



Professional Association of Exporters and Importers

“Leaders and Partners in Worldwide Regulatory Compliance”

May 2010

Volume 24, Number 1

PAEI Board of Directors:

Call for Nominations and Letters of Intent

By Jo-Anne Daniels, PAEI President

It is time to elect new Directors for the Board of PAEI.

This year we have two PAEI Board of Director positions open for the term which begins 2011 and ends 2013. We want to welcome new members to sit on the Board for the next three years.

PAEI was formed over 20 years ago in response to the changes in export controls with the mission to offer quality educational programs, and networking opportunities to those professionals involved in import and export activities. The board is looking for new ideas and opportunities to make an investment in the education of our members.

Holding a PAEI board position is your door to opportunity. Many members have shared with us that they learned about their current position through PAEI and others related that they found opportunities through networking that led to career advancement.

I would like to thank each and every member who would consider running for a Director position. The door is open at PAEI and we value new talent and energy. Please give me a call on 650 438-1411 or e-mail me at jo@trade-resources.com and I will answer your questions about the Director position and responsibilities. I look forward to hearing from you and hope to receive your nomination and completed [letter of intent](#).

Sincerely,

Jo-Anne Daniels
 PAEI President & Board Member
 Trade Resources & Associates, President
 650 438-1411 jo@trade-resources.com

Inside this issue:

| | |
|---|---------|
| PAEI Elections | Cover |
| PAEI Board of Directors and Officers Contact Information | 2 |
| Commodity Specialist Teams and Field Director of Audit Recap and pictures | 3 |
| Commercial Encryption Seminar Recap and pictures | 4 |
| U.S. Customs Proposes Two Changes to Record-keeping Requirements For Brokers | 5 |
| Fact Sheet on the President’s Export Control Reform Initiative - Press Release from The White House | 5 – 6 |
| Protecting Code As Free Speech : Keeping the Internet Open, Free and Publically Available to the World – Taking the Next Step | 6 - 13 |
| PAEI Members Forum | 14 |
| PAEI LinkedIn Members Only Group | 14 |
| BIS STELA System | 14 |
| PAEI Membership Directory | 14 |
| Upcoming Events | 14 |
| Foreign Corrupt Practices Act – When Favorable Actions Become Actionable Favors - Compliance, Culture and Internal | 15 |
| Upcoming BIS Seminar “EMCP” | 16 - 17 |
| Watch Us Grow! | 18 - 19 |
| P.A.E.I. Membership Application | 20 |

**ZERO IN ON THE
RIGHT EMPLOYEE!**

We'll advertise them free of charge!

**Advertise your job
openings with P.A.E.I.!**

Detailed instructions on how to post jobs are
available at <http://www.paei.org/>

Visit our web site for meeting
details, membership information, and
valuable trade resources.

<http://www.paei.org/>

Board of Directors; Fatima Guadamuz-Cabral, Tansie Iwafuchi, Gieselle Perez, Laura Putnam, Loree Stevens

Officers; President - Jo-Anne Daniels; VP of Administration - Open; VP of Development - Carla Ventura; Secretary - Peggy Williams; Treasurer - Dan Kromat

Committee Chairs; Education, Open; Marketing, Tansie Iwafuchi; Membership, Open; Programs, Open; Publications, Open

Publisher; Karen Hebert, Direct Mail Services

Articles for publication, letters to the editor, and requests for copies should be submitted to karen.hebert@paei.org. Articles must be submitted to the Editor NLT the 3rd of each odd month, Newsletters will be emailed the 1st of each even month. P.A.E.I. does not guarantee the accuracy of the contents of this publication. For further information concerning the topics in the newsletter consult the applicable regulations or your local Department of Commerce or Customs representative. 2009 P.A.E.I., Inc. All rights reserved.

P.A.E.I. NEWSLETTER

*Published bimonthly by the Professional Association
of Exporters and Importers, P.O. Box 612743, San
Jose, CA 95161-2743;*

*Message Center (408) 532- PAEI, or (800) 930-PAEI.
Fax: (408) 274-7611*

<http://www.paei.org/>

2009 P.A.E.I. Board of Directors/Officers

President

Jo-Anne Daniels
Trade Resources & Associates
Jo-Anne.Daniels@paei.org

Director

Loree Stevens
Finisar Corporation
Loree.Stevens@paei.org

Director

Gieselle Perez
NVIDIA Corporation
Gieselle.Perez@paei.org

Director

Tansie Iwafuchi
Tansie.Iwafuchi@paei.org

Treasurer

Dan Kromat
Varian
Dan.Kromat@paei.org

Director

Laura Putnam
Symantec Corporation
Laura.Putnam@paei.org

Director

Fatima Guadamuz-Cabral
Transnational Trade Services
Fatima@paei.org

Secretary

Peggy S. Williams
FedEx Express
Peggy.Williams@paei.org

CSTs and Regulatory audit visit to South Bay

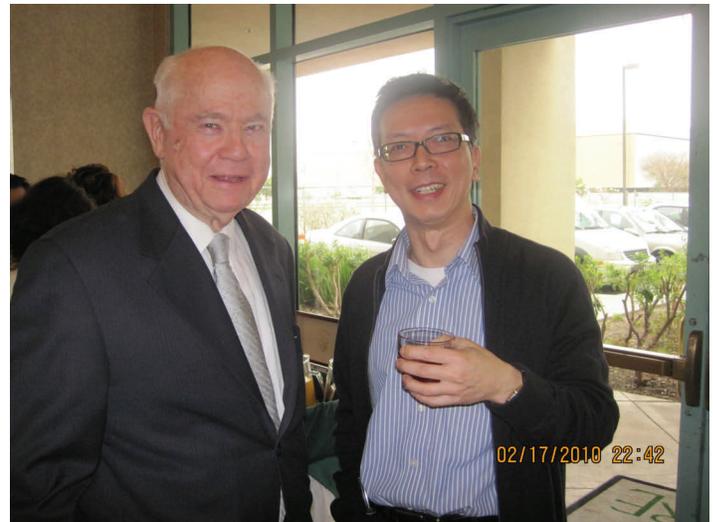
By Gieselle Perez, PAEI Director

On Feb 18th PAEI had the pleasure to host the CSTs from Teams 770, 771 and Betty Williams from Regulatory Audit at the Biltmore. Attendance at this event was phenomenal. We had over 70 attendees. The room was packed and attendees were captivated by the vast amount of information provided by the teams. The teams went over classifications of semi-conductor equipment, mass flow controllers, PC mo-



dem cards to everyone's favorite ball bearings. Prior to the break Betty Williams, Field Director Regulatory Audit provided information on QRAs, FAs and their selection process. She provided statistics from the over 1000 FAs performed. Some of the alarming stats demonstrated that 57% of FAs concluded unacceptable with the top areas on unacceptable compliance being value, duty free provisions and classifications. The seminar concluded with a legal overview by George Tuttle. George spoke to those areas of concern in FAs, namely value and classification.

PAEI would like to thank all the speakers that were able to make this event a success. We hope we can make this a yearly event.



“Commercial Encryption “Roadmap” Program

By Jo-Anne Daniels, PAEI President

March 15th PAEI had the pleasure to host the *Commercial Encryption Roadmap* program, PAEI’s first global encryption program.

Dan Fisher-Owens from Berliner, Corcoran & Rowe LLP kicked off the program delivering a presentation focusing on U.S. encryption regulations. He provided the crypto basics and then explained why crypto is so complicated. He also talked about the requirements that were removed, such as “ancillary crypto.” He discussed what to expect in the future and some practical applications including how to build crypto reviews into the business process. Dan included a great deal of support documentation for those who want to dig even deeper into encryption classifications and requirements.



Dan was followed by Helen King, Director of Global Trade Compliance at Symantec Corporation. Her topic was to speak about foreign encryption controls. Her objectives were that at the end of the seminar all attendees would be able to recognize and apply foreign government import requirement for products that contain encryption functionality and incorporate best practice into their export control programs at home. Helen took us on an encryption tour that



included France, Israel, Hong Kong, China, Russia, Brazil, India, South Africa, UAE, Saudi Arabia and Singapore. Additionally Helen generously included appendices with some great resources.

Attendees who completed the program survey thanked PAEI for putting together great events such as this program and wanted more information about how to implement a robust compliance system for encryption products. One attendee said the program far exceeded their expectations and they thought the subject matter was spot on, presenters were organized and they provided great handouts. Many attendees wished more time was allowed for the speakers who had so much material to share. Therefore, when planning future encryption programs, PAEI will devote a full day to focus on U.S. and foreign encryption controls.



U.S. Customs Proposes Two Changes To Recordkeeping Requirements For Brokers

By George R Tuttle, III, PAEI Member

March 24, 2010

U.S. Customs and Border Protection (CBP) published a proposal in the March 23, 2010 [Federal Register](#) to change some of the recordkeeping requirements for licensed customs brokers. Specifically, CBP proposes to allow brokers to maintain records off-site anywhere within the U.S. Customs territory, provided that the records can be provided to CBP within a reasonable time period upon request by CBP. CBP also proposes to remove the requirement, currently applicable to brokers who maintain separate electronic records, that certain entry records must be retained in their original format for the 120-day period after the release or conditional release of imported merchandise.

CBP is making these changes to conform with the practice of many businesses to prepare, store and transmit documents in electronic format. The new requirements would also allow CBP to remove duplicative recordkeeping requirements without hindering its ability to monitor and enforce customs recordkeeping requirements.

CBP invites public comment on these proposed changes. Any comments must be received by CBP on or before May 24, 2010.

For assistance or additional information, please contact George Tuttle, III at (415) 986-8780 or george.tuttle.iii@tuttlelaw.com.

George R. Tuttle, III is an attorney with the Law Offices of George R. Tuttle in San Francisco.

Fact Sheet on the President's Export Control Reform Initiative

Press Release from The White House

April 20, 2010

Earlier today, Secretary of Defense Robert Gates discussed the Administration's interagency review of the U.S. export control system, which calls for fundamental reform of the current system in order to enhance U.S. national security and strengthen our ability to counter threats such as the proliferation of weapons of mass destruction.

President Obama, in August of last year, initiated this comprehensive review to identify possible reforms to the system. Although the United States has one of the most robust export control systems in the world, it is rooted in the Cold War era and must be updated to address the threats we face today and the changing economic and technological landscape.

The assessment was conducted by an interagency task force created at the direction of the President and included all departments and agencies with roles in export controls. The assessment found that the current U.S. export control system does not sufficiently reduce national security risk based on the fact that its structure is overly complicated, contains too many redundancies, and tries to protect too much.

The current system is based on two different control lists administered by two different departments, three different primary licensing agencies (none of whom sees the others licenses), a multitude of enforcement agencies with overlapping and duplicative authorities, and a number of separate information technology systems (none of which are accessible to or easily compatible with the other), or agencies with no IT system at all that issues licenses. The fragmented system, combined with the extensive list of controlled items which resulted in almost 130,000 licenses last year, dilutes our ability to adequately control and protect those key items and technologies that must be protected for our national security. The goal of the reform effort is "to build high walls around a smaller yard" by focusing our enforcement

(Continued on page 6)

(Continued from page 5)

efforts on our “crown jewels.”

The review’s overall findings have the full support of the President’s senior national security team.

Key Recommendations

The Administration has determined that fundamental reform of the U.S. export control system is needed in each of its four component areas, with transformation to a:

- Single Control List,
- Single Primary Enforcement Coordination Agency,
- Single Information Technology (IT) System, and
- Single Licensing Agency.

Implementation

The Administration will engage with Congress to consult and seek its input on the proposed reforms. To deploy the new system, the Administration has prepared a comprehensive, three-phase approach and is currently moving forward to make specific reforms which can be initiated immediately and implemented without legislation. The approach will make the necessary changes to the current system to transition it to the revised, enhanced system in Phase III:

- **Phase I** makes significant and immediate improvements to the existing system and establishes the framework necessary to create the new system, including making preparations for any legislative proposals. This phase includes implementing specific reform actions already in process and initiating review of new ones.
 - **Control List** – refine, understand, and harmonize definitions to end jurisdiction confusion between the two lists; establishes new independent control criteria to be used to screen items for control into new tiered control list structure.
 - **Licensing** – implement regulatory-based improvements to streamline licensing processes and standardize policy and processes to increase efficiencies.

- **Enforcement** – synchronize and de-conflict enforcement by creation of an Enforcement Fusion Center.

- **IT** – determine enterprise-wide needs and begin the process to reduce confusion by creating a single U.S. Government (USG) point of entry for exporters.

- **Phase II** results in a fundamentally new U.S. export control system based on the current structure later this year. This phase completes deployment of specific Phase I reforms and initiates new actions contingent upon completion of Phase I items. Congressional notification will be required to remove munitions list controls or transfer items from the munitions list to the dual-use list, and additional funding will be required both for enhanced enforcement and the IT infrastructure.

- **Control List** – restructure the two lists into identical tiered structures, apply criteria, remove unilateral controls as appropriate, and submit proposals multilaterally to add or remove controls.
- **Licensing** – complete transition to mirrored control list system and fully implement licensing harmonization to allow export authorizations within each control tier to achieve a significant license requirement reduction which is compatible with national security equities.
- **Enforcement** – expand outreach and compliance.
- **IT** – transition toward a single electronic licensing system.
- **Phase III** completes the transition to the new U.S. export control system. Legislation would be required for this phase:
 - **Control List** – merge the two lists into a single list, and implement systematic process to keep current.
 - **Licensing** – implement single licensing agency.

(Continued on page 7)

(Continued from page 6)

- Enforcement – consolidate certain enforcement activities into a Primary Enforcement Coordination Agency.
- IT – implement a single, enterprise-wide IT system (both licensing and enforcement).

<http://www.whitehouse.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative>

**PROTECTING CODE AS FREE SPEECH:
KEEPING THE INTERNET OPEN, FREE AND
PUBLICALLY AVAILABLE TO THE WORLD
– TAKING THE NEXT STEP**

By: Dan Minutillo , PAEI member

I. INTRODUCTION

Wherever I travel in the world, as I open my laptop and click on a browser to engage the internet, I assume that Firefox or Safari or MS Explorer will be available to me so that I can open and search for the site of my choice, free and without government interference. I also assume that I could download, update, or modify the browser of my choice and any application, bell or whistle, available for use on that browser, again, without government interference. I blindly open my browser on my laptop or download an application from the internet without a second thought expecting it to pop up on click command, and it usually does. For the non-technically inclined, this happens magically on the click of a mouse or stroke of a key. For those who spend their waking hours arguing, writing, lobbying and cajoling to keep the internet open, free and publically available, this magical click has come at great expense.

The exchange of code¹ to create, improve and deliver a browser or any downloadable application is happening as you read this article at some place in the world no matter what time of day or night your read-

ing preference may be. This process takes place 24 hours per day, 7 days per week, oblivious to most people and hidden behind veils existing in cyberspace. The code created might contain cryptographic² algorithms created in the United States and controlled by most governments on import or export, whether transferred by download or otherwise. Code of United States origin³ is exchanged worldwide even in and out of countries embargoed⁴ by the United States including Iran, North Korea, and Cuba, alleged enemies of a free and open society.

The download of code is an export defined by the United States Government as the transmission or shipment of goods⁵ leaving the shores of the United States. The export of products or technology to or from embargoed countries is prohibited, controlled, and considered a punishable act by various agencies of the United States Government including the Department of Commerce, Bureau of Industry and Security and the Department of Treasury, Office of Foreign Assets Control, if done with scienter. But code used to create browsers and applications is downloaded and exchanged openly and freely between companies and individuals in the United States and their counterparts in embargoed countries without penalty or other ramifications by the United States Government. This is true even if the code exchanged contains cryptographic algorithms controlled by the United States Government for National security purposes. Why?

II. BACKGROUND

What prompted this article is a recent, successfully concluded discussion with the United States Government on behalf of a client who produces a product used by about one-third of the internet consuming public around the world. This product of United States origin is created online through the exchange

(Continued on page 8)

(Continued from page 7)

of code amongst engineers and technicians around the world, even those in embargoed countries, and even though parts of the code may contain controlled algorithms. Oddly enough, immediately subsequent to concluding this matter, arguably, the Government expanded, that is, liberalized the rules affecting such code by an Advisory Opinion⁶ which can be stretched to its logical conclusion to build an even more liberal interpretation of export regulations in favor of commercial and nonprofit companies who exchange such code as product or technology. On behalf of our client, a Voluntary Self Disclosure⁷ (VSD) was filed with the United States Government only in an abundance of caution knowing that there was no violation for any conduct mentioned in, or related to, the disclosures presented in the VSD. After investigation, the United States Government concluded likewise, issuing a No Violation/No Action letter⁸ to the client in July of 2009.

The primary thrust of the VSD relates to the interpretation of *Junger v. Daley*, 209 F. 3d 481 (6th Cir. 2000); *Bernstein v United States*, 922 F. Supp 1426 (1996), 945 F. Supp. 1279 (1996), and at 176 F. 3d 1132 (9th Cir. 1997); and *Karn v United States Department of State*, 925 F. Supp. 1, 9-10 (D.D.C. 1996), remanded, 107 F. 3d 923 (D.C. Cir 1997), asserting that the client's conduct as mentioned in the VSD is protected by the United States Constitution, as free speech under the First Amendment. Though the client's conduct falls squarely within the confines of the above cited cases, by way of argument, secondarily, the VSD cites use of the Technology and Software Unrestricted (TSU) exception⁹ found at the Export Administration Regulations (EAR) 740.13, particularly the Note to paragraph (e) of the EAR¹⁰, relating to a disclaimer of knowledge.

Please note that the TSU analysis in the VSD was secondary to the "free speech" case law analysis as cited above.

As to the free speech argument, any and all computer code not considered classified by, or, not for official use only (FOUO) of the United States Government, which is open source, freely and publically available, exchanged for any non prohibited end use is protected under the case law cited as free speech. The case law is clear. The exchange of publically available, open source, free, unclassified, and non FOUO code of the United States origin transferred between any persons or companies in any country, for any non prohibited purpose furthers the United States Government's charter promoting free speech throughout the world. Code is no different, in accordance with the cases cited, than words; and the exchange of such is Constitutionally protected¹¹ at least within the confines of the restrictions mentioned in this paragraph. Therefore, the easiest way for the United States Government to deal with the VSD, which resulted in the issuance of a No Violation Letter, is to use this freedom of speech analysis. It directly applies, is difficult to refute, advances a case law grounded theory, and promotes our Government's Constitutional guarantee of free speech throughout the world.

Right after issuance of this No Violation Letter, a tremendous amount of commercial company inquiry was addressed to the Government regarding this matter forcing it to explain what may have been unclear before – that with a few exceptions, companies offering the download of code in an open, free, and publicly available setting are generally protected from Government regulation due to free speech protections contained in the United States Constitution. From an export law view, this holds true, without repercussions from any agency of the United States Government

(Continued on page 9)

(Continued from page 8)

even if that code contains controlled algorithms, mass market¹² or otherwise, and even if exchanged in an embargoed country. So, based on this analysis, the No Violation Letter as related to the VSD is well grounded.

III. THE NEXT STEP FORWARD: DOES THE GOVERNMENT'S ADVISORY OPINION STRETCH THE LAW TO CLOSED-SOURCE SOFTWARE AND TO NON ANONYMOUS DOWNLOADS IN SPECIFIC SITUATIONS?

As mentioned supra, a Government Advisory Opinion immediately followed the conclusion of this matter. That Advisory Opinion is provided in full below.

“September 11, 2009

Thank you for your advisory opinion request dated August 10, 2009 in which you asked whether a company would be in violation of the Export Administration Regulations (EAR) if it allowed certain encrypted software, reviewed and classified by BIS as “mass market,” to be downloaded free of charge to anyone from the company’s website without restriction.

Publishing “mass market” encryption software to the Internet where it may be download by anyone neither establishes “knowledge” of a prohibited export or reexport nor triggers any “red flags” necessitating the affirmative duty to inquire under the “Know Your Customer” guidance provided in the EAR (see 67 Fed. Reg. 38857, June 6, 2002). Therefore, a person or company would not be in violation of the EAR if it posts “mass market” encryption software on the Internet for free and anonymous download and then at a later time the software is

downloaded by an anonymous person in Iran, Cuba, Syria, Sudan or North Korea.

You also asked whether the company or person posting the software may require registration – i.e., provision of a name and email address – before downloading may occur. In this case, the download of the software would not be considered anonymous and therefore allowing the download by a person in Iran, Cuba, Syria, Sudan or North Korea without the necessary licenses would constitute a violation of the EAR.

A violation would not occur if the IP address of the person downloading the software is collected by the software provider at the time of the download and stored as a “footprint” in the machine code of the software provider’s data base, but is not tracked or used for any purpose by the software provider.

Please note that this advisory opinion is confined to interpretation of the EAR, and does not address the sanctions regulations implemented by the Office of Foreign Asset Control of the U.S. Department of Treasury.

Sincerely,

C. Randall Pratt

Director

*Information Technology Controls Division
Office of National Security and Technology
Transfer Controls”*

Because of the above mentioned Constitutional protections for open source, free and publicly available code, the Advisory Opinion must be restricted to exported code not meeting the open source criteria mentioned in the above referenced case law, but containing mass market encryption. Because the Advisory Opinion covers controlled technology

(Continued on page 10)

(Continued from page 9)

(cryptography) of a very specific sort, and does not, and cannot, reach the exchange of already Constitutionally protected publicly available code. The Advisory Opinion reaches beyond the code covered by the case law and allows the general publication of *all* mass market software, whether offered with publicly available source code or not, so long as the criteria in the Advisory Opinion are met. This expansion is logical, since it makes little sense, considering the goals of the export regime to restrict publication of encryption code based on whether the publisher decided to offer its software with or without open or public source.

A. The Advisory Opinion is broken up into three parts:

1. The second full paragraph of the Advisory Opinion: The issue of anonymous downloads is addressed in this paragraph of the Advisory Opinion to show that so long as software is published online, then there is no violation of any export regulation even if a person or entity from an embargoed/sanctioned country like Iran, Cuba, Syria, Sudan or North Korea downloads it so long as the general publication is without tracking. In this scenario, this does not trigger any of the “knowledge” concerns underlying export restrictions (no knowledge, so no violation).

Open source, freely and publicly available code, which includes mass market encryption, is not the subject of this paragraph of the Advisory Opinion because such code is already Constitutionally protected in accordance with the line of cases noted above, knowledge or otherwise.

2. The third full paragraph of the Advisory Opinion: Though not the subject of this article,

the issue of registration before download to negate anonymity tripping a violation of the EAR is addressed in the third full paragraph of the Advisory Opinion (knowledge no violation)¹³; and

3. The fourth full paragraph of the Advisory Opinion: The issue of non anonymous downloads with a stored footprint is addressed in the fourth full paragraph of the Advisory Opinion (knowledge but no violation).

The fourth paragraph of the Advisory Opinion addresses whether the guidance provided in the second paragraph, allowing for general downloads for both open source and closed source software, is undermined by the ordinary practice of many internet download sites of collecting and storing internet protocol addresses. Here, the Advisory Opinion analysis correctly broadens the EAR to cover and to protect the export of mass market encryption code, even to embargoed countries, and even if such code is not open source, publicly and freely available, and even if the IP address of the person downloading the code is collected (not anonymous) by the company provider at the time of the download so long as it is stored as a footprint in machine readable code format in the company provider’s data base, not used to affirmatively track the location of the person downloading the encryption software or used for any other purpose. The mere collection of it does not trigger the “knowledge” requirement to prohibit the export. Put another way, so long as this footprint criteria is met, the export of mass market encryption software would not be considered a violation of the EAR even if the IP address of the person downloading the software is known, whether or not that address is located in an embargoed country.

Therefore, the combination of the second and fourth paragraphs means that the Advisory Opinion has

(Continued on page 11)

(Continued from page 10)

clearly broadened the interpretation of present export regulations by applying non Constitutional protections available to commercial and non commercial companies providing mass market encryption code to 1) include both open source and closed source code, and 2) allow collection and storage of IP addresses as described. These conclusions are inescapable considering the case law protecting open source code publication as free speech and the language in the second and fourth full paragraph of the Advisory Opinion, so long as the requisite footprint is collected.

To move this concept one step farther, based on a literal reading of the Advisory Opinion, it appears to negate the need to comply with the requirements of the TSU exception in the two scenarios discussed; if the code is open or closed source and if the footprint requirement is met by the provider (and it is not tracked or used for any purpose). Neither the second nor the fourth full paragraphs of the Advisory Opinion seem to be based on the TSU exception. This appears to be a step forward from the existing regulations regarding TSU.

Additionally, given the Advisory Opinion, it is difficult to see what difference it would make from an EAR violation view if the code is available commercially, for a cost, but the footprint requirement mentioned in the fourth full paragraph of the Advisory Opinion is met. It seems that this should still be considered a “no violation” even if a download occurs into embargoed countries. Given the proliferation of low-cost “Apps” and other software available for download for a small fee, it makes no sense to differentiate based on whether the software is sold or is provided for free. This is especially the case given the growing use of this sort of software for free

speech and pro-democracy purposes in those embargoed countries, as seen recently in the protest in Iran and China where American downloaded Apps and software were used to publicize pro-democracy protests and provide information to the world about human rights atrocities being conducted. The interpretation provided in the second and fourth full paragraphs of the Advisory Opinion should apply to all Apps and software containing mass market encryption so long as the footprint requirement in that paragraph is met. It is nonsensical to interpret the fourth paragraph otherwise.

IV. CONCLUSION

Finally, to move this logically even further, the language in the Advisory Opinion seems to be restricted to encryption, why? It appears that the Advisory Opinion creates a situation in which software with encryption in it, is subject to *less* regulations than benign, non crypto products which provide, for example, “weather “or “world time”. Of course such products should be of less importance to the United States Government for security purposes than products that use or contain encryption. This is even more troubling for software with affirmatively pro-free speech purposes – social networking software, blogging, micro-blogging tools relied upon by pro-democracy, human rights activists in China, Iran, Cuba and elsewhere. It makes no sense for this sort of software to face more restrictive licensing schemes than software with encryption capability. If the criteria regarding a footprint in the fourth paragraph of the Advisory Opinion are met, then why restrict the download of such non crypto products? It seems odd that products which use or contain mass market encryption could be downloaded based on the Advisory Opinion but benign, non crypto products like “world time” Apps and software currently being

(Continued on page 12)

(Continued from page 11)

used to promote United States interests such as blogging software, could not be so exported under the same criteria.

Where does that leave us regarding the Advisory Opinion? Relying on the second and fourth full paragraphs, using the above analysis, it appears that mass market encryption code, whether open or closed source, and other code which can be downloaded, meeting all the criteria discussed above, should be exportable by download without a violation of the EAR anywhere in the world without an export license, so long as the requisite footprint is kept in machine readable code in the provider's data base and is not tracked or used for any purpose by the provider without having to rely on the TSU exception. The Advisory Opinion should be clarified to provide that non encryption software provided for cost should be exportable, subject to the same standards as software without encryption (footprint so no restriction). Moreover, it appears that the United States Government should reconsider why merely collecting an email address and name of a downloader without more should reasonably trigger "knowledge" for purposes of the export regulations.

¹ A system of letters, numbers, or symbols into which normal language is converted to allow information to be communicated briefly and/or electronically making it difficult for the interceptor or hacker to decipher or understand.

² Relating to codes and secret writing; relating to or using cryptography, changing plain text to cipher text and back again.

³ Created in the United States or from the United States technology.

⁴ An embargo is the prohibition of commerce and trade with a certain country (presently embargoed by the United States are Iran, Cuba, Syria, Sudan, or North Korea) in order to isolate it and to put its Government into a difficult internal situation, given that the effects of the embargo often make its economy suffer from the initiative.

⁵ Merchandise, downloads, supplies, raw materials, and products or any other item leaving the shores of the United States and controlled by the United States Government on export for any reason.

⁶ Advisory opinions are official interpretations and applications of a Government agency's rules and regulations, with wide application when the Government makes the opinion public. If requested, for a given end-use, end-user, and/or destination, the Government will advise also whether a license is required, or likely to be granted, for a particular transaction.

⁷ A narrative account with supporting documentation that sufficiently describes suspected violations of trade regulations. A VSD reflects due diligence in detection and correcting potential violations when required information was not reported or when incorrect information was provided to the Government. A VSD can lead to mitigating factors regarding civil penalties as long as the violations are discovered and identified before a Federal government agency identifies the problem.

⁸ After filing a VSD, the appropriate Government agency can decide that there has been "No Violation" of trade law and that no Government action will be

(Continued on page 13)

(Continued from page 12)

taken against the person or company that submitted the VSD.

⁹ EAR at § 740.13, Technology and software—unrestricted (TSU). This license exception authorizes exports and reexports of operation technology and software; sales technology and software; software updates (bug fixes); “mass market” software and encryption source code (and corresponding object code) that would be considered publicly available under § 734.3(b)(3) of the EAR.

¹⁰ The Export Administration Regulations are a set of federal regulations that regulate the export and re-export of most commercial and dual use items.

¹¹The First Amendment of the United States Constitution protects the right to freedom of speech and freedom of expression from government interference. See U.S. Const. amend. I. Freedom of expression consists of the rights to freedom of speech, press, assembly and to petition the government for a redress of grievances, and the implied rights of association and belief. The Supreme Court interprets the extent of the protection afforded to these rights. The First Amendment has been interpreted by the Court as applying to the entire federal government even though it is only expressly applicable to Congress. Furthermore, the Court has interpreted the due process clause of the Fourteenth Amendment as protecting the rights in the First Amendment from interference by state governments. The cases cited in the VSD and in this article, equate software code with protected speech.

¹² Mass market software is generally available to the public by being sold at retail selling points, or directly from the software developer or supplier by means of over-the-counter transactions, mail-order

transactions, telephone transactions, or electronic mail.

¹³ Global web email services like, Gmail, Yahoo, Hotmail and others, as well as international internet service providers like AOL, provide email addresses that often give no indication of the actual location of the address holder (i.e., Joe@gmail.com, Jane@aol.com). Similarly, merely knowing a person’s name does not reasonably place a publisher on notice of whether a person is downloading from the United States or abroad, much less from Iran, Cuba, Syria, Sudan or North Korea. It is not reasonable to assert that the mere collection of names and e-mail address before downloading gives sufficient knowledge to the publisher to trigger any further obligations under the export regulations.

If you have a question about this article, contact Dan at dan@minutillolaw.com, telephone 408 998 8900, or visit the Firm website at www.minutillolaw.com.

Dan Minutillo is the author of numerous articles on global trade law and government contract law. He has taught law for UCLA, lectured at universities in the United States and to the World Trade Association, among others. Dan received the Coopers and Lybrand Service Provider of the Year Award. Dan has practiced law in Santa Clara County, California since 1977. Dan represents, among others, Google, eBay, Mozilla, Facebook, Nvidia, eHarmony, Western Digital, First Solar, Ning, Silver Spring Networks, Fisker Automotive, and many of the largest law firms in the United States to service their clients. Dan’s practice is limited to global trade law and government contract law.

PAEI Members Only Online Forum

By Gieselle Perez, PAEI Director

PAEI has updated its website to include an open forum where membership can share ideas. The site will require members to log on and create their own alias. The intention of the forum is to allow membership to anonymously share ideas. Once in the forum members can open up topics for discussions or respond to current forums. The forum will allow membership to share ideas on compliance topics. PAEI hopes that this open forum will give membership an environment for the exchange of best practices in trade regulatory compliance.

PAEI has a LinkedIn Group for PAEI Members only

PAEI is also currently on LinkedIn. If you would like to join our LinkedIn group please send an e-mail to Gieselle.Perez@paei.org. Please advise which e-mail address you use on your LinkedIn account and we will send you an invitation to join.

BIS STELA System

Effective 3/15/2010, the STELA voice response system will no longer be available and exporters should only utilize the new on-line STELA system to obtain real time BIS work item status information.

You may now check the status of your export / re-export license applications, classification requests and AGR notifications using the on-line System for Tracking Export License Applications (STELA) at <https://snapr.bis.doc.gov/stela>

Any issues or concerns please contact ITHELP@bis.doc.gov Please visit <http://www.bis.doc.gov/> for more information.

2010 Membership Directory

Has your information changed?

It is that time of year again when we prepare for the new PAEI Membership Directory. We want to make sure that we have all current PAEI members information listed with correct contact information for your membership. If your membership is more than **30 days past expiration**, and you wish to be included, please make sure to send in your membership dues. You can renew online, using a credit card, <http://www.acteva.com//booking.cfm?bevaid=16992>.

Information that is included in the PAEI Membership Directory is as follows:

**Members Name, Title, and Company Name
Telephone Number, Fax Number
And E-mail Address.**

Only current PAID members will be included in the 2010 PAEI Membership Directory.

Upcoming PAEI/BIS Events Mark Your Calendars!

- **May 25, 2010**
[FCPA Trade Meeting](#)
- **September 28 - 29 , 2010**
[BIS "EMCP"
Two Day Seminar](#)

Upcoming PAEI Events Watch for Dates and Details

- **Back to Basics for Exporting**
- **Back to Basics Importing**
- **ITAR**

Watch the PAEI Web site for these and other events, <http://www.paei.org>



Professional Association of Exporters and Importers
“Leaders and Partners in Worldwide Regulatory Compliance”
Trade Conference

**Foreign Corrupt Practices Act – When Favorable Actions Become Actionable Favors -
Compliance, Culture and Internal Controls!**

Corruption is a serious problem in today’s rapidly developing economies and U.S. companies conducting business around the world must take extra caution to prevent FCPA violations. Don’t miss this insightful and practical new event.

Topics to be covered:

- What is the Foreign Corrupt Practices Act?
- What international anti-corruption efforts are underway?
- How is the international supply chain being used to corrupt foreign officials?
- What are the trends in liability?
- Compliance tips for dealing with third parties, whether or not related.
- What methods aside from FCPA can be utilized by the government to pursue companies?
- How companies can protect their officers and directors from criminal penalties.

Speakers:

- Susan Kohn Ross, Counsel - Mitchell Silberberg & Knupp LLP

Date: Tuesday, May 25, 2010

Time: 8:30 am to 12 noon

Registration and continental breakfast will begin at 8:30 am and Program at 9:00 am

Place: Symantec - 350 Ellis Street, Mountain View, CA 94043 **NEW LOCATION**

Cost: \$60 PAEI members, \$75 non-members

To register on line please [click](http://www.acteva.com/booking.cfm?bevoid=202673) here or follow link provided,
<http://www.acteva.com/booking.cfm?bevoid=202673>.

-----Registration closes Monday, May 24 at Noon -----

If you would like to become a PAEI member and attend this event at the member rate, please go to <http://www.paei.org/join.htm> and join now.

Registration questions can be addressed to Karen Hebert at khebertdms@aol.com



**The Bureau of Industry and Security
in Collaboration with
The Professional Association of Exporters and Importers**



Presents

How to Develop an Export Management and Compliance Program

Two-Day Seminar

September 29 - 30, 2010

Santa Clara, CA

Are you interested in learning about smart export compliance business strategies? Looking for effective solutions to address an export compliance problem? On September 29th and 30th, the U.S. Department of Commerce's Bureau of Industry and Security and the Professional Association of Exporters and Importers will host speakers from the Bureau of Industry and Security, the Census Bureau, the U.S. Department of State, and the U.S. Treasury's Office of Foreign Assets Control.

Designed to help companies create or enhance their export compliance programs, this seminar will focus on industry best practices of effective export management and compliance programs. It is designed for companies whose products are subject to U.S. export controls. The objective is to help companies efficiently manage their export compliance requirements by implementing strategies and safeguards that can minimize the risk of an export violation. **This seminar is a must-attend for managers, sales staff, logistics staff, and compliance specialists who already understand the basics and are looking to use that knowledge to design or enhance an effective compliance program for their companies!**

Participants for this seminar should have a working knowledge of U.S. export regulations. This is not a regulatory seminar and does not cover subjects such as how to classify your product or how to determine whether or not your export requires a license. The seminar is for exporters who are ready to utilize their knowledge of export regulations to build an effective compliance program that addresses their export compliance responsibilities. While this is not a seminar for beginners using the Export Administration Regulations, this seminar is targeted to beginners preparing, implementing, and/or reviewing an Export Management and Compliance Program.

About the Instructors:

Officials from the Bureau of Industry and Security, the Census Bureau, the Department of State, and the Treasury's OFAC, will conduct the seminar. The instructors are compliance specialists and will be available throughout the seminar to provide guidance on "best practice" strategies for complying with U.S. export regulations, implementing an effective compliance program, and developing a written export compliance manual. The instructors will also be available for 15-minute one-on-one sessions, on a first come, first-served basis; participants should call or e-mail Orestes Theocharides at BIS' Export Management & Compliance Division directly at (202) 482-6751, [or otheocha@bis.doc.gov](mailto:otheocha@bis.doc.gov), if interested. Among the instructors who will be joining us for both days of the seminar & will be available to the exporting community, is Senior BIS Licensing Officer, Gene Christiansen, of the Office of National Security & Technology Transfer Controls.

When: Wednesday, September 29 – Thursday, September 30, 2010

Time: 8:30 a.m. – 4:45 p.m. on Sept. 29, & 8:30 a.m. – 4:30 p.m. on Sept. 30 (continental breakfast and registration available at 7:30 a.m.).

Location: Hilton Santa Clara, 4949 Great America Parkway, CA 95054.

Hotel Accommodations: Please make your room reservations directly with the Hilton Santa Clara by calling (408) 330-0001.

Reserve your room by Friday, September 10, 2010 to receive the "PAEI" discounted rate of \$155 night + taxes. To register for your hotel room online: http://www1.hilton.com/en_US/hi/hotel/SJCSCHF-Hilton-Santa-Clara-California/index.do. Click the above link or go to www.hiltonsantaclara.com

Fee: \$425.00. This registration fee includes continental breakfast, lunch, and all seminar materials for both days.

Seminar Registration: To register, [click here](#).

The deadline for registration is Friday, September 10, 2010.

No telephone, fax, nor checks will be accepted for registration. **All registrations for this event must be paid in advance and processed using a credit card online, at** <http://www.acteva.com/booking.cfm?bevaid=203737> (VISA, AMX, or MasterCard)

Last day to register is Friday, September 10, 2010. REGISTER NOW!

NO REFUND FOR CANCELLATIONS MADE AFTER Friday, September 10, 2010. PAEI Tax ID#:680117035.

For more information on the seminar, or additional registration information, please contact Karen Hebert at 408-532-7234, or via email at khebertdms@aol.com.



WATCH US GROW!

January 2010

New

| | |
|------------------|-----------------|
| Kathleen Gebeau | Qualcomm Inc. |
| Terrance Perkins | Synopsys Inc. |
| Mary Wong | Roche Palo Alto |

Renew

| | |
|------------------|-------------------------------|
| Geoff Harbell | Alliance International |
| Bill Volner | Allergan, Inc. |
| John Burgess | Omniceil |
| Will Tuupo | Omniceil |
| Rocco Gattuso | International Trade Solutions |
| Jim Stuhlberg | Synopsys, Inc. |
| Tom Mumby | IDT, Inc. |
| Pat Toich | IDT, Inc. |
| Sophia Chan | Zoran Corporation |
| Lee De Los Reyes | Zoran Corporation |
| Yvette Powell | Bare Escentuals Cosmetics |
| Vicky Ng | Bare Escentuals Cosmetics |

February 2010

New

| | |
|------------------|-------------------------|
| Mirona Azimioara | AMCC |
| Peter Michel | |
| Sheryl Felix | Goodrich |
| Lydia McClure | Applied Materials, Inc. |
| Alfred Hille | eCustoms |
| Charles Newton | eCustoms |

| | |
|----------------|----------------------------|
| Archibong Ituh | Aurora Networks |
| Joy Speicher | Space Systems /Loral, Inc. |
| Ruth Vargas | Space Systems/Loral, Inc. |

Renew

| | |
|------------------------|---------------------------|
| Jeff Rittener | Intel |
| John J Morley | Intel |
| Beverly J. Gonzales | |
| Terri Bury | McAfee, Inc. |
| Tammie Rostant | McAfee, Inc. |
| James Koroma | Bartell Drugs Company |
| Colleen Allgeyer | Vishay Americas |
| Darlene Shaffer | Vishay Americas |
| Karon Giovannoni | Matheson-Trigas, Inc. |
| Nicole Malcolm | Novellus Systems, Inc |
| Jane Solomon | Anritsu Company |
| Diana Scholtens | Anritsu Company |
| Mary O'Brien | Seagate Technology, LLC |
| Michelle Scott-Horwitz | Seagate Technology, LLC |
| Jane Watkins | Applied Materials, Inc. |
| Mona Sasamoto | Extreme Networks Inc. |
| Laura Putnam | Symantec Corporation |
| Daniel Swinehart | Palo Alto Research Center |

March 2010

New

| | |
|--------------|--|
| Sharon Roche | Shea Roche Professional Search Consultants |
| Peter Roche | Shea Roche Professional Search Consultants |



Continued from page 19

**WATCH US
GROW!**

April 2010

New

| | |
|-----------------|----------------------------|
| Annamarie Curry | Trimble Navigation |
| Janice Nord | Trimble Navigation |
| Steve Story | Global Trade Solutions LLC |

March 2010 cont'd

Renew

| | |
|----------------------|--------------------------|
| Deborah Ferry | Adaptec, Inc. |
| Larry Sullivan | U.S. Dept. of Commerce |
| Edward Radlo | Radlo & Su LLP |
| Jeff Hopkins | Altera Corp. |
| Angela Colvin | Altera Corp. |
| Anne van de Heetkamp | TradeBeam |
| Wendy Thompson | TradeBeam |
| Justin Hill | Expeditors International |
| Greg Malter | Expeditors International |
| Loree Stevens | Finisar Corporation |
| MaryAnn Omerod | VisionSafe Corporation |
| Cindy Shull Lakey | MK Data Services |
| Amber Jarzombek | RFMW, Ltd. |
| Mark Yee | Life Technologies |
| Katya Winder | Life Technologies |
| Connie Gaston | PerkinElmer |
| John Kim | Perkin Elmer |
| Ron Edmon | Endwave Corporation |
| Chet Gandhi | Endwave Corporation |
| Kati Babinec, Cuseco | Sulzer Pumps US Inc. |
| John Ramirez | |
| Toni Paytas | Thomsen and Burke LLP |
| Mike DeYoung | Dionex Corp. |

Renew

| | |
|-----------------|-----------------------------------|
| Jo-Anne Daniels | Trade Resources & Associates |
| Johanne Dictor | Trade Resources & Associates |
| Nancy Heider | SGI- Silicon Graphics Int'l Corp. |
| Agnes Devera | Ditech Networks |
| Stacy Mendez | Ditech Networks |
| Ray Hirata | Lam Research Corp. |
| Iris Zhang | Lam Research Corp. |
| Aimee Shoemaker | Palm, Inc. |

May 2010

New

| | |
|---------------------|---------------------------|
| Peter Miller | |
| Ariane Wolfe | Applied Geomechanics, Inc |
| Keiko Yu | JSR Inc. |
| Christopher Moehrke | Adobe Systems |

Renew

| | |
|-------------------|------------------------------------|
| Char Henderson | Seki Technotron USA |
| Sherri Fumo | Seki Technotron USA |
| Lillian Lopez | Novellus Systems, Inc. |
| Marc Smith | Logistics & Compliance Specialists |
| Bill Dodge | JSR Inc. |
| Mercedes Aguillar | Adobe Systems |
| Lydia Bostillo | Adobe Systems |



P.A.E.I. Membership Information

The Professional Association of Exporters and Importers is an organization of professionals involved in import/export activities. Objectives of the association include promoting and fostering the role of the import/export professional, providing on-going education relative to regulatory issues, exchanging information and enhancing industry's participation in import/export control issues and policies.

P.A.E. I. sponsors quarterly luncheon meetings with featured guest speakers, a bimonthly newsletter, networking and job placement opportunities.

P.A.E.I. membership represents both large and small companies in the high-technology community. Membership is open to all persons interested in personal and professional growth in the international arena. Two types of memberships are available and are valid for one year from date of payment. For more information call the PAEI Message Center at telephone (800) 930-PAEI.

Complete this application and return it along with your check. Make checks payable to: Professional Association of Exporters & Importers, P.O. Box 612743, San Jose, CA 95161-2743. PAEI's TAX ID NO: 680117035. You may also pay online for your membership at the PAEI web site <http://www.paei.org/>.

Check Membership Choice:

_____ \$25 Student (must be full time student) _____ \$50.00 Individual _____ \$150.00 Corporate**

Name: _____

Title: _____

Phone: _____ Fax: _____

E-mail: _____

Company/Corporate Name: _____

Mailing Address: _____

City, State and Zip: _____

****Corporate members please indicate second name:**

2nd Name: _____

Title: _____

Phone: _____ Fax: _____

E-mail: _____

How did you hear about P.A.E.I.? _____