Before the
U.S. Department of Commerce
Office of the Secretary; National Telecommunications and Information Administration; International Trade Administration; National Institute of Standards and Technology

In the Matter of the Notice of Inquiry on "Global Free Flow of Information on The Internet"	)	Docket No. 100921457-0457-01

COMMENTS OF THE ENTERTAINMENT SOFTWARE ASSOCIATION

Kenneth L. Doroshow
Senior Vice President & General Counsel
Entertainment Software Association
575 7th Street NW, #300
Washington, DC 20004
(202)-223-2400

December 6, 2010

Introduction

The Entertainment Software Association submits these comments in response to the September 29, 2010 Notice of Inquiry on the "Global Free Flow of Information on the Internet" (NOI).[1] The ESA is the U.S. association exclusively dedicated to serving the business and public affairs needs of companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the Internet.

Providing consumers thrilling new game experiences through the Internet is vital to the present and future success of the video game industry. From gamers wielding dueling guitar controllers separated by thousands of miles, to multiplayer fantasy games in which thousands of players engage in pitched combat, the video game industry harnesses the interactive potential of the Internet like no other entertainment medium. Many factors influence an online game service's success, but everything depends upon our ability to send and receive data using the Internet. No matter how good the game may be, if we cannot reach our customers, then we cannot share our innovative products with them. Barriers to the efficient flow of data across the Internet are problematic, not only for digital distribution of game content but also for protecting that content against theft. Ensuring that information moves across the Internet freely and efficiently is a goal worthy of the Department's best efforts.

The NOI covers a broad range of Internet policy issues, and we commend the Department for its thorough examination of these critical challenges. Many if not all of the issues implicated by this NOI involve highly complex policy considerations where the risk of unintended consequences is great absent a well-thought out policy framework. We trust that this NOI is merely the start of the discussion and that the Department will actively engage with all stakeholders in the months ahead to identify practical solutions to the challenges summarized in the Internet Policy Task Force's forthcoming report. We look forward to working with the Department and other stakeholders in identifying approaches that strike a proper balance between the legitimate interests of government and the needs of businesses and other stakeholders who develop innovative applications and services for the Internet.

Government restrictions on the free flow of information on the Internet can take many forms, including, for example, privacy-related limitations, trade barriers, censorship, and combating fraud and other crimes on the Internet. Our filing is limited to two specific issues: (i) challenges created by certain international privacy restrictions; and (ii) the role of trade policy in improving information flow on the Internet.

[1] 75 Fed. Reg. 60068, Sept. 29, 2010.

1. Privacy-related restrictions

a. How do local restrictions on the free flow of information affect the development of cloud computing services?

Conflicting privacy and data security requirements are among the most significant legal compliance challenges facing operators of cloud computing services in the video game industry.[2] The pathway from an end user to data stored in the cloud may cross national borders. Where the data is stored may differ from where the user accesses the data or where the operator processes the data. There are compelling reasons for organizing a cloud computing service in this manner. It may be more cost-effective to operate a large server farm in one jurisdiction than another or latency considerations may dictate locating certain processing functions closer to the consumer base.

One consequence of this diffuse approach to information management is that it may implicate the laws of multiple jurisdictions simultaneously. Different jurisdictions often impose different legal standards for law enforcement access, data retention, data security, censorship, and national security, among other requirements. What may be required by one country's laws and regulations may contravene or be insufficient under another country's standards. For example, one country may mandate a six-month data retention period where another country may specify 18 months. Data held in one jurisdiction may be relevant in a criminal investigation occurring in another jurisdiction. And an operator that complies with a request from law enforcement in one country may risk violating the privacy laws of another country that also asserts jurisdiction over the data. In addition, such conflicts make it much more difficult for an operator of a cloud computing service with global reach to provide local users with both accurate and specific information on how data may be accessed by law enforcement. This in turn impedes the adoption of cloud services, because consumers want assurances that the privacy of online data will be protected by consistent, predictable rules. In short, the uncertainty created by a tangle of competing privacy and security regimes has the potential to hamper the growth of cloud computing services.

It is, of course, the right of each country to develop privacy protections best suited for its citizens. While complete harmonization of substantive laws seems unlikely, there are other options for developing a workable solution.

International privacy frameworks can be an effective tool for addressing these concerns. The U.S.-E.U. Safe Harbor is an excellent model and has made it easier and more cost-effective for U.S. businesses to operate online services in

[2] We appreciate that the focus of this proceeding is not on privacy, and we commend the Department for giving particular attention to privacy issues in its *Information Privacy and Innovation in the Information Economy* NOI. However, some privacy restrictions can be an impediment to the free flow of information on the Internet, and for that reason we think it is appropriate to comment upon that issue here.

Europe than would be the case if the companies had to work directly with Data Protection Authorities in each separate country. The Safe Harbor program is fully enforceable by the FTC and strikes a careful balance between reasonable flexibility and appropriate safeguards. We encourage the Department to consider expanded use of this model to reduce barriers to innovation caused by conflicting international privacy regimes.

b. What restrictions are there on the global free flow of information on the Internet due to government laws or regulations?

Expansive interpretations of national privacy laws that would treat IP addresses as personally identifiable information (PII) amount to a privacy-based restriction on the free flow of information on the Internet. Some countries have interpreted their laws in a way that would create barriers to the collection and use of IP addresses for copyright enforcement purposes.[3]

Treating IP addresses as PII is unnecessary. IP addresses alone do not identify specific individuals; at most, an IP address can sometimes be used to identify the general location or type of device associated with the IP address.

Moreover, treating IP addresses as PII is problematic for the copyright community. It could hamper the ability of copyright owners to measure the magnitude of online infringement and might make it more difficult to identify repeat infringers. Data on the magnitude of online infringement is vital to our industry's ability to inform government policymakers and to engage with them in policy development on enforcement issues. This data is likewise critical to our industry's ability to make well-informed decisions about how best to mitigate losses from online infringements.

Deeming IP addresses as PII might interfere with the ability of copyright owners to enlist the critical assistance of ISPs in forwarding infringement notices to end users. An IP address informs the rights holder of the particular ISP that allocated the IP address to the subscriber (end user) suspected of infringement. The rights holder then sends the IP address to that ISP with a request for the ISP to forward the infringement notice to the corresponding end user. Nothing in this

[3] See, for example, legal analyses of the situation in several member states of the European Union in the reports found at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf and http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf. More recently, in the case of *In re Logistep AG*, BGer [Federal Supreme Court], Sept. 8, 2010, No. 1C-285/2009, IC_295/2009 (Switz.), a divided Swiss Federal Supreme Court appeared to rule that IP addresses may be considered as protected personal information. It is unclear from the ruling statement, however, whether that determination applies to IP addresses in all contexts or only use of IP addresses in conjunction with the particular IP enforcement method in dispute in that case. Compare *EMI Records v. Eircom Ltd.*, [2010] IEHC 108 (Republic of Ireland High Court, Apr. 16, 2010), available at http://www.bailii.org/ie/cases/IEHC/2010/H108.html, finding IP enforcement uses fully compatible with Irish data protection law.

process enables rights holders to actually identify individuals, such as by real name or physical address. Such information is known only to the ISPs and is already protected by their privacy policies.[4] Deeming IP addresses as PII could prevent the copyright owner from collecting the IP address associated with infringing activity in the first place and may further prevent the copyright owner's disclosure of the IP address to the ISP.

Enforcement concerns are only one aspect of the problem. An expansive interpretation of PII to include routine uses of IP addresses could present other practical problems. For example, many game publishers use "age gates" to prevent children from accessing online games geared to an older audience. The ability of publishers to enforce age gates would be compromised if IP addresses were deemed PII. Typically, a publisher enforces its age gate by associating the user's response to the age gate query with the IP address of the device used to access the site. Therefore, a publisher that wanted to avoid collecting IP addresses of certain users would have no way to prevent a child from "back-buttoning" to falsely re-enter a qualifying age or otherwise use the same computer to enter falsified age information.

The unintended consequences of treating IP addresses as PII are likewise relevant here in the United States. A bill pending in the House would treat IP addresses as "covered information."[5] Also, the FTC is considering whether to deem persistent IP addresses as "personal information" for purposes of the COPPA Rule.

The Department could play a useful role in policy development on this critical issue, both here and abroad, by emphasizing the risks of unintended consequences associated with treating IP addresses as PII.

2. Addressing trade barriers to information flow across the Internet

How might bilateral or multilateral trade or other agreements promote the free flow of information over the Internet?

With respect to cloud or other Web-based services are there specific trade disciplines that can enhance market access for all providers and increase legal certainty for potential users?

Existing trade, investment, and intellectual property rules help establish a positive environment for the free flow of information over the Internet. The ESA supports proactive monitoring and enforcement of these rules, in tandem with negotiation of new agreements and implementation of the already-negotiated free trade agreements (FTAs) with Korea, Colombia, and Panama.

---

[4] Of course, if infringement occurs on a personal web site instead of a P2P network, then the IP owner has other means of identifying the owner of the website independent of an IP address.

[5] The BEST PRACTICES Act, H.R. 5777, 111th Cong. § 2(4)(A) (2010).

The WTO Agreement provides trade obligations that broaden market access by foreign suppliers of services and digital content. Since 1998, the WTO "e-commerce moratorium" on duties on electronic transmissions has facilitated duty-free transmission of digital content over the Internet to WTO markets abroad. The commitments that WTO Members have made under the General Agreement on Trade in Services (GATS) may already give cloud-based or Web-based services firms rights to operate abroad and access the Internet – either across borders, or through data centers or other corporate operations on the ground in a host country. The rights flow either from direct commitments by governments, or from commitments under the GATS Annex on Telecommunications, which requires countries making GATS commitments on a service to allow suppliers of that service to access and use the public telecom transport network – including the Internet.

U.S. FTAs enhance market access by providing high-standards protection for U.S. service exporters. FTAs guarantee market access and freedom from discrimination for businesses delivering services cross-border or through investment in FTA partners. The investment chapters of U.S. FTAs, and U.S. bilateral investment treaties (BITs), back up these market access rights with strong guarantees against expropriation and unfair treatment that greatly benefit U.S. companies that invest to provide services.

Without the GATS or U.S. FTAs, services firms and users run the risk that a trading partner will take arbitrary action inflicting damage that will never be remedied. These trade and investment agreements reduce or prevent a chilling effect on services.

For these reasons, the ESA supports early Congressional approval of the Korea-US FTA. The ESA also supports negotiation of advanced e-commerce provisions in the Trans-Pacific Partnership negotiations.

Conclusion

We applaud the Department's commitment to better understand the challenges that restrictions on information flow place upon American business and global commerce. The Internet is a vital conduit for commerce and continues to be a source for new innovations and jobs growth. We look forward to working with the Department to preserve and promote the free flow of information on the Internet.

ENTERTAINMENT SOFTWARE ASSOCIATION

By: /s/ Kenneth L. Doroshow

Senior Vice President & General Counsel
Entertainment Software Association
575 7th Street NW, #300
Washington, DC 20004
(202) 223-2400