December 23, 2011

FILED ELECTRONICALLY

Federal Trade Commission
In the Matter of the COPPA Rule Review
16 C.F.R. Part 312, Project No. P104503

Comments of LifeLock, Inc.

LifeLock, Inc. ("LifeLock") appreciates the opportunity to respond to the Federal Trade Commission's ("FTC") request for comments on proposed amendments to the Children's Online Privacy Protection Rule (''COPPA Rule'' or ''Rule'').

We commend FTC on its efforts to update the COPPA framework to protect children and meet the privacy challenges of the twenty-first century while supporting beneficial uses of information and technological innovation. Due to continuing changes in the manner by which children view and interact with online content, it is high time to review, improve and streamline for parents' benefit these online privacy protections. As the FTC is all too aware, identity theft remains the top list of consumer complaints to the FTC. Identity thieves are savvy and understand where and with whom they can be most successful. Unfortunately, this success often comes at the hands of children under the age of 13. And, the abuse of children's personal information often goes on for long periods of time.

As such, we limit our comments on the proposal's parental notice provision. As the Commission observes, a linchpin of the COPPA rule is its parental notice requirements. Protecting children requires offering parents clear and complete notice of operators' information practices. Informed consent is key. The great majority of notices, however, tend to be lengthy, complex and opaque. LifeLock is not commenting on FTC's proposed update to the "personal information" definition, parental consent mechanisms, confidentiality and security requirements or safe harbor.

LifeLock proposes the use of a simplified two-step approach that promotes transparency and establishes baseline privacy principles. The first step is a simple, standardized and transparent rating system. We believe the use of colors or numbers to indicate the risk level associated with data collection and use practices would provide parents with the most effective notice. Second, we urge the development of standardized privacy notice elements developed with industry input. These notice elements would be standardized bullet points that explain data collection and use practices in a clear and effective manner. Taken together, these actions would modernize the COPPA protections and offer the greatest protection to children under 13.

I. About LifeLock

LifeLock provides a wide range of privacy protection services to consumers, including identity theft protection and data breach response services. Headquartered in Arizona, LifeLock's 300 agents help our members keep their identities safe 24 hours a day. We have a strong focus on educating consumers and working with policymakers to better understand the increasing threats of identity theft.

For example, on July 12, 2011, we attended *Stolen Futures*, a forum on child identity theft co-sponsored by the FTC and the Department of Justice's Office for Victims of Crime. LifeLock also attempts to proactively combat identity theft through a partnership with the nonprofit FBI Law Enforcement Executive Development Association (FBI-LEEDA) and National Crime Prevention Council (NCPC). Working with FBI-LEEDA and NCPC, LifeLock hosts summits open only to elected officials and law enforcement. The one and two-day events, attended by chiefs, sheriffs, investigative supervisors, fraud unit investigators, patrol officers, community policing personnel and special agents, address a range of identity theft issues, including laws, new technologies, awareness and protection strategies, investigative techniques, databases to assist in identity theft investigations and victim's assistance.

II. The Historical Landscape of COPPA

In a 1998 report to Congress, the FTC noted that while parents instruct children to avoid speaking with strangers, that message sometimes fails to apply online.[1] Then, children used the internet for a wide variety of activities, including homework, informal learning, browsing, playing games, corresponding with pen pals, posting on boards and participating in chat rooms. In 1998, almost 10 million (14%) of America's 69 million children were online, with over 4 million accessing the Internet from school and 5.7 million from home.

Through COPPA, Congress, the Clinton Administration and the FTC focused their attention on protecting the privacy of children under 13 as they visited commercial websites. The Act has helped safeguard young consumers from aggressive marketing environments. As the law took effect in the formative period of the internet, it wisely was designed to adapt to changes in both technology and business practices. With the current expansion of digital media platforms and the growing sophistication of online data collection and profiling, however, it is now critically important that the intent of COPPA be fully implemented to protect young people from new commercial practices in today`s digital media environment.

---

[1] *See* Privacy Online: A Report to Congress (Federal Trade Commission, June 1998) available at http://www.ftc.gov/reports/privacy3/toc.shtm.

And today's digital media environment continues to explode. A recent Kaiser Family Foundation report documented expansive internet and cell phone usage.[2] While younger children—those in the 8 to10 year-old age range—spend the least amount of time with computers, they still average 46 minutes in a typical day. The amount of time spent with computers jumps by an hour for 11 to 14 year-olds. Likewise, with cell phones, five years ago the market for young people was small. Today, two-thirds of all 8 to 18 year-olds own their own cell phone.

This market penetration may be contributing to the substantial increases in stolen identities of children. In April, the Carnegie Mellon Cylab scanned the identities of more than 42,000 U.S. children to determine identity theft exposure.[3] Key findings of the report include: 4,311 or 10.2% of the children in the report had someone else using their Social Security number; child IDs were used to purchase homes and automobiles, open credit card accounts, secure employment and obtain driver's licenses; the largest fraud ($725,000) was committed against a 16 year old girl; the youngest victim was five months old and 303 victims were under the age of five. The 10.2% of impacted children stands in stark contrast to adult ID theft rates – the scanned children's rate was fifty-one times higher than adults in the same population over the same period.

LifeLock strongly agrees with FTC that children's judgment is not improving as technologies grow and utilization increases. In addition, online and mobile marketers continue to employ practices that jeopardize the integrity of children's identities. As FTC noted during a September 2011 hearing before the House Ways and Means Committee, controlling and limiting access to a child's information is one of the best ways to protect children from identity theft.[4] While parents are responsible for monitoring how their children use the internet and transfer information, updating the COPPA rule can help parents protect their children's identities without unduly burdening business.

III. The Proposal: Rating System and Standardization of Privacy Notices

A focus of FTC's proposed amendments is the need for streamlined and easy to understand notice requirements for parents. The Commission is proposing to streamline the current notice requirements in an effort to give parents information real-time basis. In specific, the FTC proposes that parents would receive notices through "just in time" messages that describe an operator's information practices at the most relevant points of interaction. The proposed revisions further describe the precise information that operators must provide to parents regarding: (1) the personal information that the operator has already obtained from the child; (2) the purpose of the notification; (3)

---

[2] *See* Generation M2: Media in the Lives of 8 to 18 Year Olds (Kaiser Family Foundation, January 2010) available at http://www.kff.org/entmedia/upload/8010.pdf.

[3] Child Identity Theft: New Evidence Indicates Identity Theft Thieves Are Targeting Children for Unused Social Security Numbers (Carnegie Mellon CyLab, April 1, 2011) available at www.cylab.cmu.edu.

[4] Child Identity Theft Field Hearing Before the House Ways and Means Committee, 112th Cong. (Sept. 1, 2011) (statement of Deanya Kueckelhan, Director of the Southwest Regional Office of the Federal Trade Commission).

actions that the parent must or may take; and, (4) how the operator intends to use the personal information collected.

LifeLock applauds the Commission's streamlined and easy-to-understand approach. Privacy policies are too long and difficult to understand. In addition, written policies may not even be the most effective way to communicate salient privacy information to parents. To further facilitate the need for clear and concise descriptions of information practices, LifeLock proposes a two-step approach. First, we propose a standardized, color-coded and numbered privacy seal or icon system. This would make immediately apparent to parents whether data may be transferred to a database of information used to compile individual profiles. For the greatest effectiveness, the privacy seal or icon should be prominently presented on the home page of the website and near the request for information. The seal or icon would also map to the key features of the privacy framework. For example, a proposed "1" or green seal/icon would apply to sites that do not disclose children's data; a proposed "2" or yellow seal/icon would indicate that information is disclosed requiring parental approval but that disclosure does not lead to wide proliferation or individual identification; and, finally, a proposed "3" or red seal/icon that indicates information is made available for sale.

Second, LifeLock proposes the tiered rating system be augmented by standardized and easy to understand language. This simplified language would appear when the user clicked on the icon or seal or on the next page of a written notice. LifeLock recommends standardized bullets describing collection, use and disclosure, rather than longer, standardized privacy notices. Again, the standardization of privacy notices is far too complex and difficult to achieve in a short period of time. This approach is much easier than standardizing privacy notices, and the bullets can be modeled after the FTC's proposed standardized descriptions.

IV. Conclusion

LifeLock is all too familiar with the impact on children and families when identities are comprised. As children under the age of 13 won't be applying for credit to buy a car or receive a credit card for years, those children who suffer from identity theft may wrestle for decades with phony lines of credit and debt. Since 2000, the Children's Online Privacy Protection Act has helped protect the identities of children. Enacted during the advent of sophisticated internet marketing, the act allows for flexibility in both technologies and business practices. With children under the age of 13 now regularly using mobile technologies and the internet, the FTC has wisely sought to utilize its authority to renew and revitalize COPPA's effectiveness. It is critical that parents are afforded clear and concise notices how operators and third parties will utilize information on children under the age of 13.

We thank you for considering our views, and are eager to continue to work with you in a constructive fashion to help implement COPPA's goals and protect the identities of children under 13.