BEFORE THE
FEDERAL TRADE COMMISSION

In the Matter Of **Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule**		**Re: COPPA** **Rule Review P104503**

COMMENTS OF AT&T INC.

AT&T Inc., on behalf of itself and its affiliates ("AT&T"), respectfully submits these comments in response to the Federal Trade Commission's ("FTC" or "Commission") Notice.[1] AT&T supports the Commission's commitment to review and improve implementation of the Children's Online Privacy Protection Act ("COPPA Rule") Rule. AT&T is pleased to continue its participation in the Commission's ongoing dialogue regarding privacy matters in general and, in particular, the roles that all stakeholders – including government officials, industry leaders, public interest groups, parents, and, not the least, children themselves -- can and should play to help ensure the protection of children's online privacy.

[1] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, P104503,75 Fed. Reg. 17089, 17093 (2010) ("Request for Comment").

At the outset, AT&T notes that the COPPA Rule has been an effective mechanism for protecting children's privacy in the face of the significant technological change that has occurred since COPPA first became effective on April 21, 2000. The COPPA Rule has helped to ensure that information is not knowingly collected from children by websites and online services without parental consent, and has contributed to the development of significant educational efforts directed toward the protection of children's privacy and promotion of online safety goals.

And while much has indeed changed since the initial COPPA Rule was adopted – and even since the last COPPA Rule review in 2008 – COPPA remains an important tool for protecting the privacy of children using the Internet. Since the FTC's last review, there are more and more ways to access the Internet (including an ever-increasing number and variety of wireless devices), more to do online once you get there, and more opportunities for individuals to share information. Interactive games and movies, social networking services and other interactive media have created new opportunities for data collection from the increasing number of children utilizing the Internet. Therefore, in order to ensure that the COPPA Rule continues to advance its statutory mission, we recognize that it is appropriate for the FTC to periodically review its efficacy in light of changes in the Internet marketplace. Given the ever-increasing number of new players entering the Internet marketplace, at a minimum this review will help raise awareness regarding existing COPPA obligations.

AT&T believes COPPA and the COPPA Rule remain and will continue to remain effective as written, even in the face of constant technological changes in the way users access the Internet and online services, precisely because COPPA is structured to focus on the collection of data from children *without regard* to *the manner in which the child has accessed a given website or online service.* Online service providers are obligated to comply with COPPA

requirements governing the collection of data from children regardless of any new platforms, devices or technology protocols that enable the underlying Internet access. As a result, changes in technology do not require changes to either COPPA or the COPPA Rule. Both will remain effective to protect children's online privacy without need of change.

In this regard, many of the questions posed in the FTC's Request for Comment deal with threshold definitional issues that arise from the statutory language – such as whether a particular technology falls within the definition of the "Internet," or whether certain items of information should be itemized in the definition of "personal information." Because rigid definitions will not keep pace with technological change (one of few certainties in today's world), the flexible language of both the statute and the COPPA Rule remain preferable to a more piecemeal definitional approach. For example, the definition of "Internet" as provided in the statute is sufficient to encompass online services or applications accessed via mobile devices or interactive gaming, and other similar interactive services. The online services and websites provided by or made available via these technologies are fully subject to the COPPA Rule, and providers of these services may not knowingly collect personal information from children under 13 without complying with COPPA restrictions. As such, we believe the definition is more than adequate as written to place industry participants on notice of their obligation to ensure the online collection of personal information from a child is treated in accordance with the requirements of the COPPA Rule.

Similarly, the term "Personal Information" is well defined by the statute, and gives the Commission flexibility to determine whether a particular piece of data falls within its scope. In particular, the definition of Personal Information is broad enough to include "mobile geolocation data" or any other sensitive data that becomes relevant in the future, when such data is combined

with individually identifiable information like name or mobile phone number.[2] So, for example, an application service provider may not knowingly collect mobile geolocation data combined with cell phone number from children under 13 without complying with COPPA restrictions.[3] AT&T acknowledges, however, that the use and collection of location information by websites and online service providers is a relatively new phenomenon since the FTC's last COPPA review and presents a number of complicated technical and technological issues that should be thoroughly understood and resolved before any more specific requirements are added to the COPPA Rule. AT&T therefore recommends that the FTC first fully engage all stakeholders to better understand the different ways mobile geolocation information is being collected and used today – and any unique issues that use may pose for children – as well as the protections already in place or in the process of being developed[4] – prior to taking any action in this area.

Developments in wireless Internet access appear to be one of the primary concerns behind this review of the COPPA Rule, and certainly it is true that mobile Internet access has and will continue to increase, both in terms of the devices that provide such access and the use of

---

[2] The term Personal Information includes "information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition." *See* 16 C.F.R. § 312.2.

[3] It should be noted that although AT&T offers parents the ability to set up a family account for wireless service, this information is purposely controlled by the account holder as an account management tool. AT&T has no knowledge which family member is associated with a particular device or telephone number on that account, nor does AT&T have any way to make that determination or, perhaps most importantly, to verify the accuracy of that information.

[4] AT&T has voluntarily adopted strong protections for subscriber location information. *See* AT&T Privacy Policy, available at: *w*ww.att.com/gen/privacypolicy?pid=13692#location (Questions about Location Information). Additionally, CTIA has developed Best Practices and Guidelines for Location-Based Services in order to set benchmarks for the mobile Internet ecosystem in a technology-neutral way. *See* CTIA, *Best Practices and Guidelines for Location Based Services* (2010) *available at* http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf .

those devices by more people, including youth. However, as noted above, both the statute and the COPPA Rule place the relevant obligations on website and online service providers, regardless of the access technology. Therefore, the COPPA Rule continues to apply to the collection of data from children by websites and online services (including applications) accessed via mobile devices.

The manner in which the market for selling mobile devices has evolved also provides parents with safeguards to protect their children from unwanted data collection. In particular, parents have a meaningful opportunity to exercise control over the online privacy of their children at the outset through the decision to provide a mobile device to their children and, ultimately, whether and to what degree that device is Internet enabled or otherwise able to access applications or other online services. Because parents must purchase the device and the accompanying mobile service on behalf of their child, they have the ability to select a device and type of service they believe to be appropriate to the age of that child – ranging from a device with no Internet access or access to online services at all, to one with full Internet capabilities.

AT&T has long been committed to developing and providing our customers, and parents in particular, access to control tools across each of our service platforms that enable them to customize and manage their own service experience for themselves and their families. For example, AT&T Smart Limits for Wireless™, which allows parents, through an easy online setup, to establish a variety of limits on how and when their children can use their wireless phone. Among other things, parents have the option of limiting the number of text and instant messages children may send and/or receive, determining who the device can call or text by blocking and allowing certain number, limiting the amount of web-browsing allowed per billing cycle, and limiting access to content inappropriate for children.

The ability to limit Internet access provides some privacy protection in that it curtails the opportunity for children's personal information to be collected. The "privacy by design" approach advocated by AT&T and others would continue to improve on existing access controls by creating an environment in which privacy tools are integrated features of Internet products, enabling parents to exercise meaningful control over online data collection for both themselves and their children. The FTC has and should continue to foster the development of privacy control tools, with a focus of making those tools an integral attribute of *any* online service – not just those directed toward children or ones for which the operator has actual knowledge that information is being collected from children. By ensuring that children's privacy is built as an integral attribute of the online experience, rather than treated as a compliance mechanism and made available only when operators think they might be subject to statutory penalties, the FTC would help to engender an environment in which privacy is truly protected, and both parents and children can have confidence and trust in the online environment.

Thanks in many ways to the involvement of the FTC, work on privacy tools is progressing. As we have seen with the widespread proliferation of parental controls made available by providers at all parts of the Internet ecosystem,[5] it is important that all stakeholders in the online environment continue to focus on the development and improvement of privacy-focused tools designed to assist parents in establishing a level of control over their child's online experience they consider appropriate – including the ability to limit the amount of data collected about their children. Today, there are a number of technologies – browser controls, widgets and

[5] See, e.g., Parental Controls & Online Child Protection: A survey of Tools and Methods, Version 4.0, Adam Thierer at http://www.pff.org/parentalcontrols/

downloads – that offer consumers the ability to set and manage their privacy preferences. These technologies provide numerous privacy benefits to consumers, but can and should be improved upon. [6] An area of strong potential and one AT&T fully supports is the further development of user-centric identity management tools ("IDM tools") and the establishment of an interoperable trust framework for the internet. The *National Strategy for Trusted Identities in Cyberspace* report due to be finalized in October 2010 [7] creates a meaningful and timely opportunity to ensure that the development of this trust framework includes capabilities for parents to control the collection of information from children online. The FTC should work to ensure that this effort, which has historically focused on traditional identity theft issues, addresses children's privacy concerns, including the development of user-friendly tools and interfaces that could potentially have numerous benefits for parents and children, including:

- Offering parents the ability to control all identity-based interactions between websites and online services with their children;
- Enhancing children's privacy by providing parents with a single place to establish privacy preferences, the ability to minimize disclosure of personal, identifying information, and greater choice regarding the nature and amount of data to be shared, when it will be shared, and the timing and manner of updating and withdrawing data;
- Providing websites a secure, standardized means of authenticating users; and

[6] And, it should go without saying that technological enhancements to privacy controls must provide an effective means of control. In evaluating the promise of various technologies than can be leveraged by parents and the industry, the FTC should take note of the thorough review of technological solutions conducted by the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States. The Task Force did an extensive review of many of the technologies discussed during this COPPA proceeding. For instance, the Task Force concluded that "age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. " See. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_D_TAB_and_EXHIBITS.pdf

[7] The White House released its draft National Strategy for Trusted Identities in Cyberspace on June 25, 2010. It stated that it expects a final report to be issued in October 2010. The draft report can be found at http://www.whitehouse.gov/the-press-office/fact-sheet-national-strategy-trusted-identities-cyberspace

- Giving website and online service providers a uniform means of determining children's privacy preferences as set by parents.

Finally, we believe that, in addition to helping to promote the development of tools to empower parents and children to protect their privacy, educational efforts are critical. The FTC is well positioned through its existing privacy and online safety initiatives, as well as through its ongoing work with industry, to raise awareness about COPPA requirements, particularly with relatively new sectors of the industry such as applications developers, and to inform parents and children about protecting their online privacy. Such educational efforts are crucial to increasing parental understanding and control over the online collection and use of both their personal information and that of their children.

Respectfully submitted,

Keith M. Krom
General Attorney and Assistant
General Counsel
Legal - Washington
AT&T Services, Inc.
1133 21st Street, N.W.
Suite 900
Washington, D.C. 20036
Counsel for AT&T Inc.

Date: July 12, 2010