Outsourcing raises a number of cross-border legal issues that are increasingly receiving attention from both consumer groups and governments. One of the hottest issues concerns the relationship between outsourcing and international privacy laws and the increasing burdens placed on outsourcing customers and suppliers to protect information.

In the United States, legal questions about privacy used to be solely the domain of constitutional law. However, those days are long gone, as privacy issues now lie at the forefront of the business community’s concerns. Companies that rely on the use of personal information, whether about employees or customers, including potential customers, have to be concerned about privacy issues, not only because of legal obligations, but also because of the public relations repercussions following the illegal disclosure of private information.

For U.S. companies, the obligations flowing from privacy regulations began slowly, but have increased rapidly. In the health care industry, for example, the federal Health Insurance Portability and Accountability Act of 1996 created a continuing obligation to develop and maintain privacy and security compliance plans. More recently, federal and state laws have been enacted that impact specific sectors of the economy: the Gramm-Leach-Bailey Act of 1996 (financial); the Children’s Online Privacy Act (children’s information); the Fair and Accurate Credit Transaction Act (financial); and, as an example of ever-increasing state consumer protection laws, California’s SB 1386 (requiring an agency, person, or business doing business in California who owns or licenses computerized “personal information” to disclose any breach of security). And those are just the domestic laws.

This article first appeared in the Issue 9 of Business & Technology Sourcing Newsletter.
For multinational companies, foreign privacy laws add even more challenges to their domestic law obligations. The fact that outside of the United States and Europe there is little consistency with regard to privacy laws and enforcement only compounds the problem. Moreover, the list of countries at the receiving end of outsourced work is growing. In addition to India and China, countries such as Ghana, Guatemala, Ireland, Jamaica, Mexico, Pakistan, and the Philippines are receiving increasingly more outsourced work.

With respect to financial information, among the tasks that are now routinely outsourced in whole or in part, are credit-reporting, income tax preparation, and loan processing services. With respect to tasks that involve medical and health information, record transcription, billing, and data entry are routinely outsourced. All of these outsourced tasks share the common trait of involving sensitive information and the privacy interests of consumers.

Outsourcing creates its own special set of privacy concerns. Most outsourcing is driven by the desire to cut cost, prompting companies to send a business process overseas to developing countries, where labor costs are lower. But the desire to lower labor costs is not the sole reason that a process gets outsourced. The ease with which electronic information can be transferred is often the linchpin of outsourcing for many tasks that might otherwise be performed domestically. The medical industry, for example, has been outsourcing transcription services overseas for some time. However, outsourcing, a process that involves sensitive information — which may include personal and financial information — is fraught with dangers that may expose a company to liability for conduct it has little control over.

This danger was particularly demonstrated in 2003, when a medical transcriber in Pakistan threatened to post patients’ private records online unless the University of California San Francisco Medical Center (UCSM) paid wages owed to her by the U.S.-based company that had sent the work to Pakistan. UCSM had outsourced the processing of the medical transcripts to a U.S.-based company that had, in turn, outsourced records to yet another domestic company. The second outsourcing company then sent the work to Pakistan for processing. It was the Pakistani company’s employee who threatened UCSM. In a similar case, an Ohio-based company, Heartland Information Services, received emails from its own employees in India (this type of arrangement is commonly called “offshoring” because while the task is being performed elsewhere, the same company is in charge of the process) attempting to extort cash from the company by threatening to publicly disclose confidential information.

The UCSM case illustrates the need for developing appropriate vendor monitoring policies. Several steps are essential. First is identifying all vendors that receive sensitive information. Second is developing contractual protections that hold the vendors liable for secondary outsourcing. And third is continuous monitoring and updating of these procedures. The Heartland case, while not involving outsourcing to a vendor, similarly stresses the need for oversight of outsourced processes.

In an effort to gain the trust of business communities worldwide, the recipients of outsourcing work are improving internal safeguards in order to better avoid security breaches. Recently, the National Association of Software and Services Companies (NASSCOM), the organization representing India’s information and technology services industry,
announced its intention to create a “self regulatory organization” to oversee best practices in India’s $20 billion “back office” services sector. The United States is the largest source of those revenues, and the proposed measures are aimed at addressing concerns in the United States about the risks associated with breaches of security. Of course, regulation has its limits in countries where outsourced work is performed by many small companies that can easily escape the nascent regulatory process, assuming one is implemented. Enforcement, including prosecution of individual employees who engage in illegal conduct, is also unlikely to be on par with what many businesses from the developed countries are familiar with. One proposed solution by NASSCOM is to launch a registry to help employers track the employment history and education qualifications, among other information, of workers.

European consumers are afforded far greater protection than their U.S. counterparts by virtue of the European Union law that permits personal data to be sent offshore only to countries whose privacy laws meet the EU’s stringent standards, both in the protections they afford and in enforcement. Few countries meet these standards. Interestingly, the United States is one of the non-compliant countries. However, information continues to flow from the EU to the U.S. under a “Safe Harbor” program, which permits transfer of information from the EU to those U.S. companies that certify to the Federal Trade Commission that they will abide by specific standards. The EU privacy law requires, for example, the use of fair information practices found in the “Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” A number of countries have enacted privacy laws modeled after the EU’s, including Argentina, Paraguay and Switzerland.

To effectively safeguard against privacy breaches, companies must be vigilant in both monitoring current privacy policies and continuously reshaping those policies to address new regulations and circumstances. Privacy law will continue to grow exponentially in complexity and breadth. Devising a privacy law compliance program will hinge on the number of countries in which a company conducts business. A global approach may work for some companies, while others may need to fashion country- or geographic-specific programs. While relying on outside counsel to assist in navigating the ever-changing landscape of privacy law remains a vital part of the process, training in-house privacy officers has become increasingly important. An effective privacy officer will have detailed knowledge about the company and how privacy laws impact its operations. This need to monitor is especially relevant as the federal and state governments consider placing restrictions on the outsourcing of work. Whatever the merits of these proposed legislations, if enacted they will have a direct impact on existing and future plans to outsource.