

Cybersecurity Collaboration Needed Between U.S., EU

Upcoming European Union privacy reform highlights the need for consistent, global legislation to help businesses protect customer and supplier information.

Technology is an important driving force for global economic development. However, in the wake of high-profile data breaches in the United States and revelations of classified U.S. surveillance programs by Edward Snowden, there will be many more global technology challenges over the next decade.

Businesses are just beginning to understand the macro-powers of regional blocs such as the European Union and NAFTA, to define not only trade, but also security, science and technology. There is currently a struggle to maintain privacy in a world increasingly dependent on digital interconnection. Although there are conflicting security threats and privacy protection issues in the U.S. and Europe, it's clear a global consistent approach is needed. Cyber war is one of the biggest threats of the 21st century, and as businesses continue to confront boundaryless crimes and terrorism, the need for collaboration on both sides of the Atlantic and a focus on long-range goals and principles is necessary.

There has been intense global interest in the European Commission's new data protection proposal and its effect on non-EU businesses and their global supply chains. In 2012, the commission proposed a major reform of the EU legal framework on the protection of personal

data. The new proposals will strengthen individual rights and tackle the challenges of globalization and new technologies. The new EU legislation is expected to address current vulnerabilities of companies' business IT systems, including payment, ERP and customer relationship management systems, as well as some of the other challenges currently facing our information society.

It's anticipated the reform legislation will provide a basic framework for data privacy legislation to other regions and countries around the globe. Supply management practitioners will see a major shift in business leadership attitudes regarding the protection of all personal data. That's because the binding nature and extraterritorial reach of the upcoming EU reform will affect any business that provides goods or services to EU citizens, as well as those that monitor the activities of EU citizens.

The reform legislation is good news for EU consumers because it holds all third parties accountable for data breaches and will streamline the current data protection requirements and procedures for all 28 EU countries. The privacy framework is expected to provide a uniform set of guidelines for all the European countries, assuring



businesses and EU consumers consistent legislation and adequate protection.

Multinational companies, such as Hewlett-Packard, that supply data services to large enterprises welcome this unified regulatory framework because it offers consistent regulation for all its European data centers. Many multinational companies already employ a dedicated data privacy officer who handles the compliance requirements with the various data protection authorities. They are also in close collaboration and discussion with the EU regulatory committees in Brussels regarding the proposed regulation.

Not surprisingly, the request by the U.S. government for personal data processed by Microsoft outside the U.S. is creating serious concerns for the cloud computing industry. The July 2014 U.S. court ruling upholding a warrant and requiring Microsoft to deliver data from a Dublin, Ireland, data center to prosecutors in a law enforcement investigation case bypasses the existing formal procedures that are agreed upon by both nations. The Mutual Legal Assistance agreement was designed to manage foreign government requests for access to information and ensure certain safeguards in terms of data protection.

Additionally, in the recent Google Spain case ruling, the Court of Justice of the European Union ruled that, as regards the issue of territoriality of the EU rules, these rules apply "even if" the physical server of a company's processing data is located outside Europe. The Court of Justice clearly stated that EU rules apply to search engine operators, if they have a branch or a subsidiary in an EU member state.

The need for collaboration

between the United States and the EU has never been greater for multinational companies and technology businesses. Consumer cloud service providers are concerned about the ramifications of conflict of laws where inconsistent or conflicting data privacy legislation could hinder their ability to do business and store data in centers in Europe or other locations. In a world where cloud computing is rapidly expanding, a modern, multinational, cross-boundary approach to privacy and data protection would help global businesses. Companies want to expand globally without the added burden of penalties for non-compliance due to conflicting country laws.

Over the next few years, the EU will be preparing for Horizon 2020, one of the biggest publicly funded worldwide research and innovation programs to date with a budget of nearly 80 billion euros. Horizon 2020 will not only raise the level of excellence in Europe's science and technology base, but also ensure a steady stream of world-class research along with major investment in key industrial technologies. It's an attractive program for multinationals searching for cybersecurity information, consistent data protection laws and those who believe privacy is (or should be) a basic human right. **ISM**

Adriana Sanford, J.D., Dual LL.M., is an ASU Lincoln Professor of Global Corporate Compliance and Ethics, a clinical associate professor in the W. P. Carey School of Business, and a College of Liberal Arts & Sciences residential college faculty fellow at Arizona State University in Tempe, Arizona. Her current academic research focuses on comparative law regarding cybersecurity, privacy and data protection.

Wilfried Grommen, located in Brussels,

is chief technologist of public sector and European institutions for Hewlett-Packard. For more information, send an email to author@ism.ws.



Around the World Wales

Capital, government, currency and religion: Cardiff; the British pound sterling; Wales is a constitutional monarchy as part of the United Kingdom.

Mind your manners: Politeness in communication is highly valued. Expect to hear a lot of "please," "thank you" and "sorry." The Welsh tend to be indirect communicators.

Down to business: Being on time for meetings, and following schedules and deadlines, matter in Wales. Decisions tend to be made from the top down. Humor is often used in negotiations, sometimes as a defense mechanism or in the form of self-deprecation and/or irony. Avoid hard-selling and any sort of conflict or confrontation.

What to wear: For men, conservative, dark or medium-colored suits with shirts and conservative ties; for women, stylish yet classic business suits or dresses and blouses. Jeans or business-casual attire may be appropriate depending on the industry.

Source: www.culturecrossing.net/basics_business_student.php?id=240