BSA®
BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

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

p: 202/872-5500
f: 202/872-5501

January 28, 2011

The Honorable Gary Locke
Secretary of Commerce
US Department of Commerce
1401 Constitution Ave. NW, Room 4725
Washington, DC 20230

RE: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, RIN 0660-XA22

Dear Secretary Locke:

The Business Software Alliance ("BSA") is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. BSA's members include businesses that function in a business-to-consumer environment as well as a business-to-business environment.[1]

BSA commends the work of the Department of Commerce Internet Policy Task Force (the "Task Force") in examining the future of privacy protection in the Internet and its ongoing role in the development of a stronger privacy framework in the United States. BSA appreciates the opportunity to be heard as part of the dialogue on the emerging privacy

[1] The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Altium, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, and The MathWorks.

framework and in response to certain of the questions and issues raised in the Report. In this letter, we provide our general observations on the proposed framework and we address certain of the Task Force's questions regarding the use of privacy technologies, improved transparency, and privacy education.

I. GENERAL OBSERVATIONS ON THE EMERGING PRIVACY FRAMEWORK

BSA agrees with the Task Force that "[s]trong commercial data privacy protections are critical to ensuring that the Internet fulfills its social and economic potential." (Report Introduction at 1.) BSA believes that the protection of personal information, and the prevention of information misuse that may cause harm, are essential to fostering trust and confidence in the online experience. Likewise, the protection of intellectual property rights is essential to the creative economy online and offline. Thus, while privacy protection must be a high priority, so too must be the ability to hold wrongdoers accountable for online piracy activities. Privacy and accountability can and should co-exist online as businesses and law enforcement combat theft of intellectual property.

More than one of every three copies of software installed worldwide is pirated. Any framework for the protection of privacy must address the inevitable tension of user privacy and the protection of intellectual property rights in a way that respects both sets of rights. The need for privacy protection cannot become an excuse for concealing the identities of individuals who pirate protected content.

In the investigation of and enforcement against online piracy of intellectual property, it is necessary to access, record and transmit personally identifiable data. For example, investigations typically reveal IP addresses and other identifying information concerning the computers of online infringers. That information is recorded and transmitted to Internet Service Providers who deliver notices to customers associated with the IP address. The information also is used to pursue civil actions for copyright infringement and other wrongful conduct. Thus, in addressing how or whether to implement Fair Information Privacy

Practices ("FIPPs"), as the Task Force recommends, care must be taken not to prescribe overly broad rules that would impede the protection of intellectual property.

With that said, BSA agrees with the Task Force's recommendation that FIPPs be expanded. BSA further agrees with the Task Force that to meet privacy goals, voluntary, enforceable codes of conduct must be promoted. (Report at 42.) Thus, in response to the Task Force's question regarding whether FIPPs should be enacted through statute or other means, BSA believes that self-regulatory regimes that accommodate the evolution of technology are preferable to government-mandated models which risk "one-size-fits-all" regulation and adverse unintended consequences. However, BSA believes that any self-regulatory regime must be accompanied by government enforcement of the deviation from announced self-regulatory principles. There has been a long history of self-regulation in the privacy area, particularly in the United States. The self-regulatory approach has produced advances in the protection of young Internet users under the Children's Online Privacy Protection Act (COPPA), and the online advertising industry continues to strive for innovative new solutions for all users. Such experiences have led to updates and improvements in the performance of self-regulatory regimes as technology even as the public and government understanding of the privacy implications of online practices evolves. Because privacy protection is dynamic, not static, government rules can fit one situation at one point in time but later fall out of date.

For example, the "opt-in/out-out" dichotomy, which dominated privacy policy discussions a decade ago, has given way to newer technology solutions that allow a better understanding of privacy choices by individuals and more informed judgments than a "yes/no" approach. These new solutions lie at the heart of the concept of data stewardship. In order to secure and maintain their 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. In this way, technology forms the basis of the self-regulatory regime, a virtuous cycle which can

and will augment legal protections. Concomitant with dynamic self-regulatory rules must be a "trust but verify" enforcement backstop by regulators and the introduction of incentives for companies to agree and adopt self-regulatory enforcement.

No matter how any privacy framework is structured, however, BSA believes that the framework should be outcome-oriented. It should focus less on prescriptive requirements and more on substantive results. A greater emphasis on outcomes – *i.e.*, a focus on what organizations achieve, not how they achieve it – will maintain strong user protections while reducing compliance burdens for data controllers. We agree with those commentators mentioned in the Report that believe that placing form over substance can and will distract organizations from the goal of protecting consumer privacy. (Report at 25.) The danger of an overly prescriptive or regimented privacy framework is that the framework can and will add excessive costs, hinder the development of technology and legitimate marketing activities, and, when improperly drafted or enforced, can lead to adverse unintended consequences. While prescriptive requirements may be necessary, they must be flexible enough to allow for – and indeed foster – innovation. Along these same lines, the framework should be technologically neutral – *i.e.*, not favor one type of technology over another – which will support the evolution of innovative data privacy and security solutions.

A final general point on the proposed framework: Although BSA agrees with the Task Force that commercial data privacy policy must cover a "continuum of harms" and that even "less severe harms" could potentially have "significant adverse effects" on consumer trust in the Internet economy (Executive Summary at 1), BSA also believes that a privacy framework that fails to account for the higher risk of harm that can result from the unconsented-to use of certain forms of personally identifiable information will not protect either consumers or businesses. Matters relating to health, finance, and children, top the lists of potential areas most at risk. By focusing on the areas and types of information in greatest danger of misuse, privacy policies maximize their effectiveness.

II. PRIVACY TECHNOLOGIES

The Task Force asks questions about existing technologies that assist in privacy and data protection (*e.g.*, whether technologies are available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations; whether there are technologies available to help companies monitor data use and to support internal accountability mechanisms). BSA believes that existing Privacy Enhancing Technologies ("PETs"), which include encryption software, anonymizers, and browser extensions that provide granular data controls, can accomplish the privacy goals set forth in the Report. Providing technical mechanisms and controls to enforce privacy policies, PETs can fortify and protect consumer decisions online and are an essential tool for user empowerment. BSA members have developed and deployed a range of privacy technologies that play an important role in providing data minimization and effective data management, both of which help in ensuring data security.

For example, BSA members developed homomorphic encryption, which allows for the use of securely encrypted personal data without viewing the actual data, thereby allowing value to be derived from information in a privacy-friendly way. This technology won the 2009 privacy innovation award from the International Association of Privacy Professionals. We believe that PETs, such as homomorphic encryption, should be an important part of in the product design phase or as part of proactive and preventive program enhancements.

In addition to the development of specific technologies, BSA members work to improve the privacy and security of networked systems and applications through their commitment to standards development. These efforts include working with international standards development organizations, such as the Organization for the Advancement of Structured Information Standards (OASIS), as well as industry forums, including the Cloud Security Alliance and the Kantara Initiative.

BSA strongly believes that when discussing the use of technologies in the context of FIPPs (or otherwise) care must be taken not to interfere with the technological tools built into software to ensure that intellectual property rights are respected and opportunities to innovate survive. Thus,

we agree with the Task Force that FIPPs that are both flexible and comprehensive, and that are made applicable to a wide range of technologies and data usages, are necessary. (Report at 25.) In this regard, we urge the Task Force not to incorporate technology mandates or overly prescriptive rules into any privacy framework. It would be harmful for both privacy and security if the use of certain technologies were mandated. Such technology mandates serve only to freeze product development, thereby preventing users from reaping the benefits of innovation. As threats to user privacy and security change rapidly, we can ill afford policies that hinder the deployment of technologies that can enhance user protection and address the most up-to-date threats.

BSA also supports FIPPs that implement the privacy by design concept, which is a roadmap to integrate privacy considerations into business models, product development cycles, and new technologies. Indeed, privacy by design is already a guiding principle for our members in solution development as the data security built into the products of BSA members is a principal protection against the unwanted sharing and misuse of personal information. For example, BSA members are involved in several industry initiatives related to online privacy, including the Open Identity Exchange (OIX) and the Trusted Technology Provider Framework (TTPF) under the Open Group and the OASIS Privacy Management Reference Model Technical Committee. In addition, several of our members established and participate in the SAFECode project, an industry initiative that identifies and promotes best practices for developing products that are secure and enhance user privacy.[2] The privacy by design concept is a good one, principally because it recognizes that privacy cannot be assured solely by compliance with regulatory frameworks. Rather privacy must become integrated into an organization's fabric and function within an organization's default mode of operation. Ideally privacy would be part of initial design; but even for existing services privacy can be viewed as a proactive and preventative program, not a reactive or remedial act. BSA believes that privacy by design can be implemented through the promotion of PETs.

[2] SAFECode is a global, industry-led effort to identify and promote best practice for developing and delivering more secure and reliable software, hardware and services.

III. TRANSPARENCY

BSA supports a balanced approach to privacy that respects and encourages informed consumer choices, while ensuring that products and services can be tailored to specific consumer's needs and industry can continue to deliver products and services that consumers value. In this regard, BSA supports the concept of transparent privacy notices and simplified consumer choice. 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 ("OECD") FIPPs, which are mentioned favorably in the Report. (Report at 25.) Industry, government and non-governmental organizations must continue to educate consumers on how to make informed choices about how their personal data is collected, used, and stored. This includes encouraging consumers to be aware of privacy practices, make choices about how their personal information will be used, and safeguard data under their control.

It has been suggested that in "take it or leave it" situations, consumers will be effectively without "choice" and thereby disadvantaged by unfavorable or unlawful terms for products or services that they would like to use. While BSA understands and appreciates this suggestion, BSA believes that the suggestion is unfounded in certain circumstances where such choice is necessary and appropriate. In fact, it is this very type of "offer and acceptance" contract that enables the smooth operation of large segments of the economy.

For example, End User License Agreements and Terms of Service ("EULAs") often specify that certain information will be collected and used to protect intellectual property rights. Although BSA members endeavor to communicate the nature of that transaction prominently before the consumer installs or uses software, the arrangement is akin to an "offer and acceptance" arrangement whereby the consumer may not use a software product without agreeing to the EULAs. This type of arrangement is necessary for the protection of intellectual property. But the EULAs also contain numerous terms that protect *both* the service provider and the consumer including, for example, alternate dispute resolution, limits of liability, damage limitations, among other things.

EULAs are not simply contracts of adhesion for which consumers would be left without remedies under applicable law. General contract laws – which remedy such things as unenforceable contract terms – apply to EULAs and provide consumers with recourse.

It is worth noting that "offer and acceptance" arrangements are not uncommon outside the privacy arena. In mass market situations, particularly in the mass market for services, it is not uncommon to have such choice. Airlines, theatres, car rental establishments, among others, all operate under these types of arrangements, and they are perfectly acceptable to the public. Indeed, it would be virtually impossible – or at least a huge burden on the economy – to operate in any other way: Imagine having to negotiate individual contracts on a mass market basis; the service industry would not be able to function. These very same considerations that make such choice acceptable for mass markets also apply to EULAs.

IV. PRIVACY EDUCATION

The Task Force recommends establishing a Privacy Policy Office ("PPO") to serve as a center of commercial data privacy policy expertise. Among the areas that the PPO would focus on is consumer privacy education. (Report at 50.) The Task Force states that private sector chief privacy officers would be collaborators in the educational effort. (*Id.*) BSA supports educating consumers on how they can make informed choices regarding how their personal data is collected, used and stored. In addition, BSA believes that 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.

BSA is a leader in consumer education efforts, and BSA runs targeted consumer awareness campaigns that educate people on the risks associated with not ensuring personal Internet safety and the laws pertaining to software purchases and/or software management. In order

to educate consumers and computer users, BSA provides tools like the Cybertreehouse, which helps children learn about Internet safety and software laws at an early age. BSA's website www.bsacybersafety.com offers videos educating consumers on the effects of not being cybersafe, provides a guide to common Internet threats and how to avoid them, and includes many other resources to help consumers protect themselves against Internet fraud. In addition, BSA makes free software audit tools and partnership resources available for businesses to learn more about proper software implementation procedures. BSA believes that education efforts such as those undertaken by BSA are an essential element of privacy, and BSA would welcome the opportunity to be a part of the educational collaboration that that the Task Force envisions (as part of a PPO structure or otherwise). We believe that the Task Force should encourage further individual education efforts by businesses, industry associations, and consumer groups, and recognize as part of its framework the already good work that has been done in this area.

****

BSA again would like to thank the Task Force for the opportunity to be heard on these very important issues surrounding the proposed framework. BSA and its members would welcome the opportunity to further exchange their views expressed in this paper in more depth with the Task Force.

Sincerely,

Robert W. Holleyman, II
President and CEO
Business Software Alliance