

1150 18th Street, NW
Suite 700
Washington, DC 20036

p.202/872.5500
f.202/872.5501

April 2, 2012

Mr. Lawrence E. Strickling
Assistant Secretary for Communications and Information
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230

Comments Submitted by the Business Software Alliance

pursuant to
NTIA [Docket No. 120214135–2135–01], RIN 0660–XA27,
Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

Dear Mr. Strickling,

The Business Software Alliance (“BSA”) is the voice of the world’s commercial software industry and its hardware partners before governments and in the international marketplace¹. BSA’s members include businesses that function in a business-to-consumer environment as well as a business-to-business environment.

The recently released Administration framework on privacy and the Consumer Privacy Bill of Rights are a very significant accomplishment. The member companies of the BSA extend their congratulations to President Obama and the entire team that worked on this important policy announcement.

We appreciate the opportunity to provide these comments on elements our industry believes are important to consider as the Administration proceeds with implementing that plan.

I. General Observations on the Consumer Privacy Bill of Rights

In February 2011, we wrote to Secretary Locke supporting self-regulatory regimes that accommodate the evolution of technology and avoid government-mandated models that risk “one-size-fits-all” regulation and adverse unintended consequences. We are gratified that the foundation of the President’s Framework is an enforceable self-regulatory regime. To secure and maintain customers’ confidence, businesses must demonstrate their ability to protect customers’ personal information. At the same time, in order to allow the technology economy to thrive and grow, businesses need the freedom to innovate. By earning and maintaining that trust, businesses gain the freedom to continue to provide new – and better – privacy protections.

¹ *The Business Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward. BSA’s members include: Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, CNCIMastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, Quest Software, Rosetta Stone, Siemens PLM, Dassault Systèmes SolidWorks, Sybase, Symantec, and The MathWorks.*

This virtuous cycle lies at the heart of the concept of data stewardship, which guides BSA members in their handling of consumer data. In fact, all BSA members have implemented comprehensive, transparent privacy practices to address consumer concerns, often based on internationally agreed norms such as the Organization for Economic Cooperation and Development's Fair Information Practice Principles that lie at the heart of the Consumer Privacy Bill of Rights.

BSA also supports educating consumers on how they can make informed choices regarding how their personal data is collected, used, and stored. All computer users – consumers and businesses alike – should be educated on how to protect themselves from the growing number of Internet dangers, including fraud, unauthorized vendors selling counterfeit products, and identity theft. The protection of privacy depends on informed consumers, responsible businesses, and vigilant enforcement. This “shared responsibility” approach to privacy encourages consumers to be aware of privacy practices, to make choices about how their personal information will be used, and to safeguard data under their control.

Looking to the future, BSA member companies are each rapidly developing new services and products. They are only now beginning to unlock the potential of tomorrow's information-driven economy. For example, cloud computing is now a centerpiece of every technology company's strategy. BSA recently published a scorecard analyzing the cloud-readiness of 24 countries <http://portal.bsa.org/cloudscorecard2012/>. That scorecard looked at the privacy laws and policies of each country as a key indicator, along with their positioning on security, broadband deployment, protection of intellectual property and cybercrime. Our analysis revealed that every one of the 24 countries analyzed had room for improvement, including the United States.

Privacy law is particularly important to the advancement of cloud computing and the data-driven economy around the world, because the success of the technology depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of the cloud, providers must be free to move data through the cloud in the most efficient way. Overly restrictive privacy laws will undercut both users' trust and the opportunity for tremendous efficiencies and economic gains that the cloud presents.

As highlighted by our scorecard, success for American companies in providing cloud and other innovative services is critically depended on our ability to operate efficiently in both the US and internationally. Some countries have been implementing policies that constitute barriers to free trade in these key areas. Requirements that servers be situated locally, limits on investment and restrictions on access to government markets are a few examples.

As you proceed with your work, we urge you to keep a sharp focus on ensuring that US policies enable US companies to continue to compete – at home and abroad – based on the quality of our offerings. Rules on data privacy and mobility can create impediments to free international trade. The US-European Union Safe Harbor Framework is a great example of the kind of steps the Administration can take to ensure that American companies have a fair opportunity to compete in all markets. This initiative is important today and will be even more important in the future as the EU proceeds with developing new laws on privacy.

II. Subjects and Structure of the Multistakeholder Process on Consumer Privacy

In your request for comments you identify a number of areas where the development of enforceable voluntary industry privacy policies would be timely, including privacy policies for applications (“apps”) used on mobile platforms. We support the basic premise of starting with one discrete area, and increasing transparency in mobile app privacy policies provides as good a starting point as any. This is especially true given the policy work that has already been done in this area, including the recently announced California voluntary standards that have been espoused by many of the key industry leaders.

Whichever area is chosen first, we believe the following elements should form the basis of this work: Entities that gather user’s personal data should have clear and specific privacy policies. These policies should be transparent and provide users with information about who can access the gathered information and how it is used. Consumers should have an opportunity to review, for example, an app’s privacy policy before they download the app, and have a defined location where the consumer can find copies of the policy. Educating consumers should be a high priority, and the voluntary agreements should address this issue specifically. Finally, consumers should have tools available to report practices that do not comply with the vendor’s policies. The vendor should then have an opportunity to assess whether it is in compliance as well as an opportunity to cure the problem.

Entities that gather data should also have policies in place to ensure the collected data’s security. Today, BSA members include privacy as a determinative factor when developing new software and services; in effect designing privacy into the product from the start. In one important respect, this requires implementing effective security measures to prevent breaches. Consistent with available industry best practices and technologies, entities should take all technically feasible and economically reasonable steps to protect collected data.

With respect to the process that NTIA and Commerce implement to carry forward on your work, we urge you to use three key criteria: open participation, transparency, and building consensus. All interested stakeholders should be welcome to participate. Such an inclusive approach we feel is the best way to ensure all aspects of an issue are examined and all options are identified. Transparency, ensuring the public at large as well as participants are fully informed of the work is indispensable to broad acceptance of the outcomes. Finally, as with all well-established voluntary standards setting process, outcomes should be considered tabled and adopted only when they attract broad-based consensus. As with transparency and openness, we believe this is the only way to ensure acceptance of the outcomes.

To facilitate this work, we recommend NTIA function as a rapporteur for the work. In that role NTIA can compile and process materials based on the guidance of the working group, ensure the work is fully disseminated in a timely manner, inform all interested stakeholders of issues under consideration and when and where they will be considered. While it is conceivable that this work could proceed with NTIA as a mere observer, we believe a rapporteur role would be far more conducive to prompt, comprehensive and well-reasoned outcomes. At the same time, however, BSA believes that industry must play a leading role in each of the various multistakeholder processes. As technology companies will be responsible for adopting and implementing the various codes of conduct, these efforts must be based firmly on their expertise.

Toward that goal, NTIA should provide an overall structure to the various multistakeholder processes in order to ensure their success. As their foundations, the processes should be built on a plenary structure to include the full spectrum of participants. From there, smaller working groups can develop draft codes for review by the plenary group. At a functional level, the processes should comprise: occasional in-person sessions; regular, smaller conference calls and other meetings for issue-focused groups; email lists for the most involved individuals; and, collaborative websites for hosting material. Finally, and perhaps most importantly for the initial effort, deadlines must be implemented for each process in order to ensure movement toward successful conclusions.

Sincerely,

A handwritten signature in black ink that reads "Robert Holleyman". The signature is written in a cursive, flowing style with a large initial "R" and a long, sweeping underline.

Robert W. Holleyman, II
President and CEO