Potential US-EU Trade Pact May Enhance US Companies' Ability to Monetize Digital Trade in the EU

In January 2013, President Obama announced in his State of the Union Address that the United States will begin negotiating a US-EU Transatlantic Trade and Investment Partnership later this summer. One of the key issues that the United States will seek to address as a part of this negotiation is the significant inconsistency between EU and US data privacy laws and how these differences adversely impact digital trade between the EU and US.

US and EU privacy and data security laws dramatically differ. EU privacy and data security laws are much more favorable to consumers, while US privacy and data security laws, in comparison, favor companies.

EU Privacy Laws

In Europe, privacy is generally considered to be a human right, and this principle is reflected in EU law. In the EU, there is one comprehensive privacy law, the European Privacy Directive, and each member country has its own national law and agency that interprets the European Privacy Directive. There are significant variations in interpretation of the European Privacy Directive between countries; however, core principles reflecting this human rights approach can be seen across all EU member countries. For example: (1) companies cannot collect personal information without consumers' permission; (2) consumers have the right to review data collected about them and correct inaccuracies; (3) employers cannot read workers' private email; and (4) personal information cannot be shared by companies across borders without express prior consent from the individual.

US Privacy Laws

In contrast, in the United States, there is no single comprehensive privacy law, and privacy is not widely considered to be a human right. The word "privacy" does not appear in the U.S. Constitution, but certain sections of the Bill of Rights have been interpreted to protect privacy. For example, the Fourth Amendment bans unreasonable search and seizure, and Fourth Amendment case law generally protects U.S. residents' privacy in their homes. However, once a person leaves his home (physically or virtually), the right to privacy is not as strong.

Many federal and state privacy and data security statutes have been enacted in response to instances of data theft or misappropriation. There are a few federal laws that strongly protect consumer privacy in certain limited areas such as personal health information, personal information about children, personal financial information, education records, credit reports and video rental records. There are also state privacy laws that require: (1) owners and operators of websites and apps to post privacy notices that contain certain information relating to their corporate policies for collecting, using and disclosing users' personal information; and (2) companies that own certain personal information to notify individuals in the event of a security breach involving that personal information.

In contrast to the EU, under US law: (1) companies may generally collect consumers' personal information without their consent; (2) companies generally are not legally required to permit consumers to review data collected about them and correct inaccuracies; (3) employers may read workers' private email; and (4) companies may share personal information across borders without express prior consent from the individual.

How Differences in US and EU Privacy and Data Security Laws Impact Trade

US companies doing business in EU countries must comply with numerous requirements that do not exist under US law. For example, US companies doing business in the EU must obtain individuals' prior express consent before sharing their personal information across country boarders. This requirement is implemented differently in various EU member countries. For example under German law, signed (inked) written consent is required. In other EU member countries, electronic check boxes are deemed to be an acceptable form of prior express consent. The inconsistent implementation makes compliance by US companies even more expensive and time consuming.

If the cost of complying with these laws is too high, a US company must often decide between: (1) walking away from a deal or market; (2) altering its product or service offering so that compliance with EU privacy or data security laws is not required; or (3) breaching EU laws. In my practice, I rarely see companies choose option 3 – breaching the law. US companies understand and are sensitive to the fact that for EU consumers, this is an issue of human dignity rather than a purely economic matter. Customer trust is of paramount importance to a business' success. Adopting a 'breach the law' approach destroys customer trust which in turn leads to diminished financial returns. And, if a company chooses option 1 (walking away) or option 2 (altering its business practices), trade (and profits) are almost always adversely impacted.

If the Transatlantic Trade and Investment Partnership is able to strike the right balance between cultural beliefs and economic profit, both consumers and companies in the EU and US will benefit. We will continue to track developments on the Transatlantic Trade and Investment Partnership and periodically update you.

http://blog.helenchristakos.com/