Hewlett-Packard Company
3000 Hanover Street
Mail Stop 1050
Palo Alto, CA 94304-1112
www.hp.com

May 11, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Larry Irving
VP, Global Government Affairs
Tel. +1 202 637 6751
larry.irving@hp.com

Scott Taylor
Chief Privacy Officer
Tel. +1 650 857 7469
staylor@hp.com

Dear NTIA,

Hewlett-Packard Company (HP) appreciates the opportunity to provide feedback as part of the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy."

HP is headquartered in Palo Alto, California, and is a global provider of computing and imaging solutions and services, conducting business in over 170 countries around the world with more than 300,000 employees globally and 2009 revenues of $114.6 billion.

Respecting our customers' privacy has been in our DNA since the inception of the company and an integral part of our success. We firmly believe that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust.

Only by ensuring the privacy and security of all the customer information that we handle can we rightfully gain and maintain that trust. From becoming one of the earliest U.S. companies to participate in the U.S.-EU Safe Harbor program in 2001, to working collaboratively with industry, regulators and consumer advocacy groups, HP is committed to advancing forward-looking, workable privacy initiatives that respond to consumer needs and advance innovation.

We will provide brief comment and thoughts on all eight of the areas raised in the Notice of Inquiry.

1. The U.S. Privacy Framework Going Forward

(whether the existing U.S. policy framework provides sufficient guidance to the private sector to enable organizations to satisfy applicable U.S. laws and regulations; whether there are particular modifications to U.S. privacy laws that would better support innovation)

HP has been very public in calling for omnibus U.S. federal privacy legislation. We firmly believe that it is time for the U.S. to establish a comprehensive, flexible, and harmonized

legal framework for protecting consumer privacy. Recent research shows trends that consumers want it, we believe companies need it, and the economy will be better for it.

HP is a strong proponent of effective corporate self-regulation. We believe that the future of e-commerce depends on companies acting in an accountable and responsible manner to advance consumer needs. At the same time, however, we recognize that consumer privacy presents a series of challenges that have not yet been fully addressed. For example, the patchwork of state-based privacy regulations in existence today confuses consumers as to the extent of their protections in any given context, and forces companies to contend with a mix of differing and often conflicting regulations.

Further, heightened consumer concerns about existing privacy threats – from spyware to phishing, spam to data breach, and any number of other challenges – risk undermining the economic health of e-commerce and innovation. No one is served – not consumers, not governments, and certainly not corporations – by a lack of customer confidence in the security and privacy of personal information in existing products and new innovations.

HP believes that the U.S. should take steps to consider a comprehensive federal approach to protecting consumer privacy – one that provides a workable *national* standard in lieu of the current patchwork of state laws. This national baseline should be built on fundamental, sound privacy principles that include:

- transparency and consumer choice;
- use and obligations;
- scalability and flexibility;
- information security;
- accountability; and
- strong enforcement.

We are not looking for the government to dictate the terms *or technologies* for protecting privacy. Rather, we would continue to urge policy makers to examine ways of establishing a workable benchmark that unifies the divergent regulations currently in existence, responds to the very real needs of anxious consumers, and, at the same time, is flexible enough to accommodate future technological innovations.

2. U.S. State Privacy Laws

(how different state-level laws and regulations affect companies' compliance costs, product development processes, business activities, and the ability to work online; what approaches do companies take to comply with the myriad laws)

Many of the state laws and statutes (e.g., data breach notification laws) have created solid foundations for improved organizational behavior and consumer protections. But as the number of state laws and statutes grow, so does the complexity in business compliance processes and costs. We believe that many of the best practices that exist in state laws should form the basis of federal legislation to ensure a predictable and uniform standard across the U.S.

3. International Privacy Laws and Regulations

(how international data privacy laws and regulations affect global Internet commerce, companies' compliance costs and product development processes, and Internet users; what hurdles do businesses face in complying with different foreign laws concerning privacy and data protection; what lessons have companies learned from the U.S.-EU Safe Harbor Framework that could be applied in the global context)

As a large multinational corporation, we have to think and operate globally. We have found the best approach to privacy is a consistent standard that is based on solid external criteria, such as the EU Directive, OECD principles and Fair Information Practices. It would create greater compliance risk and increase operational costs for us to manage privacy differently for each country/region. This is one of the reasons HP was among the first companies to self-certify in 2001 to the U.S.-EU Safe Harbor Program. The work that the Department of Commerce achieved with the European Union to establish this program was critical to our company. It not only provided a bridge, but it enabled us to set a higher, global standard within our company for privacy.

In an Internet age, data flows are global and it becomes critical to innovation that we are able to reconcile emerging privacy frameworks or regimes. This is why HP is encouraged by new, emerging privacy frameworks, including Binding Corporate Rules in Europe and Cross Border Privacy Rules in APEC. We commend the strategic leadership of the Department of Commerce in establishing APEC Cross Border Privacy Rules, and encouraging a dialog between the APEC Privacy Sub-group and the Article 29 Working Party. Most recently, the Department's support of the Galway Project on Organizational Accountability, led by the Centre for Information Policy Leadership, and your encouragement of the Use and Obligations Model, developed by the Business Forum for Consumer Privacy, are examples of the influence and leadership you can provide in aligning the global and domestic agenda.

If we are able to keep these new frameworks and concepts aligned, at least in basic approach, it will enable organizations to uphold and demonstrate capacity against clear, outcomes-based expectations and manage higher levels of compliance and accountability.

4. Jurisdictional Conflicts and Competing Legal Obligations

(whether companies face any jurisdictional conflicts as a result of complying with privacy laws, how they reconcile such conflicts, and, what, if any, effect they have on trade and foreign investment)

As stated previously, HP has created global policies and implementation standards that align to the EU Directive, Safe Harbor, and most other recognized principles. Although this makes our policy more stringent than many country laws, it aligns to our core values and a uniform approach is easier to administer. As new laws and frameworks are established worldwide, anything that can be done to align and minimize jurisdictional conflicts will benefit companies in managing compliance and creating a predictable environment that encourages innovation.

5. Sectoral Privacy Laws and Federal Guidelines

(given the U.S.'s sectoral approach to privacy regulation, how does the sectoral approach affect consumer experiences, businesses practices, or the development of new business models; are there alternatives or supplements to the sectoral approach)

The major sectoral programs, HIPAA and GLBA, have provided consumer protections for privacy and data protection, but they clearly do not extend across all industries. As mentioned above, we support omnibus federal privacy legislation in the U.S. As this legislation is developed, it needs to take into account, co-exist with, and complement those sectoral laws.

6. New Privacy-Enhancing Technologies and Information Management Processes

(what is the state of development of technologies and business and business methods aimed at improving companies' ability to monitor and audit their privacy compliance)

The new applications, business models and technologies that have emerged with the Internet provide tremendous benefits to consumers and are critical to economic growth and prosperity. Yet, these same innovations create new issues for privacy and cybersecurity. Recent research and events have shown that a number of unanticipated privacy and data security issues have begun to erode consumer confidence and trust. This creates a compelling challenge as organizations work to balance innovation and the protection of data and individual rights. Just promising to try harder is not going to be good enough. We have to get smarter and ensure that we can provide meaningful protection.

Current laws and regulations struggle to keep pace with new forms of data collection, use and storage. As consumers, advocates and regulators become more aware and more concerned about these issues, organizations will need to do more to consider the privacy risks created through innovation.

New organizational accountability frameworks are emerging that set expectations for companies to design privacy enablers and risk mitigation into every stage of product development. It is often referred to as "Privacy by Design."

HP's Privacy team has partnered with our R&D Labs to develop and deploy a Privacy by Design program to ensure that our more than 300,000 employees understand privacy implications as they conceive and develop products and programs that will collect or use personal data. The program is not just about compliance. It integrates ethics- and values-based considerations to ensure we align to company codes of conduct and consumer expectations. Most product designers – or marketing managers – are thinking about the next innovation – not about what we at HP have termed "PUF" – potentially unwanted functionality. But employees – whether they are designing a new product or launching an email marketing campaign – need to understand how to put policies, obligations, and values into effect, and to do so prior to design or deployment.

Not all innovative ideas become reality, so we need to break-down product or program development into simple stages. In the design and development stages, privacy organizations should provide proactive guidance so privacy considerations can inform early planning. This has traditionally been difficult for companies and can result in a

program being delayed or cancelled later based on privacy concerns. Early guidance related to privacy becomes a tremendous asset to an organization because it ensures privacy pitfalls can be avoided. In the deployment, maintenance, and end-of-life stages, a privacy team needs to do more than just guide. They must provide assessment mechanisms to ensure compliance with local laws, and company obligations, policies, and values. We have learned that this assessment needs to be as contextual as possible. For example, the way we need to assess privacy compliance in a global email marketing campaign is very different than assessing privacy compliance in a new PC or web-enabled printer.

To help manage this, HP has deployed an interactive, online tool that is available to every employee from our intranet. The tool, which we call "The HP Privacy Advisor," starts by asking the user a series of simple questions. As the employee answers each question, additional dynamically generated questions are posed based on the collective intelligence and risk factors that result from how prior questions were answered. Essentially, it is an intelligent privacy impact assessment that is relevant to the employee using it and scales to cover simple and complex programs. One of the greatest benefits is educating employees about privacy requirements in the context of their specific programs. Through the process, employees learn about privacy issues and can modify their approaches to ensure compliance. The assessment results are documented and reviewed by the Privacy team. Consultation is provided as necessary, and if any issues exist, approval is required prior to deployment. After a product or program launch, additional workflow is triggered to ensure deployment is consistent with expectations and that end-of-life actions are taken when appropriate.

The HP Privacy Advisor serves as the front-end process to our Integrated Assurance Management Program, which includes annual risk identification processes, ongoing monitoring, audit, and formal remediation and tracking.

By using technology, we are better positioned to guide our employees to think about privacy in the right context and at the right time. We are also able to see trends, issues and opportunities in a real-time manner. This minimizes unanticipated effects and balances our ability to innovate and ensure responsible practices when using data.

7. Small and Medium-Sized Entities and Startup Companies

(how do existing privacy laws affect small and medium-sized entities and startup companies)

The harms that can arise from a lack of appropriate privacy or security protocols transcend business of all types and sizes. If a business, for example, handles highly sensitive personal data, the impact of poor privacy or security controls will be the same to the impacted individuals regardless of whether it is a small or large company that mishandled the personal data and caused the issue. Scalability of legislation is critical, but we need to ensure that the scalability relates to "how" an organization achieves a result, not "what" needs to be achieved. The same basic rules and principles ("what") should apply to all organizations, but "how" a small company implements may be very different than a large company. If we separate the "what" from the "how," we will ensure consistent expectations and leave organizations with the flexibility for achieving that expectation.

8. The Role for Government/Commerce Department

(how should the DOC Task Force help address barriers to increased innovation and consumer trust in the information economy)

The Department of Commerce has for many years played a critical leadership role domestically and internationally for privacy. We need only look to the U.S.-EU Safe Harbor program, the leadership in the 1990s on the future of privacy, the APEC Pathfinder Project, and the recent efforts to advance the cause of privacy and innovation. HP believes that the Department of Commerce should continue to provide leadership within the domestic agenda and with our major trading partners internationally. The Department is best positioned to advocate policy that will create meaningful consumer protections and at the same time allow for innovation and economic growth. HP stands ready to continue supporting your efforts.

If you have any questions or if you would like to discuss this matter further. Please don't hesitate to contact us.

Best regards,

Scott Taylor
Chief Privacy Officer
Hewlett Packard Company

Larry Irving
VP, Global Government Affairs
Hewlett Packard Company