BSA®
BUSINESS SOFTWARE ALLIANCE

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

p 202/872.5500
f 202/872.5501

February 18, 2011

Federal Trade Commission
Office of the Secretary
Room H-113, Annex
600 Pennsylvania Avenue, NW,
Washington, DC 20580

RE: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Commissioners and Staff:

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 Federal Trade Commission Staff in examining current privacy issues and in raising questions about the future of privacy protection. BSA appreciates the opportunity to be heard as part of the dialogue on the emerging privacy framework and in response to certain of the questions raised

[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, 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.*

in the Report. Below we provide our general observations on the proposed framework and we address certain of the Commission's questions regarding privacy by design, the scope of the proposed framework, consumer choice, and privacy education.

I. GENERAL OBSERVATIONS ON THE EMERGING PRIVACY FRAMEWORK

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. These factors also are essential to the full development of the range of products and services that consumers will be willing to use and buy in the online marketplace. A proposed framework that addresses these issues fully benefits both consumers and businesses alike: privacy protections are not just for consumers; instead, businesses benefit from serving as responsible stewards of the personal information of their customers and clients. Only by doing so can businesses earn the trust that underlies the exchange of such private information. Thus, BSA calls for policies that foster a vibrant online marketplace where citizens and businesses can use information tools with confidence, by making certain that laws effectively prohibit and punish fraud, theft, and other crime over the Internet.

A viable and secure online environment requires several elements. Key among these are: protecting privacy; meeting the needs of both consumers and businesses; and, allowing opportunities for

innovation. So too is protecting intellectual property. Just as users need to be confident that the collection of personally identifiable information is not undertaken without notice and consent, businesses must be able to ensure that users of web sites and online systems are who they say they are. The Commission needs to give consideration in establishing the framework to the pernicious and widespread phenomenon of wrongdoers using privacy as a shield to engage in the piracy of intellectual property.

More than one of every three copies of software installed worldwide is pirated. While efforts to cut piracy in large businesses may be successful, piracy can increase as a result of new users from small businesses entering the market for the first time. 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. It is instructive to remember that passwords protect both the user and the site operator. Both groups have an interest in making sure that a transaction is secure and protects the respective interests of privacy and ownership of intellectual property.

BSA also 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, so long as government enforcement of

deviation from announced self-regulatory principles is available and rigorously enforced. 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 even as the public and government understanding of the privacy implications of online practices has evolved. 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. 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.

In addition, BSA commends the FTC for proposing a privacy framework that includes "commonly accepted practices." We believe that this comment has merit and should explicitly include important business functions that are data-driven such as security access controls and user and employee authentication; cybercrime

and fraud prevention and detection; and, protecting and enforcing intellectual property and trade secrets.

A final general point on the proposed framework: Despite the criticisms of the harms-based approach to privacy protection contained in the Report, BSA believes that it remains appropriate for privacy protection to focus on the risk attributable to the misuse of certain types of data in setting the level of protection for that data. 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 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 BY DESIGN

The Commission advocates the introduction of "privacy by design," which is a roadmap to integrate privacy considerations into business models, product development cycles, and new technologies. BSA also supports the concept of privacy by design, which is already a guiding principle for our members in solution development. 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 agrees that companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Indeed, the data security built into the products of BSA members is a principal protection against the unwanted sharing and misuse of personal information.

However, BSA believes that in defining and integrating the principle of privacy by design into the proposed framework 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. In this regard, we urge the

[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.

Commission not to equate privacy by design with technology mandates, and overly prescriptive rules. It would be harmful for both privacy and security if privacy by design resulted in a requirement for the use of certain technologies. Such technology mandates serve only 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.

Rather we ask the Commission to consider how privacy by design could be achieved through promotion of Privacy Enhancing Technologies ("PETs"). PETs include encryption software, anonymizers, and browser extensions that provide granular data controls. 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 privacy by design 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.

III. SCOPE

The Commission asks whether it is feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device." BSA does not take a direct position on the feasibility of including such data within the framework. However, BSA does believe that if such data is included in the framework, the Commission must consider the need to use the data in combating online piracy and promoting security.

In the investigation of and enforcement against online piracy of intellectual property, it is necessary to access, record and transmit data that can be "reasonably linked to a specific consumer,

computer, or other device." 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. In the case of promoting security, cyber security companies do process such pieces of information as URL's and IP Internet addresses to predict which machines located in cyber space will propagate malware. Once the machines which are sending malware are identified, the computers of consumers and organizations can be protected by blocking them from malware transmissions. Thus, in addressing the scope of privacy protection to be accorded to "data that can be reasonably linked to a specific consumer, computer, or other device," care must be taken not to prescribe overly broad rules that would impede the protection of intellectual property or the security of consumers and organizations.

IV. CONSUMER CHOICE

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 consumers' needs and industry can continue to deliver products and services that consumers value. In this regard, BSA supports the concept of improved privacy notices and simplified consumer choice. All BSA members have implemented comprehensive privacy practices to

address consumer concerns, often based on internationally agreed norms such as the Organization for Economic Cooperation and Development's (OECD) Fair Information Practices. 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.

The Commission asks under what circumstances it would be appropriate to offer choice as a "take it or leave it" proposition. We understand the Commission to be concerned that in such "offer and acceptance" 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 concern, BSA believes that the concern is unfounded in certain circumstances where "offer and acceptance" choice is necessary and appropriate.

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 "offer and acceptance" choice acceptable for mass markets also apply to EULAs.

V. PRIVACY EDUCATION

The Commission asks how businesses, industry associations, consumer groups, and the government can do a better job of informing

consumers about privacy. 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. We believe that the Commission 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 Commission 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 Commission.

Sincerely,

Robert W. Holleyman, II
President and CEO