April 2, 2012

Lawrence E. Strickling
Assistant Secretary for Communications and Information and
Administrator, National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, DC 20230

Comments Submitted by Symantec Corporation
pursuant to
NTIA Docket No. 120214135–2135–01, RIN 0660–XA27
Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

Dear Assistant Secretary Strickling:

Symantec Corporation appreciates the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA) Request for Public Comments on the "Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct."

As a global leader in providing security, storage, and systems management solutions, Symantec is committed to assuring the security, availability, and integrity of our customers' information. The protection of privacy and personal data is a top priority for us. Today, we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives an unparalleled view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing and spam.

Symantec is pleased to provide input both into the implementation of the multistakeholder process and to the substance of what this effort should address. Now more than ever, increasing amounts of information is transmitted, processed, shared, and stored across electronic networks. This new era brings with it new opportunities – and new challenges – for the privacy and security of personal data. The President's framework recognizes this reality, and we appreciate that it looks to the private sector to take the lead in developing an enforceable self-regulatory regime.

The March 5, 2012 Federal Register Notice requested comment in two areas: **Consumer Data Privacy Issues to Address Through Enforceable Codes of Conduct** and **Implementing the Multistakeholder Process.** Because we believe that the latter question informs our response to the former, we will address the two areas in that order.

Implementing the Multistakeholder Process

We are pleased that the foundation of this effort is involvement with the private sector; it will only be successful if the codes of conduct produced are the result of a shared effort. A proscriptive or top-down approach that fails to incorporate the views and concerns of those who will have to abide by the codes is likely to be rejected by citizens or companies – or both. Moreover, such a rigid approach would not adapt with the constantly evolving technological landscape, and could paradoxically increase vulnerabilities while stifling new business models and innovation. And while it is unlikely that the codes will be able to satisfy fully all the disparate viewpoints that will be brought to the table, a process that allows for multiple views to be heard is the most likely to bring out the best ideas and to result in a shared sense of ownership over the final product.

Open participation, transparency, and building consensus have rightly been identified as the touchstones for this effort, and the NTIA can facilitate all three when it defines the process that will be followed. It will be important to develop a framework that ensures that all voices, not just the loudest, are heard. This can be achieved by adopting a structure that balances the participation of industry, interest groups, and other stakeholders. Meetings and discussions should be well publicized with sufficient notice to all interested parties. While in-person participation should be encouraged, every effort should be made to make the process accessible over the internet and by telephone.

In addition, the NTIA should ensure that all meetings, discussions, and gatherings are made available for later review, including any materials presented. In order to facilitate ongoing discussion, the NTIA should consider establishing an online forum for continuous discussions, and should encourage the development of "unofficial" discussion threads. While we recognize that not every idea can be incorporated into the final codes of conduct, it is essential that all interested parties are given the opportunity to voice their views.

The Request for Comment also asked for input on how to define "consensus," and rightly notes that it does not have a single definition. In order to balance the desire for inclusion with the need to be efficient and make progress, the multistakeholder process should recognize that consensus does not necessarily always mean unanimity.

Consumer Data Privacy Issues to Address Through Enforceable Codes of Conduct

If they are to be successful, the codes of conduct cannot be overly restrictive and cannot be binding unless a company affirmatively adopts one. They also must be clear and easy for consumers to read so that a lay person can understand quickly how his or her data will and will not be used and stored. Codes must be principles-based and technology neutral; technical language or overly legalistic descriptions will limit the ability to gain support, slow voluntary adoption, and ultimately impair effectiveness. We were pleased to see that the President's Framework recognizes that protecting privacy is a shared responsibility between consumers and the companies that hold personal data, and the codes of conduct should reflect this.

On the topic of the merits of convening the first multistakeholder process to address the principle of transparency in the privacy notices for mobile applications, we urge you to define tightly this or any other subject matter under discussion. Doing so will allow stakeholders to determine from the outset whether they need to be involved in a particular process. Further, the more focused the inquiry, the easier it will be to achieve consensus by avoiding extraneous and potentially controversial issues.

Of course, this effort will not take place in a vacuum; many of the issues that will be considered during the process are also being considered by other nations around the world. And while the United States and its international partners typically share the goal of enhancing privacy protection for their citizens, history has shown that we take different approaches to privacy. The NTIA, and the stakeholders who join this effort, must ensure that both the process and the resulting codes of conduct do not undermine government and the private sector's efforts to reconcile differing approaches. Data knows no borders, and many of the companies that will be asked to implement the voluntary codes of conduct are global entities that must adhere to cross-border legal requirements.

The "safe harbor" framework developed by the Department of Commerce in consultation with the European Commission is an excellent example of how to reconcile this effort with international partners, and the codes of conduct must be developed in a manner that both maintains this framework and ensures that the codes are compatible with regulations and codes being developed by other nations. A code of conduct that is incompatible with the approach of a major international partner will not be beneficial. Companies will not want to adopt it, and consumers will not be provided any assurance of how their data would be managed by an entity that is required to comply with multiple, inconsistent frameworks.

Finally, it is essential that the codes of conduct do not impair legitimate efforts to detect fraud or improve security. The codes must allow for controlled analysis of some data to detect fraudulent or illicit activity. If in the name of privacy we facilitate the ability of criminals to hide on a network and steal personal information, we will have precisely the opposite result we desire. Privacy is not realizable without security, and we must ensure that any codes of conduct do not hinder either of these objectives.

Symantec thanks you for the opportunity to provide this input, and looks forward to working with the NTIA on this significant initiative. We are available for any additional queries or discussions.

Sincerely,

Cheri F. McGuire
Vice President
Global Government Affairs & Cybersecurity Policy
Symantec Corporation