January 28, 2011

By Electronic Filing

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Docket No. 101214614–0614–01

Dear Internet Policy Task Force:

The Entertainment Software Association ("ESA") appreciates the opportunity to comment on the Internet Policy Task Force's green paper on consumer privacy, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Privacy Framework."[1] The ESA is the exclusive U.S. organization dedicated to serving the business and public affairs needs of businesses that publish computer and video games for video game consoles, personal computers, and the Internet. With more than 35 members, the ESA represents nearly all of the major video game console manufacturers and game publishers in the United States.

The ESA commends the Department for releasing this Green Paper for public comment and for seeking input through its initial Notice of Inquiry and May 2010 symposium on information privacy and innovation in the Internet Economy.[2] The Department's efforts have fostered an important dialogue about how to ensure the privacy of commercial data in this time of rapid technological change.

The ESA encourages the Department to continue its efforts to address today's privacy challenges with a framework that promotes innovation. With more than two-thirds of all American households playing video games, the entertainment software industry added $4.9 billion to the U.S. Gross Domestic Product in 2009 and continues to grow as a source of employment in communities across the nation.[3] While innovation is one factor that has contributed to this tremendous growth, the industry's strong commitment to consumer privacy is another. Indeed, recognizing the importance of privacy to building consumer trust, the ESA established the Entertainment Software Rating Board ("ESRB") in 1994. The ESRB is a nonprofit, self-regulatory body that, among other things, helps ensure responsible online privacy practices for the interactive entertainment software industry.

---

[1] *See* DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010) [hereinafter GREEN PAPER].
[2] *See* 75 Fed. Reg. 21,226 (Apr. 23, 2010) (Notice of Inquiry); 75 Fed. Reg. 19,942 (Apr. 16, 2010) (Notice of Public Meeting).
[3] *See* Entertainment Software Association, Industry Facts, http://www.theesa.com/facts/index.asp.

The remainder of these comments responds to some of the specific questions raised in the Department's Green Paper. The ESA hopes that these comments, which are based on our deep understanding of the entertainment software industry and our experience helping to develop privacy programs for the industry, will assist the Department with developing a framework that protects consumer privacy interests while also encouraging continued innovation over time.

I. FAIR INFORMATION PRACTICE PRINCIPLES ("FIPPs") PROVIDE VALUABLE GUIDANCE FOR INDUSTRY, BUT MUST REMAIN FLEXIBLE.

The ESA agrees with the Department that carefully developed Fair Information Practice Principles can provide industry with valuable guidance. Our industry is committed to sound privacy practices, as evidenced by game publishers' participation in several different privacy programs. One of those programs is the ESRB's Privacy Online program, which has developed a set of FIPPs that apply, *inter alia,* in the website gaming context.[4] Specifically, the ESRB actively monitors participating websites for compliance with six key FIPPs:

1. Notice. Each participating business must implement and publish a "Privacy Statement" that informs consumers about its information practices.

2. Choice. Participating businesses must offer consumers a range of choices regarding the use of data appropriate to the sensitivity of the data, the potential uses of the data, the burden created by offering choice, and applicable law.

3. Limiting Data Collection and Retention. Participating businesses may collect and maintain data only for a valid business reason, but businesses have flexibility to define the reasons they determine are valid based on their particular business models.

4. Data Integrity and Security. Participating businesses with records of personal identifying information must take reasonable measures to assure their reliability and prevent loss, with options to select a wide variety of methods appropriate to the business's situation.

5. Data access. Participating businesses are required to give customers a reasonable opportunity to access and correct errors in personal information that the businesses store, with reasonableness determined based on the circumstances.

6. Enforcement and accountability. Participating businesses must implement effective and affordable mechanisms that ensure compliance with their information privacy policies and provide appropriate means of recourse for consumers.

[4] *See* Entertainment Software Review Board, Web Publishers - Principles and Guidelines, http://www.esrb.org/privacy/regs (last visited Jan. 24, 2011).

Like the ESRB's principles, and similar principles established by other reputable privacy programs utilized by publishers of entertainment software, it is important that the principles developed by the Department remain building blocks that industry can use to invent innovative privacy protections that withstand the test of time, rather than hardened rules that frustrate innovation with minimal consumer benefit or that quickly become obsolete as technology evolves. In short, while broad privacy principles can help guide industry innovation, government should resist the temptation to transform these principles over time into prescriptive, ossified privacy rules.

In particular, market participants should have flexibility to exercise appropriate business judgment where particular FIPPs are in tension. For instance, while the ESA agrees with the Department that transparency and purpose specification are laudable goals, there is an inherent tension between them. As the Department recognizes, "[w]hen information is presented in a way that is highly complex or detailed, it may not be transparent,"[5] but purpose specification often would necessitate detailed disclosures. It is important for a business to be afforded the latitude to balance the purpose specification and transparency principles to suit the particular contexts in which it operates. For instance, handheld systems and games as well as mobile smartphone-based gaming applications should have the flexibility to provide shorter, more high-level disclosures, given the small screens on which they are viewed.

Likewise, in order to ensure a balance between privacy concerns and the promise of innovation, businesses should be given flexibility to choose whether to issue Privacy Impact Assessments ("PIAs") and, if issued, to choose the format in which they are presented. If a business were required to produce a PIA each time it plans to release slightly modified hardware or make a change to software (for instance, by patching a video game), the pace of innovation would be slowed. Even if PIA issuance requirements were limited to more significant product/service developments, the administrative burden of producing them would often outweigh the associated benefits to consumers. Accordingly, businesses must retain the freedom to issue PIAs if, and when, they deem them useful. Additionally, the ESA urges the Department not to channel all businesses into a standardized cross-industry PIA format. Such an approach will either fail to capture the information that would be most useful to consumers in any given context or result in long statements of limited use in practice.

The ESA also urges the Department to continue working with industry and other stakeholders to define the scope of the comprehensive FIPPs. As the Department recognizes, the concept of FIPPs has been incorporated into numerous international frameworks and advanced by a number of government agencies in different contexts. And although the individual principles advanced in these frameworks generally overlap, there are important differences. For example, while the FIPPs proposed by the Department and those employed by the Department of Homeland Security contain the data minimization principle, the FIPPs

[5] GREEN PAPER at 31-32.

employed by the OECD and those endorsed by the FTC in 2000 do not.[6] The ESA will continue to work with the Department, consumer advocates, and others in industry to help define an appropriate, consolidated set of FIPPs.

II. VOLUNTARY, ENFORCEABLE "SAFE HARBOR" CODES WOULD BENEFIT CONSUMERS AND INDUSTRY ALIKE.

The ESA supports the Department's proposal to create a safe harbor for businesses that adhere to voluntary, enforceable codes of conduct that have been developed through an open, multi-stakeholder process. The ESA believes that these codes, like the framework itself, should promote both innovation and consumer privacy. The codes may cover different communication platforms. Whatever the scope of the codes may be, it is important that the corresponding safe harbor covers the full range of communication platforms that otherwise are subject to the code. This approach provides an optimal path for producing enforceable rules that can protect consumers while obviating the dangers posed by one-size-fits-all models.

The entertainment software industry has supported similar safe harbor programs in the past with much success. For example, in 1999 the ESRB's Privacy Online program became one of the first privacy seal programs sanctioned by the Federal Trade Commission as an authorized "Safe Harbor" under the Children's Online Privacy Protection Act ("COPPA").[7] The Privacy Online program sets forth a number of children's privacy requirements with which participating websites must comply to obtain safe harbor status. Through the Privacy Online program, ESRB actively monitors the compliance of over 400 websites.[8]

Based on the industry's outstanding experience with the Privacy Online safe harbor program, the ESA agrees that trade associations or similar non-governmental entities can have a role to play in supplementing Federal Trade Commission enforcement of voluntary codes. Because they possess a deep understanding of the industries they support, these entities should be the "front line" of enforcement whenever possible. Specifically, where a business commits to following a voluntary, enforceable code, it should be given the opportunity to demonstrate its good-faith compliance with the code under the monitoring of an agreed-upon trade association or similar entity. The Commission would act as a backstop, intervening only where the trade association or similar entity is failing to police participants in a responsible manner.

---

[6] Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Jan. 28, 2011); Organization for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 25, 2011).

[7] For more information on the ESRB's Privacy Online program, please visit http://www.esrb.org/privacy/index.jsp.

[8] *See* Entertainment Software Review Board, Websites Certified by ESRB Privacy Online, http://www.esrb.org/privacy/sites.jsp (last visited Jan. 25, 2011).

The ESA also agrees with the Department that it is sensible to require industry codes of conduct to be approved by the Commission before they are afforded safe harbor status. In response to the Department's question regarding the point at which Commission review of drafted codes should be available, the ESA believes the approval process should be available at the time the code is created. Any further delay in review could create a cloud of uncertainty for businesses that would hinder adoption and compliance of the code, thereby undermining its benefits.

In addition, the ESA does not believe all industry participants should be obligated to comply with a single code or develop codes through the same trade association. Rather, consistent with the Department's important goal of flexibility, multiple codes for a single industry should be considered and, where appropriate, allowed, as long as they are approved by the Commission. Such an approach will promote innovation by supporting various business models and tailoring privacy protections to the context in which users are engaging with businesses.

III. THE ROLE OF THE PRIVACY POLICY OFFICE ("PPO"), IF CREATED, SHOULD BE CAREFULLY DEFINED.

The ESA believes that the PPO could serve several useful functions provided its role is carefully defined. For instance, as the Green Paper suggests, the PPO could facilitate stakeholders' creation of voluntary, enforceable safe harbor codes and could play an important role in international outreach.[9] Additionally, the PPO could be available at the request of outside entities to convene stakeholders for discussions on emerging issues. The ESA believes it is important to make clear that the mission of the PPO is to focus on protecting privacy interests while facilitating innovation.

The ESA also believes that the PPO should not be given a broad or undefined mandate. If the PPO were given an open-ended mission, the ESA is concerned that it could add redundancy and confusion to an already active federal privacy ecosystem. Moreover, as the Green Paper suggests, the PPO's mandate should be clear that it has no role to play in investigation or enforcement, which should remain the province of the Federal Trade Commission.[10]

IV. INTEROPERABILITY AND HARMONIZATION SHOULD BE PURSUED ON BOTH THE INTERNATIONAL AND NATIONAL LEVELS.

The ESA supports efforts to work toward increased international cooperation on privacy issues. Conflicting privacy and data security requirements are among the most significant legal compliance challenges facing companies in the video game industry. This is particularly true with respect to cloud computing services where there is tremendous uncertainty about which jurisdiction's laws apply to data stored in the cloud. As the

[9] *See id.* at 44-51.
[10] *See id.* at 45, 51-53.

Department pursues greater harmonization and coordination abroad on privacy issues, the ESA urges the Department to continue emphasizing the importance of preserving the United States' balanced and flexible model of privacy regulation that sets out principles for companies to follow but at the same time leaves room for companies to provide those protections in a manner that allows innovation to flourish.[11]

Harmonization of privacy laws is also important within our borders. This is especially true with respect to data breach notification where, as the Department notes, there is a "maze" of current laws on the topic. The ESA agrees with the Department that Congress should enact federal legislation creating a comprehensive data breach framework for electronic records, and it welcomes a dialogue on the particular provisions that would be appropriate for such legislation.

V. CONCLUSION.

The ESA and its members are committed to protecting consumers' privacy as well as developing innovative entertainment software experiences. The ESA believes that the Department's Green Paper offers a number of excellent suggestions, which, if properly developed with appropriate sensitivity to the need for flexibility, can advance both opportunities for innovation and appropriate privacy protection to the benefit of all participants in the digital economy ecosystem.

Respectfully submitted,

Erin M. Egan
Lindsey L. Tonsager
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004

Counsel to the Entertainment Software Association

cc: Michael Warnecke, ESA

[11] *See id.* at iii ("United States Internet policy has avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust in this area. The United States has developed a model that facilitates transparency, promotes cooperation, and strengthens multi-stakeholder governance that has allowed innovation to flourish while building trust and protecting a broad array of other rights and interests.").