

Privacy and Security Law Issues in Off-shore Outsourcing Transactions

Margaret P. Eisenhauer¹
Hunton & Williams - Atlanta Georgia

15 February 2005

Outsourcing arrangements often involve the processing of large volumes of personal information about a company's customers or employees. In many cases, this information includes sensitive information, such as financial data, medical data, payroll and benefits information, social security numbers and purchasing histories. This paper outlines the general issues that companies must consider when they permit outsourcing partners to transfer personal data across national boundaries. In particular, it examines issues that may arise under U.S. law, and also considers the regimes in three popular outsourcing destinations, the Philippines, India and Canada.

Introduction to Global Privacy Laws

As most corporate executives know, different countries have taken different approaches to privacy. The European Union, for example, has long-standing laws that strictly limit the processing and transfer of all personal information.² The United States has taken a more focused approach, limiting companies' ability to process data when that processing creates the possibility of real harm to individuals. When considering any type of data processing -- internal or by a vendor -- the company must consider what regulations apply to the processing in the jurisdiction where the data was collected. When data is transferred³ to another jurisdiction for processing, such as in an off-shore outsourcing relationship, the company must also consider how the laws (or lack of laws) in the target jurisdiction may affect the processing and its rights with respect to the information. With regard to any trans-border data flow, each company must consider two separate legal perspectives. First, it must consider whether any laws in the country where the data originates will continue to regulate the data post-

¹ **Peggy Eisenhauer**, counsel in the Firm's Atlanta office, leads the Hunton & Williams' privacy and information management practice group. She helps companies develop and document privacy and fair information practices, including policies governing the use and distribution of public and non-public data and the use of customer and employee information. She has extensive experience with US and international privacy laws, including the privacy and security regulations under Gramm-Leach-Bliley and HIPAA, the Fair Credit Reporting Act, and the USA PATRIOT Act. She is a frequent speaker on privacy and information management topics. *Ms. Eisenhauer is admitted to practice law in Georgia and Florida.*

² The EC Data Protection Directive recognizes the European view that privacy is a fundamental human right, and establishes a general comprehensive legal framework that is aimed at protecting individuals and promoting individual choice regarding the processing of personal data. The Directive imposes an onerous set of requirements on any person that collects or processes data pertaining to individuals in their personal or professional capacity. It is based on a set of data protection principles, which include the legitimate basis, purpose limitation, data quality, proportionality, and transparency principles, data security and confidentiality, data subjects' rights of access, rectification, deletion and objection, restrictions on onwards transfers, additional protection where special categories of data and direct marketing are involved, and a prohibition on automated individual decisions. The Directive also regulates transfers of personal data. Subject to some limited exceptions, personal data may not be transferred to non-EC jurisdictions that do not offer an "adequate level of protection" for the data. The U.S. has not been found to be adequate, nor have India or the Philippines

³ The term "transfer" encompasses both actual (physical) movement of data to a processor located in another country as well as the remote access by the foreign processor to data held in the home jurisdiction. From a data protection law standpoint, the legal analysis does not change if the data itself travels or if it is merely accessed from a location in other jurisdiction.

transfer. For example, U.S. financial institutions' information is regulated by the Gramm-Leach-Bliley Privacy and Safeguards Rules, and these will continue to apply, even if the data is transferred off-shore.

Second, it must consider whether laws in the country where the data is processed give rise to any additional risks or benefits. For example, if U.S. data is transferred to Europe, the European data protection laws may themselves impose additional obligations on the processing of the data. These additional obligations may constitute risks in that the company (as the owner of the data) may have liability if the requirements of the EU laws are not followed by its agents. The laws may also be beneficial in that the company may use the law to its advantage in the event of misconduct by its processor

This paper explores some of the issues that should be considered when U.S.-based companies evaluate outsourcing the processing of personal information, particularly to vendors located in India and the Philippines.

The United States

Laws that Impact Data Processing

The United States has never enacted a comprehensive data protection or privacy law in the EU-model. Instead, the U.S. has enacted laws to address particular privacy harms (such as collection of personal information from children) and to regulate certain applications of data (such as use of credit reporting data).

Additionally, even for highly-regulated data (such as healthcare information subject to the HIPAA regulations and financial information subject to the Gramm-Leach-Bliley (GLB) Act), the U.S. laws do not address the issue of trans-border data flows directly. These laws do impose obligations to maintain reasonable security, access controls and the like, which must be considered in any vendor relationship, domestic or off-shore. Accordingly, assuming the vendor provides appropriate security and confidentiality, U.S. laws do not now limit a company's ability to select vendors in any other geography.

The lack of a data privacy law dealing with outsourcing does not mean that a company's use of off-shore vendors is without risk. The U.S. laws do impose various obligations on companies to maintain the privacy and security of its U.S. databases, and these obligations necessitate that the company ensure the requirements of law are met. Additionally, to the extent the company has posted privacy statements (or otherwise made representations to consumers or employees) about privacy and security, the company will be expected to comply with these statements.

Several U.S. laws require companies to maintain reasonable technical, physical and administrative safeguards.⁴ Even where these laws do not exist, companies should have appropriate safeguards as a matter of course.⁵ In each case, the company should contractually impose similar requirements on any vendors or contractors that it may use for data processing. The obligation to comply with U.S. security requirements will exist regardless of whether the processor is located in the U.S. or in another jurisdiction.

⁴ See, e.g., Gramm-Leach-Bliley 15 U.S.C.A. §§ 6801 - 6909 (2003), Safeguards Rule, 16 C.F.R. Part 314 (2003) covering non-public personal financial data processed by financial institutions. Health Insurance Portability and Accountability Act (HIPAA) 45 C.F.R. Part 164 Subpart C (2003), Safeguards Rule, covering protected health information processed by healthcare providers, health plans and information clearinghouses. California's AB 1950 also requires companies that do business in California to safeguard certain types of personal information.

⁵ Some laws also require public disclosure of security breaches. Companies that do business in California, for example, must notify California residents if sensitive personal information about them is acquired (or reasonably may have been acquired) by an unauthorized person. This law applies to breaches involving sensitive customer data (such as credit card numbers) and employee data (such as social security numbers). See CA Civil Code §1798.92.

Similarly, to the extent that the company is bound by privacy, confidentiality or security requirements under any of its contracts, those requirements will continue to exist as obligations of the company even when third party vendors handle the processing on the company's behalf.

Finally, the company must ensure that its use of vendors (domestic or off-shore) does not create any situations where it fails to live up to representations made to consumers or employees in privacy notices or otherwise. Because the breach of privacy representations is itself an unfair and deceptive trade practice, the company would have significant liability in the event a representation turned out to be inaccurate. For example, if a company's website privacy statement states that "we take reasonable steps to secure the information we collect," the company must in fact take those steps -- for itself and its vendors. If the company were to provide web-sourced data to a third party without taking reasonable steps to ensure that the third party also had appropriate security, it would almost certainly be found to have committed a deceptive trade practice given this representation.⁶

Accordingly, it is vital that the company take reasonable steps to verify that its vendors (domestic and off-shore) can in fact meet the privacy and security standards that the company itself must meet.

Basic Security Standards

With regard to security, the GLB Act Safeguards Rule provides a good model for all companies to consider when developing an appropriate information security program. The Safeguards Rule defines an "information security program" as one that contains "administrative, technical and physical safeguards" to protect the security, confidentiality and integrity of personal information.⁷ Thus, the Safeguards Rule distinguishes the concepts of security, confidentiality and integrity, but suggests that all three concepts are integral to a complete understanding of security.

Pursuant to the Safeguards Rule, the administrative, technical and physical safeguards to be implemented must be reasonably designed to (i) insure the security and confidentiality of customer information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.⁸ The agencies that drafted the Rule appear to believe that security means protecting the confidentiality and integrity of information, and restricting access to it.

The Safeguards Rule does allow for flexibility in implementing a security program, stating that the program must contain safeguards that are "appropriate" to the entity's size and complexity, the nature and scope of the entity's activities, and the sensitivity of any customer information at issue.⁹ This permits each company to determine the appropriate level of effort required, given the personal information being protected. For data processors, the level of due diligence as well as the contractual protections imposed should also be proportional to the amount of access that the processor will have to the company's information.

⁶ State and Federal laws regulate such statements as unfair and deceptive trade practices. (See, e.g., Section 5 of the FTC Act.) Liability for making false statements can be very steep, and both the Federal Trade Commission and the state attorneys general enforce these statutes vigorously.

⁷ 16 C.F.R. § 314.1(a).

⁸ Id.

⁹ 16 C.F.R. § 314.3(a)

The Safeguards Rule requires that certain basic elements be included in a security program. Each institution must (1) designate an employee to coordinate the safeguards, (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling those risks, (3) design and implement a safeguards program and regularly monitor and test it, (4) select appropriate service providers and enter into agreements with them to implement safeguards, and (5) evaluate and adjust the program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring of safeguards.¹⁰ Confirming the ability of each of the company's vendors to meet these requirements is an essential part of the due diligence process for vendor selection, regardless of vendor location.

Political Threats to Outsourcing Arrangements

Despite the prevalence of U.S. laws that impose liability for misuse of (at least regulated) data, significant discussion of off-shore outsourcing is occurring in political and journalistic circles. In particular, various political leaders from both parties have raised questions about the ability of U.S. companies to protect privacy and security of personal information after it is sent to other countries. Questions have also been raised about the ability of U.S. regulatory agencies to ensure accountability of U.S. companies that engage in off-shore outsourcing transactions. For example, last year Representative Ed Markey sent letters to the federal financial institution regulators, the Federal Trade Commission, the Department of Health and Human Services, the Department of Homeland Security, the Internal Revenue Service and other agencies requesting information on how entities regulated by the agencies were managing outsourcing and whether the agencies could have effective oversight in such situations. The Markey letters illustrate the concerns being raised.

Through the Center for Information Policy Leadership at Hunton & Williams,¹¹ we have discussed accountability issues with many of the U.S. regulators as well as some of the international data protection authorities. The consensus view is that the U.S. regulators generally have sufficient authority to hold U.S. entities accountable for any breach of U.S. law (*e.g.*, the GLB Act) that may occur, regardless of whether the violation occurs as a result of the company's own actions or those of a vendor, and regardless of the location of the breach. Companies may outsource data processing to third parties but they cannot transfer their obligations to ensure that data processing is done in a manner compliant with applicable laws. For the company, this means that it can engage data processors anywhere it chooses, but the company itself will remain accountable in the U.S. to the Federal Trade Commission and state Attorneys General for any violations of applicable laws, terms of its consent decree, or published privacy/security representations.

To address any concerns that regulators or consumer advocates may raise about a company's outsourcing arrangements, the company will want to demonstrate both a willingness to remain accountable for managing the privacy and security of its data as well as a capability to do so. Part of the company's vendor qualification process should consider the extent to which the vendor can fulfill the company's obligations under applicable laws, consent decrees, corporate standards and policies, and the like. As discussed below, the vendor qualification process should also consider what ability the company would have to enforce its contractual rights under local law (if needed) as well as whether local law itself provides any additional rights or risks that may be important.

We also know that the Federal Trade Commission (FTC) is very focused on privacy and security risks related to off-shore outsourcing. Because the FTC regulates many companies and because it has long taken the lead among

¹⁰ 16 C.F.R. § 314.4.

¹¹ The Center for Information Policy Leadership provides strategic consulting, legal, and policy development services for information industry and information-dependent companies. The Center brings together business leaders, government officials, consumer advocates, and academic experts to provide thought leadership on a variety of information policy topics, including global privacy law development, privacy notices, public-private data sharing, and use of personal information for authentication.

federal agencies on privacy issues, its views are of particular interest. According to senior FTC staff, privacy and security risks related to off-shore outsourcing are of concern to the FTC because vendor accountability is likely more difficult for companies themselves to manage. We understand that the FTC's Financial Practices Division is planning to issue business guidance on application of the GLB Act Safeguards rule to off-shore data transfers. We do not yet know what this guidance will require companies to do, but suggest that this process be monitored closely.

It is important to note that privacy is not the only driver of the anti-outsourcing sentiment, however. If the political pressure to improve the economy by limiting companies' ability to outsource becomes great, privacy may be seen as a useful reason to impose such limits. This may happen even if the real underlying reason for the limits is to try to stem the loss of U.S. jobs.

I note that Representative Markey's letter states that the risks result from "the fact that information technology jobs, back office data processing and data analysis jobs... that used to be performed by Americans, are being outsourced to off-shore locations by companies to take advantage of the dramatically lower wages available in Third World countries." This statement highlights the underlying U.S. economic issues, which have very little to do with privacy or accountability.¹² Given the political situation, the company might want to develop messages about how its activities benefit consumers and/or the economy in a broader sense. Additionally, having an ability to terminate an outsourcing arrangement in the event restrictions are imposed should be a necessary part of each the company contract.

It is also important to consider state law issues in this regard as well. Several states have considered laws that would impact use of off-shore vendors and otherwise regulate outsourcing as a privacy issue. For example, last year, the California legislature enacted a number of laws that would have limited off-shore processing of personal data. These enactments were ultimately vetoed by Governor Schwarzenegger¹³, but we expect them to resurface later this year. According to a February 23, 2004 news report in the *BNA Privacy Law Watch*:

The measures are meant to protect jobs as well as the privacy of California residents whose personal information is shipped overseas for a variety of services such as tax return preparation, home loan financing, credit card servicing, and some state government services.

One of the bills, A.B. 1829 by Assemblywoman Carol Liu (D), already has been introduced and focuses on the public sector. It would ban state agencies from contracting for services with contractors or subcontractors unless the work will be performed solely by workers in the United States. Liu said she introduced the bill after learning the state has contracted with a company that sends food stamp and welfare recipient calls to a call center in India.

"It is ironic that we are sending welfare and food stamps-related call center jobs overseas, while the people who are being served by these 'offshored' jobs are unable to find work at home and thus get off public assistance," she said.

¹² Representative Markey was also quoted in a Boston Herald article on the privacy and security risks of off-shore outsourcing. The quote reveals the dual concerns about jobs as well as privacy: "They started off sending American jobs overseas," said U.S. Rep. Edward Markey (D-Malden), co-chair of the congressional Privacy Task Force. "Now Americans get to lose their jobs and their privacy at the same time." *Boston Herald*, November 30, 2003, Article: "Known Around The World: Private Records May Be At Risk" This article also noted that "[t]wo of the three major credit-reporting agencies in the United States are also planning to outsource operations abroad and, along with them, sensitive data about the credit histories of hundreds of millions of Americans."

¹³ On September 20, 2004, Governor Schwarzenegger vetoed SB 1451, SB 1492, and SB 888, all of which would have placed serious restrictions on outsourcing and off-shoring.

The California trend has already been echoed in other state legislatures. During this past legislative cycle, at least 32 states considered over 127 bills to restrict outsourcing. The vast majority of these bills addressed processing of state data (such as requiring government contractors to only perform tasks using domestic workers) and job security (such as prohibiting companies that relocate state jobs from doing business with the state). Approximately 30 of the bills addressed information security, including requirements that companies disclose the location of data processing facilities and call centers. Approximately 20 of the bills specifically attempted to regulate call center outsourcing, including disclosures and opt out requirements. Given the distractions of the election, the political climate was not conducive to passage -- other than for the California laws mentioned above -- but next year should be much more active.

Given this legislative focus, we expect to see a flurry of state bills this year ranging from outright bans on overseas outsourcing to laws requiring notice (and maybe choice) about off-shore transfers. Other bills may mandate security standards and/or seek to allow an individual whose privacy is violated to sue and recover damages. Companies engaged in (or considering) off-shore outsourcing should monitor these developments closely.

The Philippines

Privacy, the APEC Privacy Principles

The Philippines does not have any comprehensive data protection laws, so data flows into and out of the Philippines can occur without local restriction. The Philippine government has expressed an interest in enacting a more comprehensive data protection regime. A draft data protection law, based on the EU-approach, has been circulated. As an Asia-Pacific Economic Cooperation (APEC) economy, however, the Philippine government has also followed the development of the APEC Privacy Principles.

These APEC Privacy Principles were developed over the past two years by a working group of APEC nations to provide an alternative to the EU data protection model. The U.S. was heavily involved in this process, which also includes major economies in the Asia-Pacific region, Latin America (including Mexico) and Canada. The APEC model for privacy and data protection legislation was finalized last November, and implementation workshops are being held now.¹⁴ These Principles will likely form the basis for a Philippine law in the next few years, so this situation bears watching.

The APEC Principles are noteworthy for two reasons. First, the laws that stems from these Principles will likely present lower compliance burdens for companies because they will recognize the necessity of appropriate processing and transfer of personal information. For example, the laws will likely facilitate off-shore outsourcing by permitting these arrangements if appropriate (but not overly burdensome) protections are in place.

Second, the Center for Information Policy Leadership at Hunton & Williams developed the basic framework document that the US government has suggested for the APEC model. Professor Fred Cate¹⁵ was the primary drafter of this framework. This approach is more business-process friendly, as it takes into account the many benefits that multinational data flows have for the economies. APEC-approach-based laws will recognize that global data flows are facilitated if the laws focus on ensuring that local companies are accountable for data processing activities. They will also reflect an understanding that enforcement and restrictions should be tied to harmful uses of data, not the mere processing of data itself. These concepts, while revolutionary compared with the EU approach, are necessary to enable the types of 21st century data flows that would support the company's needs.

¹⁴ The first implementation workshop is being held next week (Feb 21 and 22) in Seoul, Korea.

¹⁵ Professor Fred H. Cate serves as Senior Policy Advisor to the Center for Information Policy Leadership and Distinguished Professor at the Indiana University School of Law—Bloomington.

Other Philippine Laws

In order to manage the risks associated with its own liability for vendor malfeasance, the company will want to ensure that it (and its vendors) can enforce their contracts and protect their computer systems and data in the foreign country. In general, the Philippine legal system provides legal and equitable remedies that are analogous to those found in the United States.

The Philippine legal system is quite well developed, and is based on respect for the rule of law and court decisions. There are excellent local law firms in the Philippines, and the legal industry is quite mature. In particular, the Philippine legal system recognizes rights of data owners and would likely provide a reasonable forum for achieving redress in the event of a security or privacy issue.

With regard to information security, it is important to note that the Philippines has made great progress the past few years in enacting legislation to enable both companies and law enforcement agencies to address security concerns and computer crimes, such as hacking. Prior to the infamous “I LOVE YOU” virus incident in 2000, the Philippines did not have laws that made computer hacking and similar behavior a crime. After this incident, the Philippine government enacted the Electronic Commerce Act of 2000. This Act provides civil and criminal penalties for unauthorized access to computer systems, and imposes legal obligations of confidentiality on persons who receive electronic data, keys, messages or other information.

The mere existence of this Act is important. As the company considers outsourcing processor locations, it should do some amount of due diligence on the recourse it would have in the event of a security or privacy breach. For example, while legal (monetary) recourse for a security breach might exist in the U.S., it would be important to consider whether the company could reasonably get an injunction (or other comparable order) in a local jurisdiction to compel return or destruction of misappropriated data. It appears that the Philippine legal system would offer these types of relief.

India

As with the Philippines, India has not yet enacted a comprehensive data protection law. Various EU-style data protection initiatives have been (and are being) considered. The bills drafted are generally based on the U.K. Data Protection Act, although India has also indicated that it would like to negotiate a Safe Harbor-type accord with the EU¹⁶. This accord would resemble the U.S. Safe Harbor framework. Recent press coverage of the growing U.S. political rhetoric against off-shore outsourcing due to privacy concerns as well as continued pressure from EU trading partners has motivated the Indian government’s efforts to address the lack of privacy protections.¹⁷

The Indian government has enacted a comprehensive set of electronic commerce regulations, the Information Technology Act 2000. This Act addresses computer crimes, including hacking, damage to computer source code, and breach of confidentiality provisions. The Act also created a Cyber Appellate Tribunal to handle cyber crime

¹⁶ The Safe Harbor framework is a political agreement between the U.S. and the European Union, pursuant to which U.S. companies can publicly certify (to the Department of Commerce) that they follow the privacy principles established by the Safe Harbor program. This certification then provides the EU with adequate assurances so that the company can transfer personal data from Europe to the U.S. without further administrative requirements.

¹⁷ Although India is not an APEC economy, it is possible that the Indian government may nonetheless be influenced by the APEC Privacy Principles. I understand that several U.S. companies that are active in India have already made the APEC materials available to their advocates and trade associations in India.

cases. We understand from the Privacy & Human Rights sourcebook¹⁸, that Indian courts in 2003 convicted the first individual charged with cyber-crime. According to the sourcebook:

In February 2003, India convicted its first cyber-criminal when a Delhi High Court sentenced Arif Azim on the charges of online cheating. In the said case, Arif Azim, while working for a call centre near Delhi stole the credit card information that belonged to an American citizen and used it to order a color television and a cordless hand phone. This case has highlighted the security and privacy risks for companies to outsource some of their processing operations in India where there is a lack of a clear privacy legal framework.

It should be noted, however, that the Indian government has been particularly criticized for lack of enforcement of the cyber crimes Act. A November 2003 news report in the *San Francisco Chronicle* about the off-shore processing of credit reporting data noted that India has only charge 11 individuals with violations of the Act, and only prosecuted 2 of those people fully.¹⁹ The report suggests that this lack of local enforcement puts U.S. companies and citizens at risk. It is likely that the gap between the law and its enforcement will continue to create problems for companies that select processors in India, and the company should consider what steps it can take to minimize the risks associated with non-responsiveness of the Indian authorities and court systems.

Closing Thoughts

As each company considers its outsourcing options, it must understand both the impact of laws of the country where the data originates and well as the laws of the country where the data will be processed. Because the responsibility for compliance with the originating-countries' laws will continue to rest with the company and because the company will also need to ensure that it complies with requirements of applicable state laws as well as any representations it has made, due diligence about the vendor and the receiving-countries' legal systems must be complete.

Once the due diligence is complete, the company must ensure that appropriate protections are built into its vendor contracts. These protections include thoughtful contractual provisions related to confidentiality, appropriate use, data security, audit rights, insurance and remedies. We recommend that a safeguards schedule be included in the outsourcing contract in order to provide sufficient detail on the security expectations. Ongoing vendor monitoring and management is also essential. In each case, the level of effort needed will depend on the amount and sensitivity of the personal information being processed.

For all off-shore relationships, I also recommend that the company develop a formal plan for responding to "worst case scenario" type events, such as misappropriation of personal data. This plan would contain an analysis of legal remedies available in the jurisdiction. It would identify both local legal resources that could be called upon quickly as well as the legal recourse that would be sought in the event of a security incident or breach of contract.

If you have any questions or comments about any of the matters described in this paper, please do not hesitate to Peggy Eisenhauer at 404-888-4128 (in Atlanta) or via email to peisenhauer@hunton.com.

¹⁸ See www.privacyinternational.org.

¹⁹ CREDIT AGENCIES SENDING OUR FILES ABROAD, *San Francisco Chronicle*, November 7, 2003.