Intel Corporation is pleased to file comments on the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy." Intel commends the Department for conducting this inquiry and for their critical efforts on addressing privacy and innovation.

Our comments will address Intel's beliefs that: (1) there is a need for preemptive, comprehensive privacy legislation; (2) such legislation should be based on a robust reading of the OECD Fair Information Practices; (3) legislation should be technology neutral and allow for regulatory flexibility to address changing business practices; (4) the Department should encourage the adoption of the principle of Privacy by Design; (5) the Department should promote the accountability model for privacy protection; and (6) the Department should be commended for its work on the APEC Cross-Border Privacy Rules and should set a goal for adoption of those rules in 2011.

I. Need for Federal Privacy Legislation

Intel is a company that believes in the importance of innovation to help solve important social issues of our time, and to provide real benefits for the lives of individuals. Through our experience in technology innovation, we see a world undergoing a dramatic evolution. Individuals are more connected, and a global flow of data is required for today's information economy. Information technologies are providing tremendous capabilities for virtually every aspect of our lives - how we work, play, socialize, and educate. With the opportunities that accompany this new digital society also come new risks, including more sophisticated computer-related threats, many of which directly affect user privacy.

Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, irrespective of country of origin, to continue the innovations necessary to drive the global digital infrastructure, and remain competitive in the global marketplace. Laws and regulations impacting the ability to collaborate and share information across country boundaries need to keep pace with our technical need for such international collaboration. At the same time, in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the global digital infrastructure forward. Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth. Intel strongly believes that comprehensive and preemptive U.S. federal privacy legislation is a key mechanism for building this consumer trust in the Internet and ecommerce.

II. OECD Fair Information Practices

Intel supports federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines. The principles in these guidelines are as follows:

1) **Collection Limitation Principle** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.
2) **Data Quality Principle** – Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3) **Purpose Specification Principle** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4) **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with principle 3, above, except: (a) with the consent of the data subject, or (b) by the authority of law.
5) **Security Safeguards Principle** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6) **Openness Principle** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7) **Individual Participation Principle** – An individual should have the right: (a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her; (b) To have communicated to him or her, data relating to him or her (i) Within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her; (c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d. To challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed or amended.
8) **Accountability Principle** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

III. "Use and Obligations" Model

Intel supports what is known as a "use and obligations" model, which has been thoroughly explained in The Business Forum for Consumer Privacy's paper entitled "A Use and Obligations Approach to Protecting Privacy," *available at* http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf. The "use and obligations" framework states that the way an organization *uses* data determines

the steps it is *obligated* to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use. It imposes on organizations obligations based on five categories of data use: (1) fulfillment; (2) internal business operations; (3) marketing; (4) fraud prevention and authentication; and (5) external, national security and legal.

We believe that federal legislation should incorporate such a model, and we believe that the Department, with its understanding of the complexities of different business models, is well-positioned to promote with policymakers an understanding of the benefits to innovation and the growth of e-commerce of such an approach.

IV. Technology Neutrality and Flexibility

Intel encourages the Department to promote legislation that is technology neutral and gives flexibility to the FTC to adapt the bill's principles to changes in technology. Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving technological society, as the creation of legislative and regulatory requirements will invariably trail innovation of new technology. Therefore, a focus in the application of principles, neutral to the technology used, enables a flexible, effective and timely response.

V. Accountability

Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.[1] Though definitions of what is meant by "accountability" vary across these instruments, a useful approximation is the following:

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.*[2]

---

[1] The accountability principle is included in:

- Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)
- Asia Pacific Economic Cooperation Privacy Framework (APEC Privacy Framework)
- The European Union's Directive on the Protection of Personal Data
- Canadian private-sector privacy law: The Personal Information Protection and Electronic Documents Act (PIPEDA), and
- The Safeguards Rule of the Financial Services Modernization Act of 1999, commonly referred to as the Gramm Leach Bliley Act.

[2] Center for Information Policy Leadership, submission for Galway conference convened with the OECD in Dublin, Ireland.

Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles which have privacy and security integrated as foundational elements. Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way now.

We encourage the Department to promote an accountability model and to educate policymakers on the benefits of such an approach.

VI. Privacy by Design

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of the concept known as "Privacy by Design." Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation.

The consensus view of these regulators – including the European Article 29 Working Party, the FTC, and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient. Intel believes that a Privacy by Design principle should encourage the implementation of accountability processes in the development of technologies. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

Thus, we would encourage the Department to take a leadership role in promoting a principle requiring that organizations should ensure that privacy is included as a principle in product and service development processes.

VII. APEC Privacy Framework

Intel commends the leadership of the Department of Commerce for its ongoing work within the Asia Pacific Economic Cooperation (APEC) to develop and implement a privacy framework. Since the APEC Ministers endorsed the Privacy Framework in 2004, the Department, in conjunction with other federal agencies, has taken a leadership role and made great progress to develop a system of Cross-Border Privacy Rules that would ensure accountable cross-border flows of information while both protecting consumers and allowing for the benefits of ecommerce. As the U.S. hosts APEC next year, we encourage the Department to continue its active leadership within APEC with the goal of ensuring adoption of the cross-border privacy rule system in 2011 during the U.S. host year.

VIII. Conclusion

Intel again thanks the Department for their leadership in this important issue. We are supportive of the Department playing a role in this debate, and we look forward to continuing our engagement in helping to think about ways to improve the overall protection of privacy and the promotion of innovation and ecommerce.