Comments of the New York Intellectual Property Law Association
Privacy Law Committee
Chairman: Jonathan Moskin
Foley & Lardner LLP
Dated: New York, New York December 23, 2011

On September 27, 2011, the Federal Trade Commission ("FTC") published proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule"). The Privacy Law Committee of the New York Intellectual Property Law Association[1] provides the following comments directed to the parental consent provisions (16 C.F.R. § 312.5)

The statute defines ''Verifiable parental consent'' as ''any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure, described in the notice.'' 15 U.S.C. §6501(9) The current COPPA Rule provides that operators:

> must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent.

16 C.F.R. § 312.5(b)(1). Among the contemplated amendments to the current methods of obtaining verifiable parental consent set forth in 16 C.F.R. § 312.5(b)(2), the FTC proposes dropping the so-called sliding scale approach. The FTC also proposes, in addition to the current rule allowing an operator to have a parent use a credit card in connection with a transaction, also "allowing operators to collect from the parent a form of government-issued identification, such as a driver's license, or a segment of the parent's social security number, provided the operator verifies the parent's identity by checking this identification against databases of such information, and provided that the parent's identification is deleted by the operator from its

[1] The "NYIPLA" is a professional association of more than 1,500 attorneys in the United States and abroad whose interests and practices lie in the area of patent, copyright, trademark, trade secret, privacy and other related areas of law. NYIPLA members include in-house attorneys working for businesses that own, enforce and challenge intellectual property interests and privacy matters, as well as attorneys in private practice who represent both intellectual property owners and accused infringers. NYIPLA members frequently engage in intellectual property licensing matters, and issues concerning marketing and other business conducted on-line, as well as ownership of intellectual properties, trade secrets and privacy rights. The NYIPLA further strives to educate the public and member of the bar in the field of intellectual property law and continually works with foreign associations to harmonize international law in this field. NYIPLA members and in particular its Privacy Law Committee, represent both plaintiffs and defendants in developing and protecting cutting edge technologies including emerging communications technologies that give rise to the kinds of privacy concerns that arise under the COPPA rule. As a result, the NYIPLA has a strong interest in the meaning and application of privacy laws applied online and in connection with such technologies.

records promptly after such verification is complete." In both respects, the NYIPLA believes the proposed rulemaking should be reconsidered. Indeed, as discussed below, the NYIPLA is concerned that, in these respects, and no doubt unintentionally, the proposed new COPPA rules risk sacrificing *parental* privacy in the name of safeguarding *children*.

The NYIPLA initially notes that there is no perfect method for obtaining verifiable consent in the anonymous context of the internet. Children at increasingly younger ages (perhaps aided by older siblings, friends or others) are becoming ever-more proficient at using electronic technologies and social media. As a result, there may be no effective means to safeguard all such children from bad actors that collect information from the most vulnerable of internet users, nor can any general rule anticipate all specific means of evading such safeguards if children are determined to do so. In short, there can be no automatic or electronic substitute for actual and effective parental supervision. (Even actual and direct parental supervision is, alas, at best an imperfect tool, even under the best of circumstances.) Indeed, often the most that can be done in situations where children seek to evade parental, practical or legal controls is to impose mandatory delays or waiting periods to limit the risks of impulsive behavior by unsupervised children. For instance, often the greatest temptation to engage in "risky" behavior on-line is in group situations (such as a party or other gathering) or on-line group situations (such as Facebook-style instant messaging and public posting of comments within a group or internet chat rooms or similar platforms featuring broad-based instant messaging). In all such instances, peer pressure may encourage children to act irresponsibly.

Moreover, the NYIPLA believes the greatest risks to children arise, not from the likely majority of responsible businesses, which recognize the risks of legal liability (or even threatened liability) or negative publicity from perceived violations of public norms, but rather, from unscrupulous or careless merchants (or, worse, entities merely posing as merchants). The proposed rule change appears likely to chill legitimate online behavior, while having little overall impact on the conduct of such "bad actors." Moreover, the rule change would result in more, not less, personally identifiable data being collected online, increasing (not decreasing) the potential sources of privacy violations and security breaches. As a result, and consistent with other general principles advanced by the FTC, the NYIPLA believes that all forms of data collection should be minimized, particularly where such data is collected from children.

With these observations in mind, the NYIPLA believes that encouraging operators to collect from children their parents driver's license numbers or other government-issued identification numbers, or a segment of the parent's social security number, should be reconsidered. Indeed, the NYIPLA entertains doubts as to the propriety of the existing rule encouraging "parental" credit card transaction to serve as a form of verifiable consent. Children sophisticated enough to seek to evade parental consent requirements are likely savvy enough to know where and how to obtain parental credit card information, driver's licenses or the like (thus calling to mind the infamous 1965 incident in which the television comedian, Soupy Sales, encouraged his young viewers to send in the little green papers in their parents' wallets). It may well be that children are less likely to know where or how to find a parent's social security number, but if they do, there is also reason to be concerned that children will not appreciate the sensitivity of such information. (Parents themselves are often ignorant of or inattentive to the risks of sharing such personally identifiable information online.) As such, given the opportunity, children may

without hesitation disclose a parent's entire social security number, even if best practices recommended by the FTC were to limit the necessary information to the final four digits. As the FTC notes, there is a great potential for children to have "easy access to and use of alternative forms of payments (such as gift cards, debit cards and online accounts.)" We submit that children likewise often have ready access to their parents' wallets, and that children who are inclined for whatever reason to try to evade online parental controls should not be encouraged to sacrifice their parents' privacy by seeking out and disclosing such information.

Even if the parent is a willing participant in the process, the NYIPLA believes that parents' privacy rights should not needlessly be put at risk so as to protect the privacy of their children. Indeed, although the FTC proposes that operators be required to delete social security numbers or other parental data immediately, the mere act of collecting such data raises security issues, and not all internet operators can be expected to comply completely with such a rule. Moreover, once such operators have been encouraged to obtain such personally identifiable information, there is good reason for even the most scrupulous of internet operators to want to retain such information: precisely so that they can defend themselves from potential charges of failing to observe parental consent requirements. It is not clear how the FTC contemplates that operators will be able, later, to verify compliance in the first instance once the information has been deleted. Moreover, because the far greater concern arises from the conduct of less-scrupulous internet operators, collecting such personally identifiable information of the parent under the imprimatur of compliance with FTC regulations simply invites abuses. Once again, parental privacy should not be sacrificed in the name of protecting children and, in particular, should not be placed in the hands of children seeking their own immediate gratification.

For many of the reasons set forth above, the NYIPLA further believes that the current sliding scale approach to parental consent (so called "email plus") should be retained (if perhaps in slightly modified form). Bearing in mind that limiting impulsive behavior is one of the greatest benefits of the parental notification procedures, and further considering that parental privacy should not be sacrificed needlessly for the sake of protecting children, the current "email plus" system is a practical, if admittedly imperfect, solution to a problem for which no perfect solution may exist. *Delaying* collection of personal information from a child until a letter is received signed by the parent (even if forged) or pending receipt of delayed email confirmation (once again, even if provided surreptitiously by the child) creates an obstacle to immediate risky behavior, whether at the urging of peers or for any other reason. Similarly, requiring telephone confirmation with a putative adult (even if the rule is susceptible to evasion) creates a significant barrier – particularly if the telephone call center personnel are appropriately trained. Equally important, the separate step (especially if the separate step is also conducted at a time removed from the initial request by some span that the child can not predict or anticipate) makes it vastly more difficult for a child to "game" the system. To be sure, a child can create a false parental email account or phony street address, but no system envisioned by the FTC can provide a complete guarantee – particularly if the child whose interests are to be protected is sufficiently sophisticated to conceive and carry out such schemes. Moreover, each such method permits the operator to create and retain a record of compliance that can be verified at a later date, and does so without raising separate security issues by requiring retention of sensitive personally identifiable data.