https://doi.org/10.48009/1_iis_2016_196-205

Issues in Information Systems
Volume 17, Issue I, pp. 196-205, 2016

U.S. EU SAFE HARBOR & PRIVACY SHIELD: STUDENT EXPLORATION OF GLOBAL IT ISSUES AND PROFESSIONALS WHO DEAL WITH THEM

Lorrie Willey, Western Carolina University, lwilley@email.wcu.edu
Barbara Jo White, Western Carolina University, whiteb@email.wcu.edu
Janet C. Ford, Western Carolina University, jford@email.wcu.edu

ABSTRACT

Globalization of information systems courses is supported not only by the Association to Advance Collegiate Schools of Business but also by current model curriculum guidelines for undergraduate programs in information systems. Though globalization of the information systems curricula is often mentioned in conjunction with a general information systems course, a course in information systems project management, software development, or IT security courses are also ideal areas in which to include a global component. Moreover, combining an exploration of global issues with a practical look at related IT professions, students can experience some of the real-world issues and activities of their chosen profession. This paper explores the concerns surrounding the U.S.-European Union (EU) Safe Harbor and its replacement, the EU-U.S. Privacy Shield, as a global awareness class activity combined with an exercise in IT professions which require a knowledge of those international agreements.

Keywords: Data Security, Safe Harbor, Privacy Shield, Globalization, IT Professions

INTRODUCTION

The recent rise and fall of the U.S.-EU Safe Harbor agreement (Safe Harbor) and the subsequent replacement of that agreement with the EU-U.S. Privacy Shield agreement (Privacy Shield) is an interesting and somewhat alarming look at how business activities can be quickly and extensively impacted by influences external to the U.S., in this case the EU. Globalization is becoming a major player in the IT classroom and using current events and career planning in learning exercises develops student skills at several levels. This paper provides an overview of the privacy issues as related to the U.S.-EU data protection conflict, the rise and fall of Safe Harbor, the new Privacy Shield agreement, and then a teaching exercise that allows students to explore data privacy issues in a global perspective while also exploring professions in which some knowledge of Privacy Shield information is essential.

Globalization in Information Systems and Business Education

A study by the Association to Advance Collegiate Schools of Business (AACSB) addressed the state of globalization in business education (AACSB, 2011). The 2011 report noted various alternative methods for including content in business programs that relate to globalization, defined as the "process" of "extending the reach of educational engagement beyond one's home borders and deepening the richness of understanding about the increasingly global foundation of business" (AACSB, p. 7). The AACSB does not recommend any one method of including global content in business courses (AACSB, 2011) but supports any efforts to provide students exposure to global events. Such exposure, in relation to their studies, will be an important component to a business education and will aid students in gaining a better global understanding (Kedia & Englis, 2011).

In addition to AACSB's encouragement of global studies in business, model curriculum guidelines for undergraduate degree programs in information systems also show increasing support for the inclusion of global and globalization concepts. The Association for Computing Machinery, in collaboration with the Association for Information Systems, has produced model curriculum guidelines in 1997 (Davis, Gorgone, Couger, Feinstein, & Longenecker,), 2002 (Gorgone, Davis, Valacich, Topi, Feinstein, & Longenecker) and 2010 (Topi, Valacich, Wright, Kaiser, Nunamaker Jr., Sipior & de Vreede). While the 1997 guidelines (Davis et al.) provided only a vague reference to global and globalization concepts, by 2010 (Topi et al.), these concepts were included in several

specific recommended courses such as the information systems foundational course, an information systems strategic management course, and a project management course. In addition, global and globalization concepts are also mentioned in several elective courses. The use of supplemental materials involving course-related global events can turn an information systems class into one that will help students develop a broader awareness of their world and profession and to make classroom to real-world connections (Tedford, 2003). Supplemental materials can include charts, maps and news items (White, Hale & Willey, 2014), and a global activity linked to a review of information systems professions adds relevancy to the exercise in a practical way for students. Making a course more relevant to student professional and personal goals, as well as more global, will provide increased value in the content of the course (Muddiman & Bainbridge Frymier, 2009), increased student interest (Sikes, 2010) and increased competency in global knowledge (Hedderich, 2011).

The globalization of business presents myriad challenges for current and future IT professionals as companies seek to comply with different and often conflicting legal standards regarding the collection, handling, distribution, and protection of data, particularly personal data. Businesses depend upon the transfer and manipulation of personal data for a variety of purposes, and an absolute prohibition on personal data transfers between countries would disadvantage business interests as well as consumers on both sides of the border. When international trading partners are confronted with divergent national data protection standards, they must negotiate and implement a mechanism that will satisfy the needs and concerns of both countries.

The now-defunct Safe Harbor agreement and its replacement, the Privacy Shield agreement, illustrate such a mechanism. Studying the concerns that led the European Court of Justice (ECJ) to invalidate the Safe Harbor agreement and how the Privacy Shield agreement addresses those concerns will be beneficial to IT students who may someday find themselves in positions with companies, or even governments, that must grapple with differing data security compliance issues.

FROM SAFE HARBOR TO THE PRIVACY SHIELD

Trade between the United States and the European Union involving personal data transfers from the EU to the U.S. is problematic for U.S. companies since privacy standards for personal data are more defined and stringent in the EU The two governments had to develop the means by which U.S. companies could comply with the laws of the EU While there are several options for compliance to support the $260 billion digital services trade that occurs between the U.S. and the EU (Pritzker, 2016) including model contract provisions, the Safe Harbor and now the Privacy Shield provide self-certifying processes that demonstrate U.S. compliance with EU standards.

Personal Data and Privacy Rights in U.S. and EU

The U.S. Constitution, drafted and ratified before instant and widespread collection and dissemination of personal data was conceived of, does not contain any specific personal privacy language. There is no single, comprehensive federal law that addresses the protection of personal data, nor is there a central governmental body that regulates or oversees the collection, use, and transfer of personal data (Jolly, 2015). To the extent that personal data is protected at the federal level, it is through a variety of laws that focus on particular industries. Examples of federal laws that contain data protection provisions include the Financial Services Modernization Act (2014), popularly known as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountancy Act (2014), and the Fair Credit Reporting Act (2014). Additionally, the prohibition of unfair or deceptive trade practices under the Federal Trade Commission Act (2014) supplies the Federal Trade Commission with grounds to bring enforcement actions against companies found to have wrongfully collected, used, or distributed personal data (Jolly, 2015).

Protection of personal data at the state level is similarly piecemeal. State laws regarding the protection of personal data are far from uniform, and may be grouped by sector, entity type, privacy concern, or some other categorization. Some states require websites to develop, implement, and make available a privacy policy on what data will be collected, who may have access to it, and whether and how an online user may opt out of the data collection. Seventeen states require government websites to establish and implement privacy policies for their websites also (State Laws Related to Internet Privacy, 2016). Thirty-one states have enacted laws addressing the disposal of data or procedures whereby personal information is rendered unreadable. Some of the state data disposal laws apply to

government entities as well as private entities (Data Disposal Laws, 2016). Forty-seven states, the District of Columbia, and three American territories have enacted security breach notification laws that require owners or possessors of personal data to notify the subjects of the data in the event of a breach or unauthorized disclosure (Security Breach Notification Laws, 2016).

The EU takes a broader approach to personal data security, providing more universal requirements and more specific privacy rights protections. Influenced by the United Nations Universal Declaration of Human Rights, which includes the privacy right to be free from the intrusion of others, EU data privacy protections are linked to protections associated with private and family life, home and correspondence. Protection of personal data, defined as information that can identify a person, also serves as a form of respect of a person's private life (European Agency for Fundamental Rights, 2014). Personal data is not to be transferred to entities outside the EU unless that entity has safeguards in place meeting EU standards (United Kingdom Information Commission Office, 2016). Basically, the EU regulations provide that the data must be lawfully processed, used for legitimate purposes, relevant to the need for use, stored only as is necessary, and that transfers of personal data require the subjects' knowledge and the right to object to transfers (European Agency for Fundamental Rights, 2014) Also, data controllers must allow for the correction, blocking or removal of personal data (Data Protection in the European Union, n.d.).

The Rise and Fall of Safe Harbor

Since U.S. companies wanting to do business in the EU must meet the EU's legal requirements for data privacy, systems had to be developed to allow for that trade. While a company could privately attempt to meet all standards set by law, a more universal resolution was found: a negotiated agreement between the U.S. and the EU establishing the means for U.S. companies to certify compliance, called Safe Harbor.

Under Safe Harbor and through a self-certification process, U.S. companies demonstrated compliance with EU regulations. Safe Harbor required: notice to the individual about the purposes for collecting and using personal data, choice for the individual as to whether the information will be disclosed to third parties and used for a purpose for which the data was not initially collected, access to the data by the individual and the ability to correct, amend or delete the data, reasonable security measures to protect the data, relevancy of the data collected for the intended use and the means for individuals to enforce the standards (U.S.-EU Safe Harbor Overview, 2013).

Tensions between the U.S. and EU over concerns that Safe Harbor did not provide sufficient protection and enforcement for EU citizens came to a head with the decision of the ECJ in *Schrems v. Data Protection Commissioner and joined party Digital Rights Ireland, Ltd*. in October 2015 (*Schrems*, 2015). Schrems objected to Facebook transferring his personal data from Ireland to servers in the U.S., and the court expanded its review of the issue to include concerns about American National Security Agency surveillance made known by Edward Snowden. As to Safe Harbor, the ECJ "further observes that in his action Mr. Schrems in reality raises the legality of the safe harbor regime…" (*Schrems,* Paragraph 35). Regarding businesses in the U.S., the ECJ held that Safe Harbor did not uphold the data privacy standards demanded by the EU (*Schrems*, 2015).

For two years prior to the court decision, the U.S. and EU had been working to tighten up Safe Harbor standards to satisfy the demands of the EU. The sinking of Safe Harbor surely increased the pressure to come to some agreement. Without an agreement, U.S. companies were in limbo regarding data transfers from the EU, were unsure of their legal responsibilities and liabilities, and were faced with more time consuming and costly options to meeting the EU standards, such as storing data in the EU or model contracts (Casper, 2015).

The Rise of the Privacy Shield

Fortunately, only about four months after the ECJ decision, the EU and U.S. announced a replacement for Safe Harbor: the new and improved version entitled the Privacy Shield. The Privacy Shield continues to provide U.S. companies with a self-certification process. However, enforcement of the agreement is now more stringent because once a company is certified, U.S. law will address enforcement concerns. Some provisions under the agreement address the ability for individuals to complain and have complaints addressed within a reasonable time, increased cooperation between EU data protection agencies and the U.S. Department of Commerce and Federal Trade

Commission, limiting personal information collected by certifying organizations to only what is relevant, and the compliance notice and choice requirements when data will be transferred to third parties. The Privacy Shield also provides for more governmental monitoring for compliance and includes a new content area allowing EU individuals to address concerns over certain U.S. intelligence activities through a Department of State Ombudsperson (U.S. Department of Commerce, 2016).

The EU approval process of the agreement is not complete. The Working Party on the Consequences of the *Schrems* Judgment expressed its dissatisfaction with the Privacy Shield agreement's U.S. national security exemptions which allow for the collection of some data for national security reasons, the method for a review system and the role of the U.S. ombudsperson. (Statement of the Article 29 Working Party, 2016). But to date, the U.S. has not chosen to amend the agreement to meet those demands (McCarthy, 2016). Moreover, the U.S. must enact legislation to address its obligations under the agreement. During this interim period, U.S. companies must seek out other options, for example EU-approved model contracts, but the likelihood for litigation once the Privacy Shield takes full effect also looms as a threat (Lee, 2016).

STUDENT EXPLORATION OF GLOBAL ISSUES AND IT PROFESSIONS DEALING WITH SAFE HARBOR AND THE PRIVACY SHIELD

The story of Safe Harbor and the Privacy Shield brings global current events into the classroom and highlights the impact that international law and activities have on U.S. business. To increase student engagement, it is possible to focus the discussion of the impact of the Safe Harbor case on companies involved in data transfers from the EU.

Data Security and Protecting Personal Data

Data security and associated breaches are commonly in the news and students may be familiar with recent breaches at Target, Home Depot, among others. The ECJ decision in *Schrems* certainly contributes to a global view of data security. Adding relevant global supplemental materials in an IS security class can be particularly meaningful security attacks and breaches occur in both in many countries (White et al., 2014) and across borders and often occur with coordination of those in various countries. Any efforts by one or more countries to stem security breaches and cyberattacks impact many other countries (Kim, Wang & Ullrich, 2012). With respect to the information systems curriculum, the 2010 guidelines (Topi et al.) marked the first time a security class was included as a sample elective class in addition to the topic of *security* being included in six of the seven core classes in the guidelines. Classroom discussion involving Safe Harbor and Privacy Shield serves to illustrate the relevance of global awareness of how various governments are addressing data security issues.

Data Security and IT Jobs

It is important to begin conversations with college students regarding career paths early in order to help students match skills and jobs (Green, 2012). The story of Safe Harbor and the Privacy Shield provides a chance to link knowledge with IT jobs. Anyone working in an IT department for a company that engages in the transfer of data from the EU will be required to know and keep abreast of the U.S. EU data privacy agreements. A quick search at Indeed.com, a job search aggregator, showed a variety of IT job titles whose responsibilities include knowledge of Safe Harbor (see Table 1).

Table 1. IT Job Titles Requiring Safe Harbor Knowledge (www.indeed.com)

Cyber Security Data Architect	Pre-Sales Cloud Architect
Data Management and Protection Services Manager	Security Analyst-Vendor Risk Management
Director of Cyber Security	Senior Consultant Data Loss Prevention
Director-Privacy	Senior IT Auditor
Identity Management Engineer	Senior Privacy Analyst
Infrastructure Manager	Senior Specialist II
IT Compliance	Solutions Architect

IT Security Engineer	Sr. IT Infrastructure Manager
Manager	IT Audit Data Analysts

A Snapshot of Companies with Safe Harbor Certification

As companies anticipate transitioning to the new Privacy Shield, they will complete a process similar to Safe Harbor certification. A variety of companies with Safe Harbor certification from Airbnb to Go Daddy to Yelp, are expected to retain certification under Privacy Shield. A recent snapshot of some of those companies with Safe Harbor certification are illustrated in the following charts which can be used as classroom tools to facilitate discussions including: general discussions on Safe Harbor; predictions of what a pie chart may look like based on a scan of raw data; discussions of the importance of IT professionals working with multinational companies; as well as discussions of European geography, to say the least.

While the EU has not issued final approval of the Privacy Shield and U.S. legislative implementation is pending, the Privacy Shield is expected to serve as an enhanced version of Safe Harbor, including the certification process. As of March 31, 2016, there were 5557 companies in 105 different industry sectors that had gone through the self-certification process under Safe Harbor (U.S-EU Safe Harbor List, n.d.). For the purpose of this study, all firms in a subset of the industry sectors, Computer Services and Information Services, were included for further analysis. The two above industry sectors accounted for 2532 unique companies that were tagged with one or both of the two industry sectors (see Figure 1).

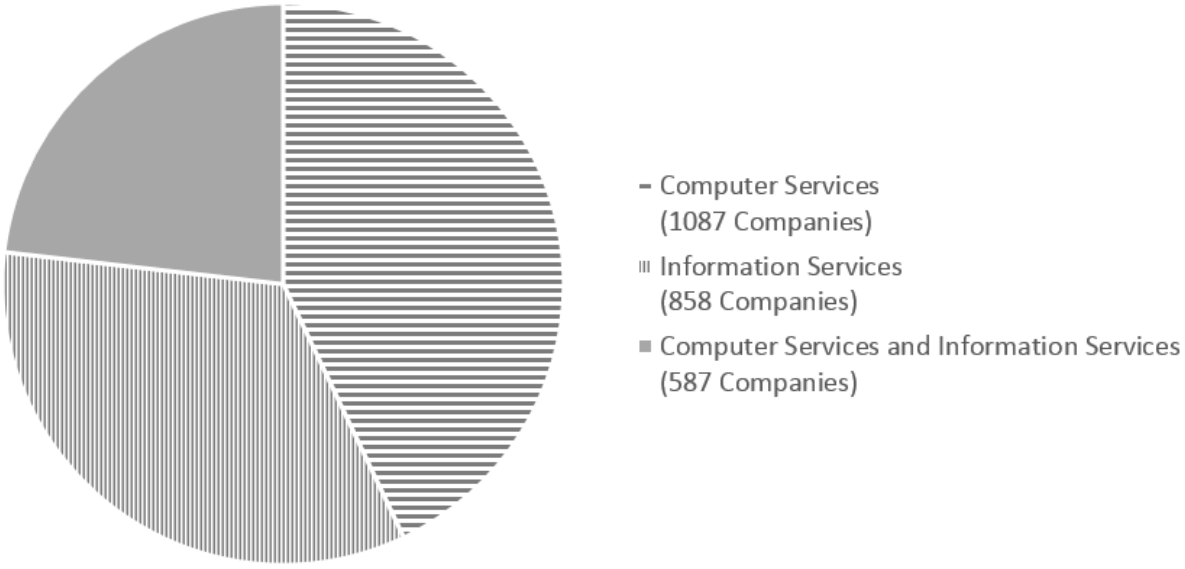

Figure 1. Industry Sector Categorization of Computer-Related Companies On the Safe Harbor Certification List

Of the 2532 unique companies above, a little over a fourth, or 688 companies (27.17%) do not have current Safe Harbor certification while 1844 companies (72.8%) are current in their Safe Harbor certification. A t-test was conducted to determine whether companies with current certification differed from companies without current certification in terms of the number of European countries with whom they trade. A t-test showed that companies with current Safe Harbor certification trade with more European countries (M = 26.59, SD = 11.72) compared to companies without current certification (M = 23.23, SD = 11.72, $t(1083) = 6.67$, $p < .0001$).

Furthermore, companies with current certification tend to engage in trade that includes data transfers with the more western European countries more often than they do with the more eastern European countries (see Figure 2 on the

following page). This could be a starting point for an internet search and discussion about the political, commercial and cultural differences between eastern and western Europe.

.

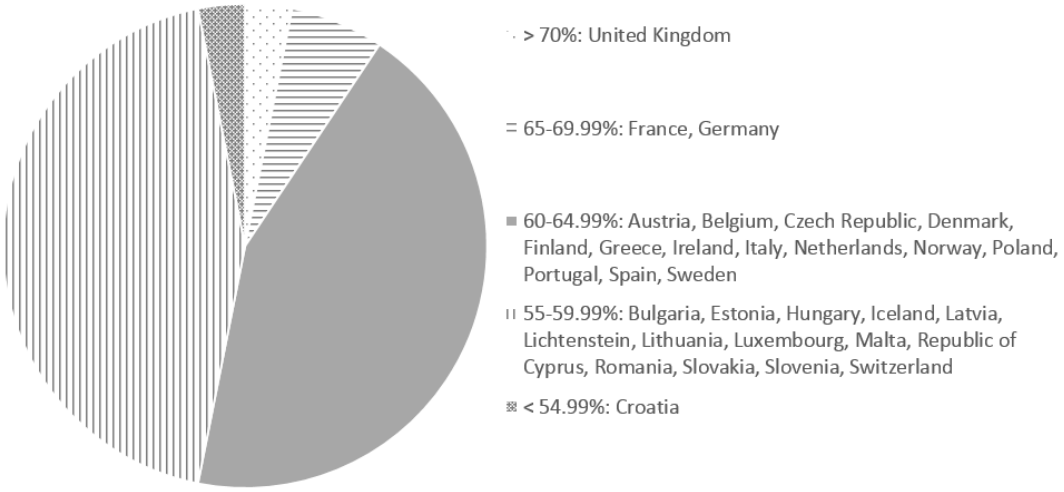

Figure 2. European Countries With Whom U.S. Safe Harbor Certified Countries Transfer Data

.

CONCLUSION

Since the Privacy Shield Agreement was announced February 2016, there has not been an opportunity to conduct this exercise in class. However, global exercises are common in CIS classes and prior experience with class exercises involving career exploration overall students engaged and excited about looking at their futures as IT professionals.

The direct impact of the fall of U.S. EU Safe Harbor through the decision in the *Schrems* case and the rise of the Privacy Shield agreement is an effective illustration with which to introduce the impact of global activities on U.S. businesses. Incorporating current global events into the information systems curriculum in conjunction with identifying IT jobs provides students a real-world look at IT global issues and the professionals who must deal with them.

REFERENCES

AACSB International (2011), Globalization of management education: Changing international structures, adaptive strategies, and the impact on institutions, Emerald Group Publishing Limited.

Casper, C. (2015). Has Safe Harbor's Ship Sailed? Gartner, Inc. Available: https://www.gartner.com/doc/3151821/safe-harbors-ship-sailed

Data Disposal Laws (2016). National Conference of State Legislatures. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

Data Protection in the European Union (n.d.) Available: http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf

Davis, G. B., Gorgone, J. T., Couger, J. D., Feinstein, D. L., & Longenecker, Jr, H. E. (1997, December). IS'97: model curriculum and guidelines for undergraduate degree programs in information systems. In *ACM SIGMIS Database* (Vol. 28, No. 1, pp. 1-94). ACM.

European Agency for Fundamental Rights (2014). Handbook on European Data Protection Law. Available: https://iapp.org/resources/article/handbook-on-european-data-protection-law/

EU US Privacy Shield Fact Sheet (2016 February). Available: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2014).

Federal Trade Commission Act, 15 U.S.C. §§41-58 (2014).

Financial Services Modernization Act, 15 U.S.C. §§ 6801-6827 (2014).

Green, A. (2012). 8 Ways College Could Better Prepare Students for the Job Search. US News and World Report. Available: http://money.usnews.com/money/blogs/outside-voices-careers/2012/08/15/8-ways-college-could-better-prepare-students-for-the-job-search

Gorgone, J., Davis, G. B., Valacich, J. S., Topi, H., Feinstein, D. L., & Longenecker, H. E. (2003). IS 2002 model curriculum and guidelines for undergraduate degree programs in information systems. *Communications of the Association for Information Systems, 11*(1), 1.

Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d – 1320d-9 (2014).

Hedderich, N. (2011). The challenge of transcultural competence: Background reading of target culture current event articles. *Global Business Languages*, *16* (1), 9.

ITI Fact Sheet (2016, February 4). The EU US Privacy Shield. Available: http://www.itic.org/dotAsset/2/c/2c5b5a4a-05ef-40b0-8703-9a67f6235ff8.pdf

ITI Fact Sheet (2016, February 16). The EU US Privacy Shield What's at Stake. Available: http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf

Jolly, Ieuan (2015) Data Protection in United States: Overview, Thomson Reuters Practical Law. Available: http://us.practicallaw.com/6-502-0467

Kedia, B. L., & Englis, P. D. (2011). Internationalizing business education for globally competent managers. *Journal of Teaching in International Business, 22*(1), 13-28.

Kim, S. H., Wang, Q. H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66-73.

Lee, M. (2016). Out with the Safe Harbor and In with the Privacy Shield. US News and World Report. Available: https://www.mapi.net/blog/2016/03/out-safe-harbor-and-privacy-shield

McCarthy, K. (2016). Tweak Privacy Shield rules to make people happy? Nah – US govt. The Register. Available: http://www.theregister.co.uk/2016/04/20/changes_to_privacy_shield_not/

Muddiman, A., & Bainbridge Frymier, A. (2009). What is relevant? Student perceptions of relevance strategies in college classrooms. *Communication Studies, 60*(2), 130-146.

Pritzker, P. (2016, February 29). Statement from U.S. Secretary of Commerce Penny Pritzker on Release of EU-U.S. Privacy Shield Text. Available: https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-release-eu-us-privacy

Schrems v. Data Protection Commissioner, Case C-362/14 (2015). E.C.L.I. _____ (delivered October 6, 2015).

Security Breach Notification Laws (2016). National Conference of State Legislatures. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Sikes, V.M. (2010). Current events, the economic downturn and critical pedagogy. *Curriculum and Teaching Dialogue, 12*(1/2), 41.

State Laws Related to Internet Privacy (2016). National Conference of State Legislatures. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment (2016). Available: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

Tedford, P. (2003). Using current events as a teaching tool for an undergraduate data structures course. *Journal of Computing Sciences in Colleges, 18*(4), 50-55.

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, Jr., J. F., Sipior, J. C., & de Vreede, G. J. (2010). IS 2010: Curriculum guidelines for Undergraduate Degree Programs in Information Systems. *Communications of the Association for Information Systems, 26,* 359-428.

United Kingdom Information Commission Office (2016). The Guide to Data Protection. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/

U.S. Department of Commerce Issues Fact Sheet on the EU-U.S. Privacy Shield Agreement (2016, February 2). Available: https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield

U.S.-EU Safe Harbor List (n.d.). Available: https://safeharbor.export.gov/list.aspx

U.S.-EU Safe Harbor Overview (2013). Available: https://build.export.gov/main/safeharbor/eu/eg_main_018476

U. S. Department of Commerce (2016, February 2). Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework. Available: https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework

White, B. J., Hale, M. C., & Willey, L. (2014). Globalizing security classes using Google Trends. *Issues in Information Systems, 15*(2), 39-48.

APPENDIX
CLASS ACTIVITY: STUDENT EXPLORATION OF GLOBAL ISSUES AND IT PROFESSIONS

This activity could span one or two class sessions or could be expanded to include a more major research activity.

In the classroom

The activity begins with a classroom discussion on data privacy and security. Suggested questions include: How does the U.S. protect private personal data? If a company wants to expand to another country, what laws must it follow? Does anyone know anything about data privacy laws in the EU? Have you heard anything in the news about issues between the U.S. and EU involving data privacy?

These questions can lead to a short lecture/discussion on the subject of this paper without reference to the Privacy Shield agreement. The class lecture/discussion would focus on: the different approaches to data privacy rights in the U.S. and the EU; the need compliance with EU standards if doing business in that region; the rise of Safe Harbor and its basic requirements; the *Schrems* case. **No** mention is made of the Privacy Shield agreement; that is to become the basis of the student's first task.

The following questions can be asked to set the stage for the first activity: What will happen to U.S. companies doing business in the EU now? What impact does this have on those working in an IT department with those U.S. companies? What impact could this have on trade between the U.S. and EU? Tell the students that there is a new agreement that was recently announced. **Again, no** mention is made of the Privacy Shield agreement.

Activity: Search for Privacy Shield Factsheets

Advise the students that they work in an IT department for a multinational company that trades with the EU and for which the company has relied on Safe Harbor in relation to its EU data transfers. The employee's supervisor has asked the employee (student) to provide some basic information about the Privacy Shield that replaces Safe Harbor. The supervisor tells the employee that some sort of short fact sheet on the agreement is needed. The employee starts investigating the issue on the Internet and attempts to find a fact sheet. (You may suggest search terms such as U.S. EU Safe Harbor or EU U.S. Privacy Shield.)

Activity: Search for IT Jobs Requiring Safe Harbor/Privacy Shield Knowledge

Once the employee (student) starts reading about the new Privacy Shield and the conflict in EU and U.S. requirements, the employee begins to consider looking for a job where knowledge of those issues and the agreement would be useful to move up the IT ladder. Now the employer returns to the Internet to start a job search using job aggregators (like indeed.com) or specific IT job search sites like dice.com. Students should provide a list of five jobs for which this specific knowledge is listed as a job requirement, skill or preference including the job titles and short descriptions of how the EU U.S. data agreements relate to the jobs listed. Students can work in groups to aggregate data collected and create related charts.

More Class Discussion

Suggested questions: Why will it be important to stay alert to global news for IT? How could not staying current negatively affect a company or the job security of IT professionals working for affected companies?

Questions specifically as to the search for the Privacy Shield fact sheet: What is the name of the new agreement? Where did you find information? Did you find a fact sheet? What are some of the facts about the Privacy Shield?

Questions specifically about jobs requiring this knowledge: What jobs are available for those who know about the EU U.S. Privacy Shield? Would you be interested in a job like that and why?

Instructor Resources Related to the Exploration Activity

Factsheets on which this exercise is based are available online (EU US Privacy Shield Fact Sheet, 2016; ITI Fact Sheet, 2016, February 4; ITI Fact Sheet, 2016, February 16; U.S. Department of Commerce Issues Fact Sheet, 2016).