 Issue 147

Dr. Rao Vepachedu¹, JD, PhD, LLM

CONTENTS

PRIVACY SHIELD
POST PROSECUTION OPPORTUNITIES
Due to globalization, more than 70 percent of the world’s purchasing power is located outside of the United States. Therefore, US companies that export products and services grow faster and are 8.5 percent less likely to go out of business than non-exporting companies\(^2\). US exports of goods and services totaled $2.1 trillion in 2011. Exports are a growing and substantial part of the US economy, accounting for 13.8 percent of our nation’s GDP\(^3\).

Free Trade Agreements (FTAs) have proved to be one of the best ways to open up foreign markets to US exporters. Trade Agreements reduce barriers to US exports, and protect US interests and enhance the rule of law in the FTA partner country. The reduction of trade barriers and the creation of a more stable and transparent trading and investment environment make it easier and cheaper for US companies to export their products and services to trading partner markets. In 2015, 47 percent of US goods exports went to FTA partner countries. US merchandise exports to the 20 FTA partners with agreements in force totaled $710 billion. The United States also enjoyed a trade surplus in manufactured goods with our FTA partners totaling $12 billion in 2015. The US and the EU launched negotiations on the Transatlantic Trade and Investment Partnership (T-TIP) in June 2013\(^4\).

The United States and the European Union already share the largest trade and investment relationship in the world. In 2014, the United States exported $498.4 billion in goods and services to the EU, which was an increase of almost 6 percent from 2013. Over 21 percent of U.S goods and service exports went to the 28 members of the EU in 2014, supporting an estimated 2.6 million US jobs. The top goods export categories to EU were chemicals; transportation equipment; computer and electronic products; machinery, except electrical; and miscellaneous manufactured commodities. In 2013 (latest year available), the top...
US service exports to the EU were charges for the use of intellectual property, other business services, travel (for all purposes including education), financial services, and transport.

Over 97,000 companies exported to the EU in 2013 (latest year available). Of those, 96 percent were small and medium sized enterprises (SMEs) with fewer than 500 employees. Small and medium-sized firms generated almost 30 percent of the United States' total known exports of merchandise to the EU in 2013. The European Union also accounted for $73.8 billion in SME goods exports from the US that year.

However, there was one problem. In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. The objective of this new set of rules is to give citizens back control over their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy. Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations which collect and manage the personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law. Under the EU Data Protection Directive 95/46/EC, personal data can be transferred outside of the European Economic Area (EEA) only when the recipient country provides an “adequate level of protection” for the data and according to the European Commission the US fails to meet that requirement.

Last October, citing Edward Snowden’s revelations about mass surveillance by US authorities, an EU court struck down the Safe Harbor Decision.

Building bridges by dismantling walls to open a new era for transatlantic commerce, by delivering concrete and practical results for the citizens and companies is the goal of the European Union and the United States. To accomplish this goal, the US and the EU developed a new framework called Privacy Shield, which replaces the Safe Harbor, to address the mandatory privacy and cross–border data transfer regulations. As a result of this effort, the US and the EU have signed an Umbrella agreement, representing a major step forward in US_EU relations. The agreement sets high standards for the protection of personal data transferred by law-enforcement authorities. It also strengthens legal certainty and enhances the rights of citizens which in turn will facilitate US_EU cooperation to combat crime, including terrorism. The EU and the US are committed to work together in the implementation of this agreement to ensure that it benefits both citizens and law enforcement cooperation.
On 12 July, the European Commission adopted the US-EU Privacy Shield. This new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers. The new arrangement includes: strong data protection obligations on companies receiving personal data from the EU safeguards on US government access to data; effective protection and redress for individuals; annual joint review to monitor the implementation.

This new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers. The new arrangement includes:

- strong data protection obligations on companies receiving personal data from the EU
- safeguards on US government access to data;
- effective protection and redress for individuals;
- annual joint review to monitor the implementation.

The new arrangement lives up to the requirements of the Court of Justice of the European Union, which had declared the Commission’s 2000 Decision on US_EU Safe Harbor invalid on October 6, 2015.

The US_EU Privacy Shield is based on a system of self-certification by which US organizations commit to a set of privacy principles – the US_EU Privacy Shield Framework Principles, including the Supplemental Principles issued by the US Department of Commerce and contained in Annex II to this decision. It applies to both controllers and processors (agents), with the specificity that processors must be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles.

Some steps before self-certification:
- Determine whether your company is eligible
- Craft a privacy policy that is, or ensure your current policy is, Privacy Shield compliant.
• Establish an independent recourse mechanism
• Have a compliance verification mechanism in place
• Designate a contact for Privacy Shield

The policy must address the organization’s commitment to all seven Privacy Shield Principles: Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse/Enforcement and Liability.

To satisfy the US Department of Commerce that the Human Resources Privacy Policy (HRPP) fully addresses the principles, the policy submitted by the certifying organization must contain a long list of required elements including, among others, the following:

• An identification of all US affiliates that will access transferred personal data and their commitment to adhere to the principles;
• The categories of personal data collected;
• The purposes for the collection;
• The third parties to which data may be transferred;
• A description of data subjects’ access rights; and
• A contact for requests to exercise individual rights and submit complaints.

The HRPP must be posted where it will be available to all EU based employees whose personal data will be transferred to the US subject to the Privacy Shield. This typically means that the policy will be posted on the corporate intranet. Organizations that choose not to publicly post their HRPP will be required to submit the policy with the self-certification form.

EU subsidiaries must take the following steps before transferring their employees’ personal data to the US pursuant to the Privacy Shield. To demonstrate its commitment to compliance to its EU employees (and their representatives) and, if needed, to regulators, the US parent corporation should consider taking the following steps:

• Confirm that EU subsidiaries comply with local requirements for cross-border data transfers to the US.
a. Provide their employees with notice of data processing, including transfer to the US pursuant to the Privacy Shield;

b. Consider local law restrictions on cross-border data transfers, particularly on transfers of sensitive personal data, such as employees’ health information;

c. Confer with works councils or trade unions, if any and if legally required, concerning data transfers to the US; and

d. Depending on the country, register with or notify the local DPA of data processing, including cross-border data transfers.

• Establish policies and procedures to implement the privacy shield privacy principles.
  a. Notice And Choice Principles
  b. Accountability For Onward Transfer Principle
  c. Security Principle
  d. Access Principle

• Establish an annual verification process for the following:
  a. The HRPP privacy policy is “accurate, comprehensive, prominently displayed, completely implemented and accessible”;
  b. The HRPP conforms to the Privacy Shield Principles;
  c. Individuals are informed how to submit complaints, both internally and to the relevant EU data protection authority;
  d. Employees with access to transferred personal data have received training and will be disciplined for policy violations; and
  e. The organization conducts periodic compliance reviews.
  f. The verification must be signed by an authorized corporate representative and must be produced upon request to employees, or in the context of an investigation or complaint proceeding.

• Be prepared to resolve complaints in the EU.
Guide to Self-Certification

1. Confirm Your Organization’s Eligibility to Participate in the Privacy Shield
2. Develop a Privacy Shield-Compliant Privacy Policy Statement and HRPP
3. Identify Your Organization's Independent Recourse Mechanism (Dispute Resolution)
4. Ensure that Your Organization's Verification Mechanism is in Place
5. Designate a Contact within Your Organization Regarding Privacy Shield

Independent Dispute Resolution Service Providers

1. BBB EU Privacy Shield Program
2. DMA Privacy Shield Program
3. EU Data Protection Authorities (DPAs)
4. JAMS Privacy Shield Program
5. ICDR/AAA Privacy Shield Program
6. TRUSTe
POST PROSECUTION OPPORTUNITIES

Under the Enhanced Patent Quality Initiative (EPQI)\textsuperscript{14}, the USPTO currently has three programs designed to encourage compact prosecution after a final rejection:

1) After Final Consideration Pilot 2.0 (AFCP 2.0)
2) Pre-Appeal Brief Conference (PABC)
3) Post-Prosecution Pilot (P3) Program

\textbf{After Final Consideration Pilot 2.0 (AFCP 2.0)}\textsuperscript{15}: The After Final Consideration Pilot 2.0 (AFCP 2.0) has been extended through September 30, 2016. AFCP 2.0 authorizes additional time for examiners to search and/or consider responses after final rejection. Under AFCP 2.0, examiners will also use the additional time to schedule and conduct an interview to discuss the results of their search and/or consideration with you, if your response does not place the application in condition for allowance. In this way, you will benefit from the additional search and consideration afforded by the pilot, even when the results do not lead to allowance.

\textbf{Pre-Appeal Conference}: This pilot program offers applicant who has filed a notice of appeal and who wants a panel of experienced examiners to perform a detailed review of appealable issues within a set period of time, an opportunity to request a review of identified matters on appeal employing an appeal conference currently employed in the Office, but prior to the filing of an appeal brief. The goals of the program are (1) to identify the presence or absence of clearly improper rejections based upon error(s) in facts, or (2) to identify the omission or presence of essential elements required to establish a prima facie rejection. Applicant must file the request with the filing of a notice of appeal and before the filing of an appeal brief\textsuperscript{16}.

\textbf{Post-Prosecution Pilot (P3) Program}: The Post-Prosecution Pilot (P3) Program incorporates the effective features of two programs the AFCP 2.0 program and the PABC program aimed at effective prosecution. The P3 started on July 11, 2016 and runs for 6 months and is limited to 200 requests per technology center (8 centers, a total of 1600 requests). The P3 is open to nonprovisional and international utility applications. There is no fee to participate in the P3, but there are limitations and exclusions\textsuperscript{17}.
REFERENCES AND NOTES

1 Dr. Rao Vepachedu is a registered patent attorney with extensive experience in the management of intellectual property and extensive experience in research and teaching. He currently works for Cardinal Intellectual Property (CIP), Cardinal Risk Management (CRM), and Cardinal Law Group (CLG). In addition, he is the president of Vepachedu Educational Foundation Inc. (www.vepachedu.org), a 501(c) (3) educational foundation. For more information visit: www.linkedin.com/in/vepachedu, http://www.avvo.com/attorneys/60201-il-sreenivasarao-vepachedu-764535.html, and http://www.crm-ip.com/vepachedu.html. Contact: svepachedu@yahoo.com or rao.vepachedu@cardinal-ip.com.


4 FREE TRADE AGREEMENTS: http://trade.gov/fa/

5 Data transfers outside the EU: http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm


12 We read Privacy Shield so you don’t have to: https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/


15 Certification And Request For Consideration Under The After Final Consideration Pilot Program 2.0
http://www.uspto.gov/sites/default/files/forms/sb0434.pdf

16 New Pre-Appeal Brief Conference Pilot Program, OG Notices: 12 July 2005:

17 Post-Prosecution Pilot: http://www.uspto.gov/patent/initiatives/post-prosecution-pilot

- Applicant cannot have previously filed a proper request to participate in the Pre-Appeal or the AFCP 2.0 programs in response to the same outstanding final rejection.
- Once a P3 Request has been accepted, no additional response(s) under 37 CFR 1.116 will be entered, unless requested by the examiner.
- It is also impermissible to request to participate in the Pre-Appeal program or request consideration under AFCP 2.0 once a P3 request has been accepted.

18 In addition to the primary sources cited above, additional references include:

Disclaimer All information is intended for your general knowledge only and is not a substitute for medical advice or treatment for special medical conditions or any specific health issues or starting a new fitness regimen.

"Where the mind is without fear and the head is held high, Where knowledge is free Where the world has not been broken up into fragments, By narrow domestic walls." Rabindranath Tagore (1861-1941), Gitanjali, 1912.

One World One Family
AUM! SWASTI!
Om! Asatoma Sadgamaya, Tamasoma Jyotirmaya, Mritvorma Amritamgamaya, Om Shantih, Shantih, Shantih! (Aum! Lead the world from wrong path to the right path, from ignorance to knowledge, from mortality to immortality, and peace!)
SWASTI! AUM!