTC, armed with the COPPA, looms in the background should misconduct occur. Unfortunately, neither the FTC nor the industry can guarantee that children will not journey away from sites dedicated to them, easily provide personal information to any requesting site, or post information on a bulletin board. As a result, it is time to call on parents to provide online protection where the COPPA and the Industry cannot. This proposal seems relatively obvious, yet many have overlooked the important function that parents serve. In fact, absent participation by parents, even the strongest legislation or industry action will not secure a child's privacy online.

Only informed parents can effectively ensure that their children's information is safe. Thus, protecting a child's privacy online would first require educating parents about the dangers their children confront in the Internet world. However, this education is not only for those Internet literate parents. The education would consist of a campaign, such as that begun by GetNetWise, to alert parents about the information collection practices and the resulting risks. Arguably, the COPPA's requirement of verifiable parental consent will serve to involve and alert parents of the children's web sites' practices. However, that assertion is premised on the assumption that all children's web sites will comply with the COPPA and that children will not effectively evade that requirement. Because such assumptions are currently in doubt, parents must be notified in addition to and in spite of the existence of the parental consent requirement.

The proposal does not require the constant supervision of a child's Internet use. It only requires that parents direct their children to proceed wisely in the Internet world. Very simply, the lesson is a familiar one: "Don't talk to strangers <online>!"[167] Instead of the unknown individual on the street, the stranger is the Internet. As a result, a child should be leery any time the "Internet" requests that a child disclose personally identifiable information. For older children, a more elaborate lesson may be in order given that they may recognize the potential dangers more readily. For example, there are certain precautions they may take, including: using a

167. *See also Staff Report*, *supra* note 5, at II.C.2.

false name and address when providing personal information to gain access to a site or game; avoiding posting personal information on a bulletin board or in a chat room; and selecting a screen name that does not provide any personal information.

This Note does not advocate that parents should be totally accountable for their children's activities online, as it is web operators that are the proven bad actors. However, because the effectiveness of legislation and Internet Industry guidelines remain to be seen, parents should not sit idly and presuppose their children's security online. Even though they may be the only remaining option, parents are in the best position to protect a child's personal information from being released online. The proposal is not fool proof. Certainly, the mere inclusion of parents will not *end* the release of information by children, the misuse of that information, or even the prey of children by online predators. Nevertheless, by excluding parents, a necessary party to the privacy discussion, the future of a child's safety online looks bleak.

VI. CONCLUSION

The Internet is no doubt a valuable tool that serves endless purposes for both children and adults. However, both children and adults are susceptible to the customary practice of collecting personal information of users online without that user's knowledge or consent. While adults remain unprotected from such a practice, Congress set out to ensure the security of an online child's personal information with the passage of the COPPA. In a fruitless effort to thwart legislation and in response to consumer concerns, the Internet industry also has made an effort through seal programs and coalitions dedicated to protecting children's information online. In addition to legislation and Internet industry guidelines, software has become available to prevent the collection of personal information from an online user. Filtering software provides parents with complete control of their children's online use.

Given the many ways that currently secure a child's online journeys, one would guess the mission is complete. However, children remain inadequately protected. Their information continues to be collected or released without their parent's knowledge or consent. Naturally, such a state of affairs begs the question: Can children be completely secure online? The answer remains to be seen. However, this Note suggests that the answer will never be affirmative unless we include a necessary party to the group of already existing resources: parents. If legislators and the Internet share their information with parents, then parents will be as driven in the effort to protect their children online. In fact, no matter how strict

industry guidelines are or how effective filtering software is, there is no substitute for putting valuable information in the hands of the parents who can then assure that their children are safer online.

Accordingly, to effectively protect a child's safety online, both sides of the computer necessarily must act. The industry must continue the efforts of protecting online privacy and children, educated by their parents, must conduct themselves carefully online. While the industry continues to demonstrate its reluctance to behave accordingly, hopefully, parents, who are in the best position to address the problem, will act hastily.