

SCIENCE AND TECHNOLOGY LAW REVIEW

www.stlr.org

EXPORTING TRUST WITH DATA: AUDITED SELF-REGULATION AS A SOLUTION TO CROSS-BORDER DATA TRANSFER PROTECTION CONCERNS IN THE OFFSHORE OUTSOURCING INDUSTRY

Sunni Yuen*

Personal data privacy has recently surfaced as a prominent issue in offshore outsourcing. Concern about the security of data transferred to offshore outsourcing destinations with weak or non-existent information privacy laws has enabled a new industry of trustmark providers, which offer accreditation and monitoring services to companies that seek self-regulation with respect to data privacy. However, a uniform international approach is vital to ensure that a minimal level of protection attaches to data transferred in the outsourcing business. Through its “adequacy requirement,” the European Union Data Directive has emerged as the predominant working model of a uniform standard for cross-border data transfer privacy protection.

Yet a fully international adoption of the Directive has been frustrated by sovereignty concerns, differing cultural perceptions of privacy, and bargaining power disparity. This has enabled the United States to negotiate a bypass of the adequacy requirement altogether. An audited self-regulatory trustmark industry would be a more effective approach that preserves the United States’ sector-specific and self-regulatory system. Businesses wishing to outsource would apply and receive certification from a trustmark provider, which would guarantee that the business has undertaken contractual mechanisms and implemented internal practices to comply with the EU Data Directive standard of data protection. The trustmark providers would audit such businesses for continual compliance, and in turn be subject to regulation by a single agency under European Commission oversight.

* J.D. Candidate 2008, University of Pennsylvania Law School; B.A. 2005, Cornell University. My sincerest thanks to Professor Philip J. Weiser and Professor F.M. Scherer for their tremendous guidance, encouragement, and inspiration. I am also very grateful to Professor Wendell Pritchett for his invaluable support.

1. INTRODUCTION

The world's most popular search engine¹ recently suffered a renewed bout of criticism for being inconsistent with its corporate mantra of "Don't be evil"² when it announced³ plans to acquire online-advertising broker DoubleClick.⁴ While content producers and civil liberties groups have previously accused Google of violating this mantra by pursuing commercial goals at the expense of their respective copyright and free speech concerns,⁵ this fresh round of criticism is distinctive for two reasons. First, all Google users, rather than any particular special interest group, comprise the affected party. Second, in response to objections from privacy advocates and competitors, Google

¹ See *Who's Afraid of Google?*, Economist, Sept. 1, 2007, at 9 [hereinafter *Google Economist*] (describing Google as the "world's most popular search engine" and "[t]he world's internet superpower"); see also Press Release, Nielsen//Netratings, Nielsen//Netratings Announces August U.S. Search Share Rankings (Sept. 19, 2007), http://www.nielsen-netratings.com/pr/pr_070919.pdf (reporting that in August 2007 alone, 53.6% of all search queries were conducted at Google Search).

² Google Code of Conduct, <http://investor.google.com/conduct.html> (last visited Nov. 6, 2007) (explaining that the motto exemplifies adherence to the "highest possible standard of ethical business conduct" to protect Google's "reputation as a company that warrants [its] users' faith and trust").

³ Press Release, Google, Google to Acquire DoubleClick (April 13, 2007), <http://www.google.com/intl/en/press/pressrel/doubleclick.html> ("The combination of Google and DoubleClick will offer superior tools for targeting, serving and analyzing online ads of all types, significantly benefiting customers and consumers . . .").

⁴ See Larry Dignan, *Google/Microsoft Testimony: Neither Side Seems Honest*, Seeking Alpha, Sept. 28, 2007, <http://seekingalpha.com/article/48454-google-microsoft-testimony-neither-side-seems-honest> (criticizing Google's assertion that the company was "late to display advertising" because of concern for consumer privacy, necessitating the acquisition of DoubleClick so the company can catch up); Marc Rotenberg, Letter to the Editor, *Google's Proposals on Internet Privacy Do Not Go Far Enough*, Fin. Times, Sept. 24, 2007, at 12, available at <http://www.ft.com/cms/s/0/764c5338-6a32-11dc-a571-0000779fd2ac.html> (asserting that neither Google nor DoubleClick has "done a particularly good job protecting online privacy and the combined company would pose a unique and substantial threat to the privacy interests of internet users around the globe").

⁵ See *Google*, Economist, *supra* note 1, at 9 ("Television networks, book publishers and newspaper owners feel that Google has grown by using their content without paying for it. Telecoms . . . are miffed that Google prospers . . . by free-riding on the bandwidth that they provide . . . [and] [l]ibertarians dislike Google's deal with China's censors."); see also Josh McHugh, *Google vs. Evil: Google Sells Its Soul*, Wired, Jan. 2003, at 130, 132-34, available at http://www.wired.com/wired/archive/11.01/google_pr.html (discussing how Google was pressured to remove links from its index to anti-Scientology websites after a copyright violation complaint from the Church of Scientology and how Google struck an agreement with Chinese authorities to limit the search results available to China's internet users for politically sensitive queries).

proclaimed that an international body ought to promulgate new international standards on the collection and use of consumer data “to create minimum standards of privacy protection that meet the expectations and demands of consumers, businesses and governments.”⁶

Google’s call for an international data privacy standard is a smart move.⁷ A rash of highly publicized data theft cases both in the United States⁸ and abroad⁹ has made even the lay Internet user wary¹⁰ of entrusting so much information to a company that primarily derives its profits from “paid search” advertising – that is, by “selling to

⁶ Peter Fleischer, Global Privacy Counsel, Google, Address at UNESCO Conference on Ethics and Human Rights in Information Society: The Need for Global Privacy Standards 7 (Sept. 14, 2007), available at <http://portal.unesco.org/ci/en/files/25452/11909026951Fleischer-Peter.pdf/Fleischer-Peter.pdf>.

⁷ Google has also responded to privacy organizations’ criticisms by publicly announcing that it will reduce the storage term of identifiable information from search logs to eighteen months and that of its cookies (data-tracking files containing unique ID numbers) to two years. See Posting of Peter Fleischer to The Official Google Blog, <http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html> (July 16, 2007, 9:52 EST) (“[L]ogs anonymization and cookie lifetime reduction . . . are part of our ongoing plan to continue innovating in the area of privacy to protect our users.”). But see Anick Jesdanum, *Will New Google Cookie Policy Enhance Privacy?*, MSNBC, July 18, 2007, <http://www.msnbc.msn.com/id/19833569/> (reporting however, that the policy change may have little practical effect since the cookies will automatically renew whenever users “revisit the Google search engine”).

⁸ There have been over 215,951,442 records containing sensitive personal information involved in security breaches since early 2005. The Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (last visited Nov. 6, 2007). This includes the 163,000 records maintained by ChoicePoint that were compromised by I.D. thieves, Bank of America’s lost backup tape containing 1.2 million records, and the Department of Veteran’s Affairs’ stolen laptop holding 28.6 million records of all American veterans discharged as of 1975. *Id.*

⁹ See Larry Greenemeier, *International Citibank Customers Shaken By Data Breach: Bank halts PIN-based transactions in three countries after customer data is compromised at a third-party company*, InformationWeek, Mar. 8, 2006, <http://www.informationweek.com/showArticle.jhtml?articleID=181502068> (reporting that Citibank refused to “name the third-party business whose systems were breached” and did not “specify how or when its affected customers were notified”).

¹⁰ Popular media has extensively documented Google’s various privacy issues. For instance, the New York Times has reported privacy concerns over Google Maps’ “Street View” feature (which provides detailed pictures of people’s private homes and of pedestrians in public places). Miguel Helft, *Google Zooms In Too Close For Some*, N.Y. Times, June 1, 2007, at C1 (reporting concerns over street view snapshots in which a person’s facial features and license plate number are clearly visible). And the Simpsons cartoon series has satirized the threat to privacy posed by Google Maps’ “Street View” feature. *Inside the Googleplex*, Economist, Sept. 1, 2007, at 56, 56 [hereinafter *Googleplex*].

advertisers information about what you are doing”¹¹ so that advertisers are better able to target you.¹² The information collected from Google users includes search queries (which comprise a record of one’s interests), responses to advertisements, e-mail correspondence, calendar data, credit card information, contacts, social networks, documents, spreadsheets, photos, videos, and, at some future date, possibly even medical records and precise physical location (based on cell phone information).¹³ All this data constitutes *personal information*, any piece of information that can potentially be used to uniquely identify, contact, or locate a single person.¹⁴ Privacy concerns stem from breaches and abuse in the collection, storage, transfer, and use of this uniquely identifiable information. Since Google’s services operate by means of “vast clusters of servers, spread out in enormous datacenters around the world,”¹⁵ users’ personal information is routinely routed to and stored in datacenters abroad, which makes remedies for their breach and abuse difficult – not least because of the jurisdictional and enforcement issues.

The issues Google faces as a global “corporate custodian” of personal information are analogous to the data privacy issues that companies engaging in offshore outsourcing face. Similar to Google, these companies routinely transfer personal information abroad and must balance business goals (i.e., profit-seeking and efficiency) with increasingly vocal consumer concerns over data privacy.¹⁶ A recent survey reports that 82% of U.S.-based participants felt there ought to be regulation regarding the use of their data “to ensure that companies outsourcing services offshore had adequate security and privacy

¹¹ *Google Economist*, *supra* note 1.

¹² Compiling information dossiers on users, in which, for instance, one’s search history is matched with his location and agenda in his calendar to “serve increasingly useful and welcome search results and ads.” *Googleplex*, *supra* note 10, at 58.

¹³ In addition to online search services, Google provides a plethora of other services for uploading and organizing individual information such as an online sharable calendar (Google Calendar), desktop search (Google Desktop), blogging tools and space (Blogger), image indexing and editing software (Picasa), word processing and spreadsheet programs (Google Documents), and social networking (Orkut). *Googleplex*, *supra* note 10, at 56, 58. These services are all linked to a central Google user account such that “Google could soon, if it wanted, compile dossiers on specific individuals.” *Id.* at 56.

¹⁴ This includes but is not limited to financial information such as bank account and taxpayer numbers, genetic and fingerprint data, location information, and health information.

¹⁵ *Googleplex*, *supra* note 10, at 57.

¹⁶ Companies that outsource services to offshore providers arguably face greater challenges in ensuring protection of the transferred information since they have less managerial and structural control over the third-party offshore provider, compared to a company like Google, which merely transfers information to an overseas office.

safeguards.”¹⁷ The survey results are hardly surprising given that Americans may remember headlines from 2003 about the disgruntled offshore medical transcriber in Pakistan who threatened to disclose the University of California San Francisco medical center’s patient records if she wasn’t given her “dues.”¹⁸ In another high-profile case in 2005, customer records outsourced by the Hong Kong and Shanghai Banking Corporation fell vulnerable to three unscrupulous call-center employees in Bangalore who transferred approximately US \$350,000 to fake accounts in Pune.¹⁹

Nonetheless, offshore outsourcing remains a legitimate strategic option in a global economy. The “key inhibitor preventing companies (from using) offshore outsourcing remains data security.”²⁰ Information transferred abroad is only protected insofar as the terms of the contract provide and as the destination country permits, in terms of enforcement and recognition of a cause of action. This may cause difficulties given that, outside the European Union, existing data protection standards worldwide are largely asymmetrical. Thus, a U.S. company’s ability to safeguard the personal information it transfers to a credit card processing company in a country with weaker data protection laws is largely limited to its ability to enforce any data protection clauses in the outsourcing contract. Consequently, risk-adverse firms have an incentive to draft weak data protection contractual assurances or to exclude them altogether, so as to minimize their own liability for the actions of the outsourcing supplier. Even those firms that are *required* by national laws to include data protection provisions in their outsourcing contracts face the problem of enforcing such provisions in a foreign sovereign state.

¹⁷ David Bender & Adam Chernichaw, *Privacy Concerns: Controls or Consequences, Overseas Outsourcing Could Prove Costly*, 236 N.Y. L.J., Oct. 10, 2006, at 5 (2006). See Larry Ponemon, Ponemon Institute, *Americans’ Perceptions about Outsourcing Personal Information*, June 5, 2006, http://www.whitecase.com/files/publication/Americans_Perceptions_about_Outsourcing_Personal_Information.pdf (reporting that a majority of respondents are opposed to sensitive personal information sent offshore, and are particularly concerned about their health records, credit card account numbers, banking information and employee records compromised).

¹⁸ See David Lazarus, *A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay*, S.F. Chron., Oct. 22, 2003, at A1, available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL> (“[While] U.S. laws maintain strict standards to protect patients’ medical data . . . those laws are virtually unenforceable overseas, where much of the labor-intensive transcribing of dictated medical notes to written form is being exported.”).

¹⁹ Dinesh C. Sharma, *Indian Police Make Arrests in Outsourcing Fraud*, CNET News, Apr. 8, 2005, http://news.com.com/2100-1014_3-5660274.html?tag=nl (reporting that data security issues have been a growing concern for companies that outsource work overseas).

²⁰ Ed Frauenheim, *Insecurities over Indian Outsourcing*, CNET News, Apr. 26, 2005, http://news.com.com/2100-7355_3-5685170.html (citing a Merrill Lynch survey of 50 chief information officers from U.S. organizations).

While bilateral data transfer agreements may mitigate some enforcement issues,²¹ such agreements may raise barriers to trade since companies are unable to contract with more economically efficient outsourcing providers based in non-participant countries.

This Article argues that a uniform international approach is necessary to ensure that a minimal level of protection attaches to data transferred in the offshore outsourcing business. It proposes that the approach be substantively modeled on the EU Data Directive on the grounds that the Directive, as the only existing working multi-national model, has already exerted considerable influence over both the data protection *practices* of non-EU firms and the data protection *regulations* of non-Member States. With the EU Data Directive set as the benchmark for cross-border data transfer rules, firms also gain the freedom to contract with the service providers of their choice in a global market, and benefit from lower transactions costs resulting from increased certainty as to compliance with a single set of rules.

Finally, this Article presents a means of implementing the uniform standard of cross-border data transfer rules in a manner that does not usurp national sovereignty. Specifically, it proposes a dual layer of audited self-regulation²² in which offshore outsourcing contracts and practices are channeled through a trustmark industry that certifies firm compliance to the EU Directive standard and in which an independent agency under EU oversight regulates the trustmark industry itself. Part 2 of this paper will discuss the background of outsourcing, and the Coasean justification for it. Part 3 surveys both existing national and multi-national regulatory data protection efforts, including those of the United States and the European Union, as well as those of popular outsourcing destinations such as India. Part 4 analyzes the efficacy of private contractual measures as well as the aforementioned national and inter-governmental organizations' efforts in ensuring cross-border data protection. That section concludes that an international standard for data protection is needed. Part 5 examines the influence of the EU Data Directive on other nations, and argues that the Directive should be set as the

²¹ A bilateral data transfer agreement is an agreement between two nation states stipulating the conditions and procedures for the transfer of personal information of citizens from one state to another, and their subsequent treatment. The agreement can apply generally or to a specific industry. For instance, the agreement between the United States and the European Union to transfer Passenger Name Record data applies only to personal information of citizens of the European Union that is processed and transferred within the aviation industry. *See, e.g.*, Press Release, Council of the European Union, The EU and the United States Reach Agreement on Passenger Name Record (PNR) Data (July 23, 2007), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/95438.pdf; Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, U.S.-Eur. Union, July 26, 2007, 2007 J.O. (L 204) 18 (July 18, 2007), *available at* <http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf>.

²² Audited self-regulation is defined as the delegation of the power to implement rules to a non-governmental entity, subject to review and independent action by a federal agency. *See* Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as a Regulatory Technique*, 47 Admin. L. Rev. 171, 175-78 (1995) (clarifying that audited self-regulation is distinct from purely private and voluntary self-regulatory efforts).

benchmark for data privacy regulation worldwide. Finally, Part 6 advocates audited self-regulation as a means of attaining that international standard through the creation of an independent agency responsible for monitoring firm outsourcing contracts and practices for compliance. The agency would function under European Commission oversight, and effectively regulate the accreditation companies responsible for auditing firm practices and issuing certificates of compliance – the latter of which will, in effect, be mandatory for offshore outsourcing.

2. BACKGROUND AND ECONOMIC ANALYSIS OF OUTSOURCING

Outsourcing is the practice of transferring the entire responsibility for business process or information technology applications development to an external service provider – often overseas – to reduce costs and achieve a competitive advantage.²³ Functions commonly outsourced in business process outsourcing (“BPO”) include call and contact centers, document processing, payroll management, human resources management, medical record transcription services, credit card application and bill processing, insurance claims, accounting services, financial service processing and operations, airline ticketing, market research, and research and development.²⁴ As such, sensitive personal information²⁵ including birthdates, social security numbers, blood types, and credit card numbers, is routinely transferred to India, the Philippines, and other popular outsourcing destinations.²⁶

²³ Information technology outsourcing (comprising data center management, telecommunications, software development, IT architecture and system maintenance) also raises legitimate and oftentimes parallel data protection concerns, particularly where it overlaps with IT-enabled services such as IT help desks. Mark Kobayashi-Hillary, *Outsourcing to India* 92 (2d. ed. 2005). However, brevity requires that this paper focus on BPO.

²⁴ *Id.* at 69, 167.

²⁵ Personal data is defined as “any information relating to an identified or identifiable individual (data subject).” Organization for Economic Co-Operation and Development [OECD], Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80) 58 Final (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html [hereinafter “OECD Privacy Guidelines”]. The OECD Privacy Guidelines also distinguish between sensitive and non-sensitive personal data based on whether the nature of the data is treated as inherently sensitive; the drafters give medical records as an example. *Id.*

²⁶ Aside from India, China, Vietnam, the Philippines, Russia, Brazil and Poland are popular outsourcing destinations. *See* Adrienne Selko, *Logistics Industry Gets Good Marks from CapGemini Study*, *IndustryWeek*, Nov. 7, 2007, *available at* <http://www.industryweek.com/ReadArticle.aspx?ArticleID=15280>; Andy McCue, *Vietnam: The Next Offshoring Hot Spot?*, *CNET News*, July 10, 2007, http://www.news.com/2100-1011_3-6195726.html.

2. 1. *Economic Analysis of Outsourcing*

In his seminal “Theory of the Firm,” Coase posited that firms are formed because there are transaction costs to use the market.²⁷ Transaction costs, which measure the cost of obtaining a good or service through the market, include: search and information costs; bargaining costs; costs of protecting trade secrets; and policing and enforcement costs.²⁸ In their absence, arms-length transactions would be sufficient to bring a good or service through the market.²⁹ Thus, firms arise when they can internally produce the good or service more efficiently thereby saving on the transactions costs of using markets.³⁰

Firms will “grow and manage activities internally until it’s cheaper to outsource that activity.”³¹ Specifically, a firm will engage in offshore outsourcing so long as its production cost savings (i.e., the search, negotiation and enforcement costs of procuring a BPO provider) are greater than the additional transaction costs it will incur when dealing outside the firm.³² Since the strategic purpose of business process outsourcing is to delegate “one or more business process functions to an external service provider,”³³ the decision to outsource the activity or function allows the company to focus its resources

²⁷ See Ronald H. Coase, *The Nature of the Firm*, 4 *Economica* 386, 392 (1937) (“[T]he operation of a market costs something and by forming an organisation and allowing some authority (an ‘entrepreneur’) to direct the resources, certain marketing [transaction] costs are saved.”).

²⁸ See Thomas Lah, *Coase, Product Companies, and Professional Services*, informIT.com, Nov. 9, 2001, <http://www.informit.com/articles/article.asp?p=24040> (applying Coase’s model of transaction costs to the outsourcing of professional services by products companies).

²⁹ If there are no transaction costs (i.e., zero cost to finding out what the relevant prices are), then the most “obvious cost of ‘organising’ production through the price mechanism”, Coase, *supra* note 27, at 390, does not exist. This reduces the incentive for firm formation because there’s no need for an authority to coordinate resources in order to save on transaction costs. *But see id.* at 390-91 (“The costs of negotiating and concluding a separate contract for each exchange transaction which takes place on a market must also be taken into account.” (footnote omitted)).

³⁰ The Library of Economics & Liberty, *The Concise Encyclopedia of Economics*, Biography of Ronald H. Coase, <http://www.econlib.org/library/Enc/bios/Coase.html> (last visited Nov. 11, 2006).

³¹ Lah, *supra* note 28.

³² Erran Carmel & Paul Tjia, *Offshoring Information Technology: Sourcing and Outsourcing to a Global Workforce* 35 (2005).

³³ ASSOCHAM, *Business Process Outsourcing: Trends and Insights 1* (2003) [hereinafter “ASSOCHAM BPO”].

on its core competencies.³⁴ Moreover, this is attained with a much reduced transaction cost (e.g., the cost of sending the information, which has been significantly reduced with the advent of the PC, Internet, and underwater fiber-optic cable).³⁵ The introduction of the latter is particularly significant because it allows “any service, call center, business support operation, or knowledge work that could be digitized [to] be sourced globally to . . . [the] most efficient provider.”³⁶

Given that business functions such as call centers and payroll processing operations do not require firms to invest in a vast amount of expensive infrastructure (compare computers, phone lines, and Internet connectivity with factories), labor is probably the greatest production cost savings that firms can capture in offshore outsourcing. Assuming that the search, contract negotiation, governance, and risk mitigation costs a firm incurs in seeking and engaging an offshore BPO provider do not outweigh the firm’s savings from labor arbitrage,³⁷ a firm will outsource its “labor where it is cheapest to use it [so that] it can earn the greatest return.”³⁸ Offshore BPO offers the added benefit of service outside of business hours because of the time difference between India, for instance, and the United States.³⁹ Also, the BPO provider will be incentivized to fine-tune its technical expertise and upgrade cutting-edge infrastructure to remain competitive, thus enabling a firm to externalize the labor (and capital) costs of upgrading

³⁴ Core competencies consist of the fundamental parts of a business’ “value proposition” – that is, the elements or functions that constitute the company’s competitive advantage. See Paul Davies, *What’s This India Business?* 22-23 (2004) (pointing out that Microsoft does not itself engage in business functions related to its business such as printing, packaging, internal administration, distribution or security desk staffing, focusing instead on its core competence in IT research and development).

³⁵ See Barbara Crutchfield George & Deborah Gaut, *Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing*, 6 U.C. Davis Bus. L.J. 1, 9-10 (2006) (summarizing the rise of outsourcing to India in the late 1980s, and identifying the dot-com bustle and subsequent bust for creating “an entirely new form of outsourcing collaboration to tap the pool of talent in India”).

³⁶ *Id.* (quoting Thomas L. Friedman, *The World is Flat* 109 (Farrar, Straus and Giroux 2005)).

³⁷ Wage differentials between countries can translate into labor cost savings of 30 to 50% through offshore outsourcing. ASSOCHAM BPO, *supra* note 33, at 2.

³⁸ Carmel & Tjia, *supra* note 32, at 31.

³⁹ See Bryan Bertram, Note, *Building Fortress India: Should a Federal Law be Created to Address Privacy Concerns in the United States-Indian Business Process Outsourcing Relationship?*, 29 B.C. Int’l & Comp. L. Rev. 245, 248 (2006) (“Another desirable attribute of overseas BPO is the ability to realize around-the-clock operations -- when the workday ends in the United States, it is just beginning in India.”).

such infrastructure.⁴⁰ These are all compelling reasons for firms to seek outside service providers.

2.2. Incentives for Data Protection Measures in Outsourcing

The primary benefits that companies attain when they outsource include economies of scale, scope, and specialization,⁴¹ which is a product of the subsequent concentration of resources on the core competencies. Companies will necessarily

incur costs such as vendor search, negotiations, and legal fees to establish these [outsourcing] relationships. However, more important, these costs are often dwarfed by contractual *risks* associated with inefficient contracts, due to differences in information between the parties (asymmetric information), inability to observe actions comprehensively; and the inherent incompleteness of . . . contracts. These risks are often driven by the . . . parties' inherent risk aversion and bounded rationality . . .⁴²

Certainly, one chief consideration is the risk of strong adverse client or customer reactions to their personal information being sent abroad. Even outsourcing guide-books for managers warn that “[f]ailure to consider and plan for privacy issues can bring unwanted consequences, such as bad publicity, official enforcement actions, fines and penalties, and private lawsuits. Even more damaging is the loss of public trust that can result from privacy problems.”⁴³

Most firms are sensitive to public perception and this sensitivity has only been heightened by the media attention given to recent data privacy breaches. Dell, Capital One, and Conesco are several firms that have been partially motivated by data security concerns to “shift at least some customer-support operations back to the United States”⁴⁴;

⁴⁰ See Robert M. Weiss & Amir Azaran, *Outward Bound: Considering the Business and Legal Implications of International Outsourcing*, 38 Geo. J. Int'l L. 735, 738 (2007) (“[T]he expertise of foreign vendors often compares quite favorably with domestic expertise for the types of work that outsourcing requires. Utilizing the technical expertise of the vendor allows the customer to take better advantage of modern technologies while simultaneously externalizing the costs of software and hardware upgrades--costs that vendors are better able to bear effectively by distributing them among their customer base.” (footnote omitted)).

⁴¹ Eli M. Snir, *Economics of Information Technology Outsourcing and Markets* 28 (2000) (unpublished Ph.D. dissertation, University of Pennsylvania) (on file with Van Pelt Library, University of Pennsylvania).

⁴² *Id.*

⁴³ Carmel & Tjia, *supra* note 32, at 115.

⁴⁴ Norm Alster, *Customer Disservice? Critics say the Promised Savings from Offshoring Come at Too Steep a Price, while Companies Say Very Little at All*, CFO Mag., Oct. 26, 2005, at

this movement, in conjunction with unexpectedly high costs of managing offshore operations, has led a consultant to claim that “[t]he economic benefits of outsourcing customer service are grossly overstated.”⁴⁵ A data breach resulting in a loss of 10,000 customer records could “conservatively cost over \$6 million,” and in early 2006, three breaches within a month resulted in a price tag of over \$24 million in credit monitoring expenses alone.⁴⁶ The cost of repairing damaged customer relations involves more than just credit monitoring expenses, which are viewed as temporary solutions.⁴⁷ Consumers want preemptive measures taken to guarantee that their personal data is safe and kept confidential.⁴⁸

6, available at 2005 WLNR 17994801. Note however, that whether personal information processed in the United States would actually be more secure than in an outsourcing operation depends on the firm’s policies and practices and whether the information falls under industry-specific privacy legislation. As discussed *infra* in section 3.1, the United States has no comprehensive privacy regulation. However, the benefit of domestic handling of the information is that consumers are more aware of any data breaches and can more easily hold the firm accountable by publicly demanding answers and seeking legal solutions. See Justin Kent Holcombe, *Solutions for Regulating Offshore Outsourcing in the Service Sector: Using the Law, Market, International Mechanisms, and Collective Organization as Building Blocks*, 7 U. Pa. J. Lab. & Emp. L. 539, 562 (2005) (“Evidence already demonstrates that common law will apply to data collection and offshore outsourcing transactions. The U.S. Department of Commerce acknowledged this possibility in a 2000 letter to the European Commission . . .”).

⁴⁵ Alster, *supra* note 44.

⁴⁶ OutsourcingPipeline.com, Calculate the Cost of a Data Privacy Breach, <http://whitepaper.outsourcingpipeline.com/cmpoutsourcingpline/search/viewabstract/84192/index.jsp> (last visited Nov. 30, 2006).

⁴⁷ See, e.g., Posting of Michael Singer, msinger@cmp.com, to InformationWeek’s Security Weblog, *Lost Your Data? What’s It Worth to You?*, http://www.informationweek.com/blog/main/archives/2007/05/lost_your_data.html (May 16, 2007, 14:41) (criticizing both the government and companies such as IBM for offering no more than a year’s worth of credit monitoring as compensation for loss of personal information). Further, credit monitoring may not even be an effective solution to data theft since it may “fail to detect that a credit request was even made . . . [f]or example, a fraud artist may use someone else’s personal identification information – like a Social Security number – but take out a loan in his or her own name.” Eric Dash, *Protectors, Too, Gather Profits from ID Theft*, N.Y. Times, Dec. 12, 2006, at A1, available at <http://www.nytimes.com/2006/12/12/business/12credit.html>. See also Robert L. Scheier, *Your Data’s Less Safe Today Than Two Years Ago*, ComputerWorld, Aug. 20, 2007, available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9031104&pageNumber=2> (“Thieves may wait a year or more before using the data, and may use only some of it so as to not alert the card issuer . . .” thus rendering one year’s worth of monitoring useless).

⁴⁸ Consumers are often confused by credit monitoring advertisements that promise identity theft protection and can conflate “prevention” with “detection.” Dash, *supra* note 47. While

Moreover, consumers do not expect to shoulder the costs of these preemptive safeguards even though firms will want to pass these costs on to them.⁴⁹ If firms do not undertake these measures at their own costs, consumers will vote with their wallets by switching loyalty to competitors that do not take such risks with their information.⁵⁰ Of course, this is preconditioned on the existence of competitors that engage in better data protection practices or at least have not been in the headlines for data breaches.⁵¹ This means that companies with monopolistic or overwhelmingly dominant market positions are less sensitive to public perception and are therefore “more apt to risk customer alienation where near-term savings can be realized.”⁵² Potential irate customers and poor public perception do not pose sufficient incentives for firms across the board to undertake adequate data protection measures. This suggests that a uniform standard for cross-border data transfer must be mandated for all firms that currently are or are considering engaging in offshore outsourcing.

credit reporting services can assist in detection, they certainly do not, as consumers expect, prevent the security breach of personal information in the first place.

⁴⁹ Given that consumers are reluctant to spend money to prevent firms from selling personal information even *after* they’ve already entrusted the firms with the information, it is unlikely that consumers will be any less reluctant to pay a ‘privacy premium’ in selecting which firms to process their data in the first place. See Dan Tynan, *The Privacy Market Has Many Sellers, But Few Buyers*, Wired News, Sept. 3, 2007, <http://www.wired.com/techbiz/startups/news/2007/09/privacy> (reporting that “most [individual] subjects [or consumers] were unwilling to spend even a quarter to keep someone from selling sensitive information about them -- such as their weight or number of sex partners” and that commercial businesses drive the demand for electronic privacy services and products). *But see* Janice Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study 1* (June 2007), <http://weis2007.econinfosec.org/papers/57.pdf> (reporting that in the context of web retailers, “when privacy information is made more salient, consumers are willing to pay a premium for privacy when purchasing both non-privacy-sensitive and privacy-sensitive items”).

⁵⁰ See *Privacy in the Age of Transparency*, CNET News, Mar. 14, 2004, http://www.news.com/2030-1069_3-5172731.html [hereinafter *Age of Transparency*] (“Business-to-consumer companies that fail to protect customer data can lose the trust and loyalty of customers, and drive them to other companies with which they feel more comfortable sharing personal information.”); Bob Sullivan, *Bad-news Data Letters Push Consumers to Stray*, MSNBC, Oct. 4, 2005, <http://www.msnbc.msn.com/id/9581522> (reporting that “Millions of consumers say they’ve dumped companies that leaked their confidential information last year [2004]”).

⁵¹ See *Age of Transparency*, *supra* note 50 (naming Dell and Microsoft as companies making data privacy a priority).

⁵² Alster, *supra* note 44.

3. THE DATA PROTECTION REGULATORY LANDSCAPE – DOMESTIC AND ABROAD

The myriad of data protection regulations around the world runs the whole gamut from very strong to non-existent. The predominant concern with offshore outsourcing arises when information is transferred from a company (or office) operating in a country with strong data protection regulation to one with weaker (if any) regulation.⁵³ If cross-border data flows to a destination country with weak data protection laws, how does one ensure that data protection does not get diluted through the transfer process? While the regulations of the originating country of the information may technically govern the data transferred abroad, for sovereignty and jurisdiction reasons, there is no guarantee that the information will remain protected in the destination country absent local regulations providing for it. The level of protection will vary depending on whether the origin and destination countries are mutually bound by an inter-governmental standard. It will also depend on whether the origin country has nation-wide data protection regulations that hold companies who engage in offshore outsourcing accountable to the public for breaches in data sent abroad. A brief survey of the data privacy standards of some common origin and destination countries, and the privacy guidelines of international organizations such as those of the Asia-Pacific Economic Co-operation (“APEC”) and OECD will inform the analysis.

3.1. *The United States – A Sectoral Law Approach*

The U.S. approach to data protection is largely predicated on a model of self-regulation.⁵⁴ The existing federal regulations relating to data protection are industry or sector-specific,⁵⁵ rather than comprehensive. Congress has enacted sector laws relevant

⁵³ It is logical to assume that there are no issues resulting in an “upgrade” of data protection when information is transferred from a country with weaker data protection laws to one with stronger.

⁵⁴ See Holcombe, *supra* note 44, at 553 (“The most comprehensive data privacy protections relate to financial information and health care.”).

⁵⁵ The sector-specific laws address protection for categories of data as varied as cable subscriber information, personal information submitted online by children, and the biometric and biological information collected from visitors to the United States. See Marc Rotenberg, *The Privacy Law Sourcebook 2004 - United States Law, International Law, and Recent Developments* 182, 277 (4th ed. 2004) [hereinafter *Privacy Sourcebook*] (referring to *The Cable Communications Policy Act*, 47 U.S.C. § 551 (1984)); see also *The Immigration and Naturalization Service Data Management Improvement Act*, 18 U.S.C. § 1365a (2000); *The Children’s Online Privacy Protection Act*, 15 U.S.C. § 6501 (1998). Although the *Privacy Act of 1974* is the sole omnibus data privacy legislation in the United States, it is applicable only to personal information collected by the U.S. Government and thus not relevant to the outsourcing discussion.

to outsourcing in the areas of personal health, education and medical records, and personal financial information.⁵⁶ Laws such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and California's identity protection law have been identified by India's National Association of Software and Service Companies ("NASSCOM") as U.S. regulations with which offshore BPO providers must comply.⁵⁷ But because the data protection provisions of these sector laws vary in terms of the strength of protection they afford and in their enforcement mechanisms, there is no consistent approach to ensuring the protection of data in outsourcing (which spans industry lines).⁵⁸ The holes in the net of sectoral laws have given rise to self-policing and a complementary trustmark industry.⁵⁹

In order to gain consumer confidence, companies and industry bodies establish codes of data privacy practices (i.e., privacy policies) and then seek to communicate their compliance to the public. Securing a trustmark, which is defined as:

Any certificate, symbol, [or] sign, based on information or meta-information (information about information) provided by a third-party that is aiming to enhance peoples [sic] trust into a certain product, service, relationship, information provider or piece of information perceived as being trustworthy by the organization issuing the trustmark; and/or to

⁵⁶ Carmel & Tjia, *supra* note 32, at 115. See also Appendix A of this Article, *infra*, for details on federal legislation on data protection that are relevant to offshore outsourcing.

⁵⁷ Elec. Privacy Info. Ctr. & Privacy Int'l, Privacy & Human Rights: An International Survey of Privacy Laws and Developments 395 (2005), available at <http://www.privacyinternational.org/index.shtml> (follow "Privacy and Human Rights" hyperlink on the left sidebar; then follow "Privacy and Human Rights 2005" hyperlink towards the bottom of the page).

⁵⁸ For instance, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.), entrusts the Department of Health and Human Services to enforce civil penalties for non-compliance, while the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.), entrusts seven federal agencies including the Federal Trade Commission with enforcement capabilities. See Appendix A, *infra*, for more details.

⁵⁹ Ralf Bendrath, *The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection*, in *The Resurgence of the State: Trends and Processes in Cyberspace Governance* 20-21 (Myriam Dunn et al. eds., 2007), available at <http://userpage.fu-berlin.de/~bendrath/The-Return-of-the-State-in-Cyberspace-final-edit.doc> ("[A] number of codes of conduct were developed early on by different industry and trade associations . . . [many of which] award 'privacy seals' to websites that publicly declare their adherence to the specific data protection standard [but] . . . [t]hese mostly US-based certificate schemes are often less supportive of privacy . . .").

enhance the ability of people to evaluate the trustworthiness of information, services or products,⁶⁰

is one way for firms to display a badge of their membership in a community that practices personal information integrity.

The trustmark industry is currently well established on the World Wide Web.⁶¹ TRUSTe is an illustrative example of an accreditation organization that issues trustmarks to “provide identification of the web trader, connection to a redress mechanism, verification of its business practice record, and coercion of the web trader by the redress mechanism.”⁶² TRUSTe issues a web privacy seal (i.e., a trustmark) to a website operator once: 1) the operator has completed a privacy assessment report; 2) the website’s information gathering and storage mechanisms have been audited and reviewed by a TRUSTe agent; and 3) the operator has agreed to continual monitoring by TRUSTe and to address consumer complaints through online dispute resolution.⁶³ Thus, a firm which purchases membership in a TRUSTe accreditation and monitoring program seeks to assure users that it has undertaken online data protection measures by displaying a web privacy seal on the website. This system is designed so that “the simple fact of community membership creates [social] trust because membership creates expectations of behavior according to the community’s norms.”⁶⁴

3.2. India – Expanding Sectoral Laws to Attain Comprehensive Data Protection

At this time, India has no comprehensive data protection law. Instead, sectoral laws govern data protection in small areas of the economy. For example, the Telecom Regulatory Authority of India requires telecommunications service providers to guard the privacy of their subscribers when national security is not implicated, and the Public Financial Institutions Act of 1993 provides for confidentiality in bank transactions.⁶⁵

⁶⁰ Heidelberg Consensus Recommendations on Trustmarks, 2 J. Med. Internet Res., at e12(Supp. 2 2000), available at <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1761874>.

⁶¹ See, e.g., PrivacyBot.com, <http://www.privacybot.com> (last visited Nov. 16, 2006) (advertising a “6 Step Wizard” that will generate a Privacy Policy in 10 minutes, which can be displayed immediately on a provisional basis until active membership is secured by “an online Compliance Checklist and site visit by our staff”).

⁶² Thomas Schultz, *Does Online Dispute Resolution Need Governmental Intervention? The Case for Architectures of Control and Trust*, 6 N.C. J.L. & Tech. 71, 81 (2004).

⁶³ See TRUSTe, *Begin Building Trust Now*, http://www.truste.org/businesses/how_to_sign_up.php#firststep (last visited Nov. 16, 2006) (stating that the Web Privacy Seal Process is an effective means of alleviating users’ concerns).

⁶⁴ Schultz, *supra* note 62, at 82.

⁶⁵ Privacy & Human Rights, *supra* note 57, at 394-95.

However, the Information Technology Act (“IT Act”) of 2000 does address “computer crime, hacking, damage to computer source code, breach of confidentiality and viewing of pornography.”⁶⁶ Under the IT Act, hacking and tampering with computer source code is a penal offense “when the computer source code is required to be kept or maintained by law.”⁶⁷

According to ASSOCHAM, sections 4, 5, 7 & 79 of the 2000 Act also have a “bearing upon the Indian Outsourcing Industry.” Section 4 provides that “all electronic information, electronic records, electronic documents, and electronic databases [are] legal electronic records, which can be duly proved and produced in a court of law.”⁶⁸ Section 5 provides legal recognition for digital signatures as means of authenticating electronic records and authorizing the government to appoint a Controller of Certifying Authorities charged with licensing “certifying authorities before they can operate in India and [who] will act as the repository of all digital signature certificates issued under the Act.”⁶⁹ Where not otherwise expressly provided for by law, section 7 stipulates, as a requirement for retention of electronic records, that the records be retained in the form in which they were originally generated, sent, or received and that details that help identify the origin, date, and time of dispatch or receipt of said records be preserved. Section 79 details the liability of network service providers, which encompasses all intermediaries in the business of network service providing, including internet service providers and “vendors in the Indian outsourcing industry.”⁷⁰

Recognizing that “[t]he Indian Outsourcing Industry primarily deals with data,”⁷¹ the Indian government responded to negative press in the United States and the United Kingdom regarding data theft from Indian call centers⁷² by approving amendments to the IT Act in mid-October 2006. In addition to prescribing security practices and procedures for organizations handling inquiries about the personal information of customers,⁷³ the amendment permits the imposition of fines of over US \$1 million on “companies and

⁶⁶ *Id.* at 397.

⁶⁷ ASSOCHAM BPO, *supra* note 33, at 67.

⁶⁸ *Id.* at 62-63.

⁶⁹ Privacy & Human Rights, *supra* note 57, at 573.

⁷⁰ ASSOCHAM BPO, *supra* note 33, at 64-66.

⁷¹ *Id.* at 67.

⁷² See Raja M, *India Tightens Data Protection Law*, Asia Times, Oct. 20, 2006, available at http://www.atimes.com/atimes/South_Asia/HJ20Df01.html. (“The cabinet decision follows Prime Minister Manmohan Singh’s assurance to foreign IT stakeholders that India is concerned about data theft and will be acting to stop leakage. The amendments also aim to combat phishing (e-mail fraud), identity theft, video voyeurism and other types of computer crime.”).

⁷³ *India to Amend IT Act for Data Protection*, The Times of India, Oct. 16, 2006, available at <http://timesofindia.indiatimes.com/articleshow/2177219.cms> (reporting that the Amendment will be presented in Parliament’s next winter session).

individuals who fail to stop data theft and the leakage of personal information.”⁷⁴ While the amendments to the IT Act are a step closer to stronger data protection, their scope appears largely reactionary and focused instead on the retrieval of personal data. As the amendments do not address the other stages of the data protection cycle,⁷⁵ the IT Act offers only a limited form of comprehensive data protection regulation. Also, the amendments will have to provide for an effective enforcement mechanism or else risk creating legislation with “no teeth.”⁷⁶

3.3. Philippines – An Example of Data Protection by Sectoral Laws and the Prospective Adoption of the APEC Privacy Principles as an International Data Privacy Standard

The Philippines currently has a number of sector-specific laws that protect personal information. The Bank Secrecy Act and Secrecy of Bank Deposits Act govern the confidentiality of deposits with banking institutions, subject to exceptions found in the Anti-Money Laundering Act of 2001 for transactions over approximately US \$75,000.⁷⁷ The Electronic Commerce Act of 2000, which followed the infamous ILOVEYOU e-mail virus,⁷⁸ imposes a minimum fine of approximately US \$1,900 and a

⁷⁴ Raja M., *supra* note 72.

⁷⁵ See Saikat Neogi, *India Needs Comprehensive Data Protection Legislation*, *Hindustan Times*, Sept. 17, 2006, available at <http://www.hindustantimes.com/StoryPage/StoryPage.aspx?id=58aad45b-ea2a-40f3-b961-1f239e44e540> (describing the stages of the data protection cycle as the registration, storage, retrieval, and dissemination of personal data through comparative analysis of U.S. & U.K. law); see also Expert Committee, Ministry of Commc’ns & Info. Tech. of India, Summary of Proposed Amendments to Information Technology Act 2000, available at <http://www.mit.gov.in/download/Summary-final.doc> (It is unclear just how many of the recommendations made by the Expert Committee on Amendments to the IT Act in 2005 are enshrined in the approved amendments. In its report, the Committee submitted a “proposal relating to handling of sensitive personal data or information with reasonable security practices and procedures thereto [and the] . . . [g]radation of severity of computer related offences under Section 66, committed dishonestly or fraudulently [sic] and punishment thereof”).

⁷⁶ See, e.g., Neogi, *supra* note 75 (describing how India has a poor record of cyber-crime enforcement. Specifically, under the IT Act of 2000, “out of every 500 cyber crimes in India, only 50 are reported to the police and out of that only one is actually registered [and the conviction rate is as low as 2 per cent”).

⁷⁷ Elec. Privacy Info. Ctr. & Privacy Int’l, *supra* note 65.

⁷⁸ The ILOVEYOU email virus was a supervirus that destroyed media files on infected computers and self-replicated en masse, crippling servers around the world. See generally Peter Hayes, *No ‘Sorry’ From Love Bug Author*, *The Register*, May 11, 2005, available at http://www.theregister.co.uk/2005/05/11/love_bug_author (reporting that the havoc was such that the FBI was heavily involved); Paul Festa & Joe Wilcox, *Philippine ISP Cooperating with FBI in Virus Probe*, *CNET News*, May 4, 2000, <http://www.news.com/2100-1001-240089.html> (reporting that even anti-virus specialists were over-whelmed by the potency of the virus).

prison term between six months to three years for “unlawful and unauthorized access to computer systems.”⁷⁹ Most relevant to data protection, sections 31 and 32 of the Act stipulate that “only individuals with legal right of possession shall be granted access to electronic files or electronic keys” and “impose[] an obligation of confidentiality on persons receiving electronic data, keys, messages, or other information not to convey it to any other person.”⁸⁰ These provisions suggest that the Philippine legal system allows injunctive relief in the event of a security or privacy breach, which is an important consideration for firms seeking to outsource.⁸¹

The Philippines government has contemplated implementing its first national comprehensive data protection law, which will likely be informed by the Asia-Pacific Economic Cooperation⁸² (“APEC”) Privacy Principles.⁸³ Collectively, the APEC Privacy Principles assert that data subjects should be given notice as to the collection, status, and use of their information, as well as the opportunity to amend the information collected.⁸⁴ The Principles also prescribe limitations on the collection, access, and use of personal information, and recognize that “personal information controllers” (the firms) are charged with ensuring that the information is not exploited.⁸⁵

⁷⁹ Privacy & Human Rights, *supra* note 57, at 559.

⁸⁰ *Id.*

⁸¹ See Margaret P. Eisenhauer, Hunton & Williams, LLP, Privacy and Security Law Issues in Off-Shore Outsourcing Transactions 7 (2005), *available at* http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf (warning that whether a “company could reasonably get an injunction . . . in a local jurisdiction to compel the return or destruction of misappropriated data” is a factor in the due diligence work before making an outsourcing decision).

⁸² The Philippines is a founding member economy of APEC. Other founding members include the United States, Singapore, Canada, Australia, Malaysia and South Korea. See Asia-Pacific Economic Cooperation, <http://www.apec.org/> (last visited Nov. 16, 2006).

⁸³ See Elec. Commerce Steering Group, Asia-Pac. Econ. Cooperation, APEC Privacy Framework 8-19 (2004), *available at* http://www.apec.org/etc/medialib/apec_media_library/downloads/ministerial/annual/2004.Par.0015.File.v1.1 [hereinafter APEC Privacy Principles] (laying out the nine principles of the Framework, with commentary on how to encourage the development of appropriate information privacy protection that also ensures the free flow of information in the Asia-Pacific region; the stated objective of the APEC Privacy Principles is to “promote electronic commerce throughout the Asia Pacific region” by ensuring free flow of information while bolstering consumer and business confidence through the development of information privacy protection).

⁸⁴ *Id.* at pt. III, princ. II, p.8 (listing also that subjects should be given notice as to “the types of persons or organizations to whom personal information might be disclosed” and “the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information”).

⁸⁵ *Id.* at pt. i, cmt. 10, p.6 (“[W]here a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf,

Significantly, Principle IX touches on the central issue of data protection in offshore outsourcing with its assertion that firms should be accountable for exercising due diligence where the personal information will be transferred to another recipient organization.⁸⁶ However, the attached commentary provides little guidance as to how to accomplish this beyond recommending that “reasonable steps” be undertaken to ensure data protection.⁸⁷ It is unclear what enforcement mechanisms may be used to ensure continual protection of the information post-transfer, and when the due diligence would be conducted or deemed impractical.

One general substantive weakness of engaging the APEC Privacy Principles as an international data protection regulatory apparatus stems from the large amount of discretion afforded to firms in determining when it would be “appropriate” or necessary to follow the principles. The language used in the agreement highlights this weakness. For example, Principles III and V (“where appropriate” and “where practical”) and the accompanying commentary do not clearly delineate the context of “appropriateness” or “practicality.” Commentary to Principle VIII also grants firms a backdoor by making their obligation to recognize individual data subjects’ rights of access to the information for confirmation purposes largely discretionary.⁸⁸ Simply put, firms are not required to permit data subjects access to their information if doing so either compromises the

the instructing person or organization is the personal information controller and is responsible for ensuring compliance with the Principles.”).

⁸⁶ *Id.* at pt. III, princ. IX.

⁸⁷ The commentary to Principle IX reads:

Efficient and cost effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed.

Id.

⁸⁸ *See id.* at pt. III, princ. VIII, cmt. 24, p.17 (“[I]t may be necessary for organizations to deny claims for access and correction . . . [including] incidences where it would be necessary in order to protect commercial confidential information that an organization has taken steps to protect from disclosure, where disclosure would benefit a competitor in the marketplace . . .”). Since *commercial* confidential information such as trade secrets is internal to the firm, by permitting data subjects to access and correct their *personal* information the firm is the only one able to determine when this information might be endangered.

protection of firm commercial information or imposes a burden or expense that exceeds the risks posed to the individual's privacy.⁸⁹

It is also crucial to note that the APEC Privacy Principles are designed to be an aspirational rather than a binding framework. This means that member economies are free to adopt the principles piecemeal and with varying degrees of force. Furthermore, APEC members have yet to reach a consensus on the development and implementation of cross-border data transfer rules,⁹⁰ which means that member economies will have to look elsewhere for model guidelines in crafting legislation relevant to data protection in the offshore outsourcing context. For these substantive and technical reasons, the APEC Privacy Principles do not constitute a viable and consistent inter-organizational means of attaining an international standard of data protection regulation.

⁸⁹ See *id.* at pt. III, princ. VIII, p.15-16 (“[T]he burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question [or] . . . the information should not be disclosed . . . to protect confidential commercial information.”); see also *id.* at princ. VIII, cmt. 24, p.17-18 (defining confidential commercial information as “information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss”). Firms, of course, are also treated as having the discretion to calculate the risks to an individual data subject’s privacy.

⁹⁰ The Data Privacy Subgroup of APEC’s Electronic Steering Group met on Sept. 5-8th, 2006 in Da Nang, Vietnam to discuss the development of cross-border privacy rules. A number of concept papers were circulated for discussion, including a co-authored piece by Australia, Korea, Mexico, the United States and the International Chamber of Commerce, entitled the “Cross-Border Privacy Rules Implementation and Operating System.” See APEC Secretariat, 2006 APEC Secretariat Report on APEC Developments 11 (2006), available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2006/pdf.Par.0074.File.v1.1. On Jan. 22-23rd and June 25-26th of 2007 respectively, the First and Second Technical Assistance Seminars of 2007 brought key privacy experts, government officials, privacy regulators, and businesses from APEC member economies to Australia for further discussion on how to reach a consensus on the cross-border data privacy rules. The dialogue will continue in 2008. See Asia-Pac. Econ. Cooperation, Electronic Commerce Steering Group, http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html (last visited Mar. 14, 2007) (reporting that “[p]articipants explored mechanisms that enable industry to meet business and consumer needs through accountable transfers of personal information across economies, which are consistent with the APEC Privacy Framework” and that particular attention was given to the use of trustmarks); Press Release, Asia-Pac. Econ. Cooperation, Electronic Commerce Steering Group, APEC Makes Progress on Cross-Border Privacy Rules, http://www.apec.org/apec/news___media/media_releases/260607_aus_crossborderprivacyprogress.html (last visited Oct. 3, 2007).

3.4 *The OECD Guidelines and the EU Data Directive – A Working Multi-national Standard*

The OECD Privacy Guidelines⁹¹ predate the APEC Privacy Principles as the first internationally derived set of information protection principles intended to offer “harmonized protection of individual privacy rights while being flexible enough to apply across a variety of social, legal, and economic circumstances.”⁹² The eight principles⁹³ of the Guidelines provide for limits to the collection and use of personal data, transparency as to the entire process, security safeguards, and access by individuals to their information. The Guidelines also assign accountability for compliance to the data controllers (firms), and require the destruction or anonymizing of data that no longer serves the original purpose for which it was collected.⁹⁴

The OECD Privacy Guidelines are credited with having an enormous influence on “a variety of legislative and self-regulatory adaptations,”⁹⁵ including the APEC Privacy

⁹¹ OECD Privacy Guidelines, *supra* note 25.

⁹² Global Internet Policy Initiative, The International Legal Framework for Data Protection and its Transposition to Developing and Transitional Countries 1-2 (Dec. 28, 2004), *available at* <http://www.internetpolicy.net/privacy/20041228privacy.pdf> [hereinafter Global Internet].

⁹³ In more detail, the OECD Privacy Guidelines are:

- 1) ‘Collection Limitation’ – there should be limits to the collection of personal data, and that any such data collected ought to be obtained with the consent of the data subject and in a lawful manner;
- 2) ‘Data Quality’ – collected data should be relevant to a specific purpose, and be accurate, complete, and up-to-date;
- 3) ‘Purpose Specification’ – the purpose for collecting the data should be communicated at the outset so that only new purposes that are compatible with the original ones can be introduced, and data that no longer serves a purpose should be destroyed or anonymized;
- 4) ‘Use Limitation’ – data acquired for one purpose should only be used for the specified purposes unless otherwise legally required or the data subject’s consent is obtained;
- 5) ‘Security’ – data must be collected and stored so that it is reasonably guarded from loss or unauthorized access, destruction, use, modification or disclosure;
- 6) ‘Openness’ – there should be general policy of transparency vis a vis developments, practices and policies with respect to the data, and data subjects should have the means to confirm the existence and status of their information, as well as the contact information of the data controller;
- 7) ‘Individual Participation’ – data subjects should have the right to access, confirm and demand correction of their personal information, and;
- 8) ‘Accountability’ – the data controller assumes responsibility for complying with the aforementioned principles.

OECD Privacy Guidelines, *supra* note 25.

⁹⁴ OECD Privacy Guidelines, *supra* note 25.

⁹⁵ Global Internet, *supra* note 92, at 2; *see, e.g.*, Raymond Tang, Privacy Commissioner for Personal Data, Keynote Address at the 4th IAPP Privacy and Data Security Summit and Expo: A

Guidelines.⁹⁶ Five years after their introduction, the OECD extended the Guidelines to trans-border data flows.⁹⁷ Ten years later, the 1995 EU Data Protection Directive⁹⁸ (“EU Data Directive”) abstracted and made the Guidelines binding on EU member states.⁹⁹ The Directive uses the OECD Privacy Guidelines’ definitions of ‘personal data’ and ‘sensitive data,’ and incorporates all eight of the basic Privacy Principles into its standards. To render the OECD Privacy Guidelines’ principles into a working regulatory apparatus, the Directive introduces a “legitimacy” principle in Article 7, which restricts information handling to data processing operations that have a legitimate purpose, unless the unambiguous consent of the individual has been secured. Pertinent to outsourcing, Article 7 stipulates that processing that is either “necessary for the performance of a contract to which the data subject is party” or requested by the data subject entering the contract, qualifies as a legitimate reason.¹⁰⁰

View from Asia – Laying the Foundations for a Consolidated Approach Towards Privacy to Meet the Challenges Ahead (Feb. 19, 2004), *available at* http://www.pco.org.hk/textonly/english/files/infocentre/speech_20040219.pdf (stating that many Asian jurisdictions have scrutinized the OECD as a model for their own privacy legislation and moreover, the OECD “set the benchmark in several Asian jurisdictions that have had strong historical ties with Europe”).

⁹⁶ This is reflected by the preamble portion of the latter that states: “[t]his Framework . . . is consistent with the core values of the OECD’s 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data . . . and reaffirms the value of privacy to individuals and to the information society.” APEC Privacy Principles, *supra* note 83, at pt.1, p.4. While the APEC Privacy Principles have adopted the OECD definition of “personal data controller” and endorsed the “Collection Limitation, Data Quality, and Security principles,” it departs from the OECD’s Guidelines with its greater emphasis on “the benefits of participation in a global information economy.” Global Internet, *supra* note 92, at 4-5. Unlike the OECD Guidelines, the APEC Privacy Principles also do not distinguish between ‘*personal information*’ and ‘*sensitive personal information*’ and “[s]pecifically endorses ‘proportionality’” for regulation and remedy with respect to “the likelihood and significance of harm to an individual.” *Id.* at 4.

⁹⁷ OECD, Declaration on Transborder Data Flows (1985), *available at* http://www.oecd.org/document/25/0,3343,en_2649_34255_1888153_1_1_1_1,00.html.

⁹⁸ Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter EU Data Directive], *available at* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

⁹⁹ *See* EU Data Directive, *supra* note 98, ch.1, art. 4 (requiring each Member State to “apply the national provisions it adopts pursuant to the Directive to the process of data”).

¹⁰⁰ EU Data Directive, *supra* note 98, ch.2, art. 7. Other legitimate reasons include where processing are: 1) necessary for the controller to achieve compliance with a legal obligation to which he or she is subject; 2) necessary to protect the data subject’s vital interests; 3) necessary for “the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; 4) necessary for the “purposes of the legitimate interests pursued by the controller . . . third part[ies] to whom the data are disclosed” assuming that these interests are not overridden by the fundamental rights and freedoms or the interest of the data subject that are protected in Article 1. *Id.*

The Directive also officially recognizes individuals' rights to control the use of information about them, including "the right to be informed that their personal data is being transferred," the right to make corrections to the data, and the right to object to the transfer of data.¹⁰¹ Given that the Openness Principle is interpreted to "require national registration of databases and data controllers,"¹⁰² this emphasis on individual rights extends to creating a directory or record of the information handlers.

Additionally, the Directive arms itself with "teeth" by providing for the creation of a data regulatory authority and introducing sanctions, amongst other means of enforcement, for the violation of its provisions. Article 27 ensures that the Directive will be upheld within the EU by expressly requiring "member states to encourage [the] use of codes of conduct, providing a means to limit discretionary exercise of authority and a flexible means to update national interpretation."¹⁰³ Significantly, Articles 25 and 26 extend privacy safeguards to cross-border personal data transfers to countries *outside* of the European Union through an "adequacy principle." The Adequacy Principle stipulates that data may only be transferred to third countries that provide an "adequate level of data protection,"¹⁰⁴ which will be:

assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations . . . [with] particular consideration . . . given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in th[ose] countr[ies].¹⁰⁵

All the provisions introduced by the EU Data Directive significantly build on and bolster the data protection strength of the OECD Privacy Guidelines. Yet, the Directive's most powerful provisions are Articles 4, 25 and 27, which work in conjunction to create a common scheme for data protection within the European Union and abroad. The National Law Applicability Principle and Codes of Conduct Principle require member states "to enact national data protection laws complying with the Directive's

¹⁰¹ See Privacy Sourcebook, *supra* note 55, at 438, 452 (noting that the Directive grants heightened protection for more *sensitive* types of information by requiring data processors to obtain "unambiguous" consent from the individual for the transfer of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and information concerning health or sex life).

¹⁰² Global Internet, *supra* note 92, at 4.

¹⁰³ *Id.*

¹⁰⁴ EU Data Directive, *supra* note 98, ch.IV, art. 25, 26.

¹⁰⁵ *Id.* at ch.IV, art. 25(2).

standards”¹⁰⁶ and to actively engage in drafting codes by which the national provisions can be implemented.

The Adequacy Principle enhances this common scheme by prohibiting the transfer of personal information gathered from European Union citizens to outside countries without comparable data protection regimes (as determined by a finding of “adequacy”). This essentially forces those outside countries to either adopt similar data protection provisions to attain EU approval¹⁰⁷ or negotiate a bilateral agreement such as the U.S.-EU Safe Harbor Agreement.¹⁰⁸ The EU Data Directive creates a formidable enforcement mechanism against non-compliant firms from outside countries granted “adequacy status” by permitting each member state to enact and enforce its own sanctions including fines, termination of data collection, processing and transfers, as well as permitting private cause of actions for individual data subjects. One example is Spain, which permits fines of up to US \$600,000 per violation, and has already pursued both Microsoft and Telefonica for violating its laws.¹⁰⁹ As Professor Carmel explains, this complicates data transfers in offshore outsourcing:

For example, if you want to transfer data on your customers in France to India, you could ask the French data privacy authorities for approval of the transfer. This could be time consuming, and it may require you to keep going back to those authorities for approval as facts or circumstances change. Alternatively, you could get each customer’s consent, which could be an onerous task.¹¹⁰

¹⁰⁶ Global Internet, *supra* note 92, at 3.

¹⁰⁷ Since 1995:

Only a few countries that are not members of the EU have been approved by the EU to receive this regulated data. They include Switzerland, and Canada. India, China, Malaysia, the Philippines, Russia, and many other offshoring destinations are not yet deemed to have adequate protection. You cannot send EU personal data to these countries unless you use one of the approved methods of transfer.

Carmel & Tjia, *supra* note 32, at 116.

¹⁰⁸ See Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00070047.pdf [hereinafter U.S.-EU Safe Harbor Agreement] (permitting transfers of EU data to a U.S. company that has self-certified with the U.S. Department of Commerce that the company is in compliance with the Safe Harbor data protection principles and thereby secured Safe Harbor status).

¹⁰⁹ See Jody Westby, *Going Global*, Info. Security, Feb. 2007, at 22 (reporting that Spain has “levied millions of dollars of fines against corporations (primarily in the health and telecommunications sectors) for failure to comply with particular provisions of the directive”); see also Carmel & Tjia, *supra* note 32, at 117 (reporting additionally that in the “UK, individuals and/or corporate bodies may be prosecuted and fined for violations”).

¹¹⁰ Carmel & Tjia, *supra* note 32, at 116-17.

Under the scheme established by the Directive, Carmel believes that the “most efficient way to handle [cross-border] data transfers is . . . through use of EU approved data transfer contract clauses,”¹¹¹ which subject the data transferor and transferee to enforcement by EU authorities.

4. EXISTING SOLUTIONS FOR GUARANTEEING CROSS-BORDER DATA PROTECTION

In the current global regulatory landscape, there are two ways to ensure adequately strong data protection on both ends of the outsourcing transaction: (1) by contract between the outsourcing firm and outsourcing provider; and (2) through bilateral agreements on data protection between the countries of the outsourcing firm and the outsourcing provider.

4.1. *Protecting Cross-Border Data Transfers Through Contract*

Currently, firms seeking to outsource are advised to get strong contractual assurances¹¹² from the outsourcing provider *vis-à-vis* data protection. The data protection provisions of the outsourcing contract¹¹³ should stipulate the company’s: “control over and access to the data; the use of appropriate data security measures; restrictions on data use, transfer, processing, and sharing; an agreement to make changes as required by changes in privacy laws; facility audit rights; and many other similar topics.”¹¹⁴ It is also imperative that the contract provide for an effective enforcement mechanism that holds the BPO provider fully liable for adhering to the contract. In a country with weak data protection laws or weak enforcement, it may be necessary for the contract to specify data protection procedures for the BPO provider. For example, the BPO provider may be required to adopt a process where all its employees must swipe ID cards to gain admission to the office, empty their pockets and bags of cell phones, PDAs, pens and

¹¹¹ *Id.* at 117.

¹¹² Strong contractual assurances are important to holding the outsourcing provider – one factor of production – accountable to the firm. As Coase writes in *The Nature of the Firm*:

The contract is one where by the factor, for a certain remuneration . . . agrees to obey the directions of an entrepreneur *within certain limits*. The essence of the contract is that it should only state the limits to the powers of the entrepreneur. Within these limits, he can therefore direct the other factors of production.

Coase, *supra* note 27, at 391.

¹¹³ An outsourcing contract is defined as an amalgam of “contractual rights and responsibilities, ownership structure, incentive systems, and information collecting processes, all intended to maximize the benefits received by the client.” Snir, *supra* note 41, at 28-29.

¹¹⁴ Carmel & Tjia, *supra* note 32, at 118.

notebooks into lockers at the point of entry under security, shred notes of conversations with customers at the close of their shifts and conduct their work generally under supervision.¹¹⁵ The contract may also contain an indemnity clause to ensure that the BPO provider carries part of the immediate financial risk in the event of a data breach.

Nonetheless, the contractual route in offshore outsourcing still suffers from a host of problems. In addition to the issues of jurisdiction the outsourcing firm will face if it seeks an injunction or damages for breach of contract against the BPO provider in the destination country, the cost of negotiation is significantly higher for stringent data protection clauses. The search costs will also likely be higher since the outsourcing firm must find a BPO provider willing to accept and adhere to stringent data protection clauses. If the majority of BPO providers perceive such clauses as burdensome rather than beneficial, they are also likely to charge premiums for assuming the burden or risk imposed by the stringent provisions.¹¹⁶ The resulting expensive search and negotiation costs may dissuade firms that are concerned about data protection from outsourcing altogether. Attaining strong data protection through outsourcing contracts thus comes with greater transaction costs.

4.2. Protecting Cross-Border Data Transfers through Bilateral Data Transfer Agreements

Another means of ensuring strong data protection on both ends of the offshore outsourcing agreement is through the use of bilateral cross-border data transfer agreements in a similar vein to the U.S.-EU Safe-Harbor Agreement.¹¹⁷ However, unless all such agreements are made with the European Union – that is, all bilateral cross-border data transfer agreements are EU Safe Harbor ones – this approach results in a convoluted web of bilateral treaties, rather than an adoption of uniform data protection practices. Firms wishing to outsource would have to lobby legislators to negotiate bilateral agreements between their home country and those of the outsourcing providers. If the perceived cost of lobbying is greater than the projected savings from outsourcing, then there is little incentive to engage in collective action to lobby. International negotiation

¹¹⁵ See Bertram, *supra* note 39, at 245 (describing the security measures undertaken by Golden Millennium in Bangalore, where “[a]t the reception desk, visitors sign a daunting four-page form promising not to divulge anything they see inside – and even then are only allowed to peer into the workspace through thick windows” (quoting Pete Engardio, *Fortress India?: Call centers and Credit-Card Processors Are Tightening Security to Ease U.S. and European Fears of Identity Theft*, Bus. Wk., Aug. 30, 2004, at 28)).

¹¹⁶ After all, “[e]conomic theory presupposes rational parties that strive to maximize their own welfare. [BPO providers] will not freely enter into agreements that are detrimental to their own interests.” E. Allan Farnsworth, *Contracts* 762 (3rd ed. 1999).

¹¹⁷ See generally U.S.-EU Safe Harbor Agreement, *supra* note 108.

and the legislative processes are inherently slow,¹¹⁸ which makes this a less expedient solution for data protection in the information age.

Further, both the contractual route and bilateral agreements fail to address concerns raised by multi-sourcing, a developing trend with information technology outsourcing that is likely to expand to BPO. With multi-sourcing, different components of business processes are partitioned amongst multiple service providers.¹¹⁹ Firms seeking to outsource business functions to multiple service providers, which may be based in different countries, have to consider the greater transaction costs of search and negotiation. Also, not every destination country under consideration will have a bilateral agreement with the origin country, so firms wishing to practice data integrity may be deterred from seeking what would otherwise be the most efficient service provider in a particular country.

4.3. An International Approach to Data Protection is Necessary

Contractual provisions and bilateral agreements are insufficient to ensure that information is adequately protected. Similarly, a back-end approach to data privacy, where individual national regulations impose fines on firms for poor data protection practices in their outsourcing activities, is at best a reactive solution.¹²⁰ A front-end model that regulates cross-border data transfers offers a *proactive* means of preempting the breach and misuse of transferred information, as well as providing enforcement and remedies mechanisms. Unlike the back-end model, it also reduces the search and enforcement costs of firms for reliable off-shore BPO providers. Effective world-wide data protection, replete with enforcement mechanisms (i.e., an international arbitration court) requires a “front-end model” solution to the problems posed by multi-sourcing and

¹¹⁸ See Aaron-Andrew P. Bruhl, *Using Statutes to Set Legislative Rules: Entrenchment, Separation of Powers, and the Rules of Proceedings Clause*, 19 J. L. & Pol. 345, 347 (2003) (commenting on the “increasingly sclerotic nature of the usual ‘slow track’ legislative process”).

¹¹⁹ See Robert Mitchell, *GM Drives Economies of Scale in IT*, Computerworld, Oct. 30, 2006, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=267929> (reporting that GM has disseminated its IT operations to a number of outsourcing providers around the world after its Brazilian e-commerce site crashed, and the company realized that the company could not defer service relationships to an external party).

¹²⁰ Even if we assume that the countries with market demand for BPO services are willing to enact comprehensive data protection regulations that would impose fines, or create causes of action for improper data transaction practices, the back-end model merely offers relief after the fact (of the breach or abuse). Nor does it address the difficulties of multiple jurisdictions in holding firms in the BPO destination countries accountable. Because a back-end model does not approach the adoption of a uniform standard of data protection, it does not correct the problems that arise when firms wish to engage in outsourcing to the most efficient BPO providers in countries with weaker data protection laws. The remedy to these problems demands a consistent international approach. In other words, the back-end model ignores the current global regulatory landscape, in which the EU Data Directive is the most prominent standard.

that also reduces transaction costs. Although the European Union has recognized the “need to establish common guidelines . . . [over data privacy rules and] not just renegotiate agreement by agreement,”¹²¹ it is unclear that an official world-wide data protection regulation will materialize under the current political climate.¹²²

5. THE EU DIRECTIVE SHOULD BE HELD AS THE *DE FACTO* GLOBAL DATA PROTECTION STANDARD

The EU Data Directive is rapidly emerging as *the* global standard. Non-member countries are vying to meet the Directive’s “adequacy” stipulation in order to transact in information arising from EU citizens. Even the United States, with its substantial economic and political clout, had to negotiate a bypass of the procedures attached to the “adequacy” requirement (a successful endeavor that resulted in the Safe Harbor agreement¹²³). This underscores the power of the Directive’s world-wide influence on data transfer practices of entities in countries and economies of all sizes. Yet the implications of formally rendering the Directive as the global standard simply because of its current influence warrant further consideration. Some may argue that officially making the Directive the global standard smacks of imperialism, imposes on cultural norms, and impinges on national sovereignty. A brief examination of the Directive’s external influence, and the balance between privacy regulation and globalization, in contrast with other EU regulation, indicates that such costs may not necessarily override the benefits of a harmonized regime driven by the European model.

¹²¹ *EU, U.S. in Talks Over Common Data Privacy Rules*, Reuters, Nov. 22, 2006.

¹²² Concerned about any potentially negative impact the regulation may have on international business transactions, economically powerful countries (such as the United States) have asserted their sovereignty rights in resisting this. The varying technological development in countries, as well as different cultural perceptions of “privacy” and entitlement to personal information are also factors; after all, how can an international regulation be implemented when there is no consensus on the definition of “privacy”? See George & Gaut, *supra* note 35, at 28 (explaining that “[t]he *very words* ‘international regulation’ and ‘data privacy’ themselves carry different connotative (i.e., emotional or personal) meanings for people from different countries in order to understand the reasons that cross-cultural differences exist in current regulatory models of privacy protection for the U.S., EU, and India”; this is primarily due to the “unique language and culture of the people (i.e., nation) with whom one may be negotiating”).

¹²³ Administered by the Department of Commerce and enforced by the Federal Trade Commission, the Safe Harbor agreement permits U.S. companies to self-certify their compliance to the seven Safe Harbor principles. Their self-certification of their compliance to the Safe Harbor principles is treated as akin to self-certification of their compliance to the EU Data Directive. Thus, the agreement is a bypass of the normal mechanism for satisfying the adequacy principle because the United States need not enact comprehensive data privacy legislation that provides “equivalent protection” to the Directive. See generally Westby, *supra* note 109, at 22 (noting that the Directive’s principles are largely incorporated into the Safe Harbor agreement).

5.1. The Directive is Already Becoming the Global Standard

The EU Data Directive is the closest approximation to a strong global data protection standard in operation.¹²⁴ Article 25 of the Data Directive, which mandates that data be transferred only to countries that provide an “adequate level” of data protection, has convinced Malaysia¹²⁵ and Canada¹²⁶ (as well as other countries that wish to reduce impediments to BPO outsourcing) to draft or implement personal data protection legislation reflecting the Directive.¹²⁷

The impetus for countries introducing domestic legislation modeled on the Directive might issue from unequal economic bargaining power. Market access, or “transactional interconnectivity,” and economies of scale, which exist because identical regulations reduce the cost of production, are factors that incentivize nations to harmonize their regulations.¹²⁸ In other words, countries seeking access to the e-commerce and outsourcing markets of the EU must “negotiate mutually acceptable harmonized regulations that would be a compromise in stringency.”¹²⁹ However, only countries with bargaining power comparable to the EU’s in the international trade arena are able to reach a compromise agreement; the United States is the lone player to successfully negotiate a Safe Harbor Agreement with the EU.¹³⁰

Excluding the United States, players in the international trade arena will tend to follow Canada’s example¹³¹ and adapt their data privacy laws to comply with the strictest

¹²⁴ See Westby, *supra* note 109, at 22 (“Since 1995, the EU has been the global leader on how governments and companies approach privacy.”).

¹²⁵ See Cordelia Lee, *Malaysia Angles for Outsourcing*, CNET Asia, Sept. 3, 2004, <http://news.zdnet.co.uk/itmanagement/0,1000000308,39165423,00.htm> (reporting that Malaysia ranked as the “third most-attractive destination for shared services and outsourcing” in a survey by American consulting firm A.T. Kearney).

¹²⁶ Canada is a popular destination country for “nearshore outsourcing” by American and British firms because of linguistic and cultural linkages, as well as proximity. See Carmel & Tjia, *supra* note 32, at 116, 216.

¹²⁷ See Privacy & Human Rights, *supra* note 57, at 491, (“[E]-commerce concerns and the desire to comply with the adequacy provisions of the [EU Data Directive], have led the Malaysian Ministry of Energy, Communications and Multimedia . . . to begin drafting a new personal data protection bill.”).

¹²⁸ David Lazer, *Regulatory Interdependence and International Governance*, 8 J. Eur. Pub. Pol’y 474, 477-78 (2001).

¹²⁹ *Id.* at 478.

¹³⁰ *Id.*

¹³¹ Legal Aspects of International Sourcing § 1:167 (Lillian V. Blageff et al. eds., 2007); see also Ryan Moshell, Comment, . . . *And Then There Was One: the Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 Tex. Tech L. Rev. 357, 372 (2005)

standard in the data protection system – that is, the EU Data Directive.¹³² Countries with lesser bargaining power will gravitate towards adhering to the strictest standard because “[t]he possibility of a loss (as in a less strict standard than the status quo) might result in greater political mobilization than the possibility of an equivalent gain.”¹³³ In other words, the cost of failing to actively participate in e-commerce and outsourcing with members of the European Union is more likely to drive firms to organize and lobby their legislators for a political solution that permits cross-border data transfer, than the benefits derived from maintaining the existing data protection regime. Professor Lazer describes this as a “political bias against reducing the strictness of standards”¹³⁴ and further reasons that countries will harmonize to the “strictest standards in the system . . . because it is cheaper to produce one version [of regulatory policy] (even if it is to stricter standards) than multiple versions.”¹³⁵ Simply put, it is most efficient and practical to craft general data privacy regulation compliant with the strictest standard; that way, the information transaction activities of firms are equally regulated whether they are outsourcing to BPO providers in Belize or Bucharest.

As countries seeking to capture a share of the BPO market in the European Union increasingly subscribe to the EU Data Directive’s framework,¹³⁶ it is unsurprising that absent “some sort of international convention to harmonize personal data privacy laws, the EU Privacy Directive appears to be the new standard.”¹³⁷

(“Regarding data-protection standards, international momentum has swung decidedly toward comprehensive data-protection frameworks modeled on the EU’s breakthrough effort.”).

¹³² See Legal Aspects of International Sourcing, *supra* note 131, at § 1:167 (“Other countries [than the United States] will not be able to negotiate with the EU on that level. While some countries might see this as a small issue at present, it could come back to haunt them as e-commerce grows.”).

¹³³ Lazer, *supra* note 128, at 478.

¹³⁴ *Id.*

¹³⁵ In the abstract, where the data privacy regulatory policy points of the EU and other country overlap, “there will necessarily be a convergence to the stricter state’s standards . . . [and] in the resulting political bargain, no state reduces the stringency of its regulations . . . but achieves harmonization with other states.” *Id.*

¹³⁶ It is worth noting that the number of member states of the European Union will expand from the current twenty-five, which increases the number of countries upon which the EU Data Directive will be directly binding. Bulgaria and Romania will accede to the Union in 2007, while Croatia, Turkey, and Macedonia are currently candidates for accession. European Commission, Candidate and Potential Candidate Countries, http://ec.europa.eu/enlargement/countries/index_en.htm (last visited Oct. 1, 2007) (discussing the EU’s enlargement policy). The significance of this is that the sheer volume of countries seeking to enact data protection regulation that adheres to the Directive can and does render it the de facto international data protection standard.

¹³⁷ Legal Aspects of International Sourcing, *supra* note 131, at § 1:167.

5.2. *The Efficacy of the EU Data Directive*

Although viewed as a model standard of data protection, the Directive is not immune to criticism regarding its efficacy. According to the EU Commission's 2003 report, which solicited comments from interested parties and questionnaires for data controllers and subjects as part of its investigation of why member states lagged in implementing their respective national data protection laws under the Directive, critics question whether the Directive has actually resulted in increased cross-border data flow.¹³⁸

These critics claim that the Directive has actually impeded cross-border data flows both amongst member states, and between member states and non-member states.¹³⁹ To support this contention, critics point to the divergent approaches of implementation by member states, influenced by member states' individual concerns about implementing regulation that conflicts with their own existing national laws.¹⁴⁰ Critics also argue that data privacy harmonization is "untenable" because "rapid developments in the related fields of information technology and modern business practice" mean that the current EU system cannot keep pace.¹⁴¹

However, these critics misconstrue the existence of the 2003 report as demonstrating that the Directive itself is conceptually flawed. While the 2003 report acknowledged "there was considerable scope for improvement in implementing the Directive," it also set forth a "Work Programme" to make the improvements happen.¹⁴² As reported in a 2007 follow-up to the initial report, the Commission and Working Party

¹³⁸ See Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive*, at 10-11, COM (2003) 265 final (May 15, 2003), available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

¹³⁹ See Andrew Charlesworth, *Enforcing Privacy Rights: Thinking About Optimal Enforcement: Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?*, 54 *Hastings L.J.* 931, 933-34 (2003) ("[F]ar from creating a harmonized area of law, the . . . Directive . . . resulted in the Member States creating a diverse patchwork of legal and administrative rules" which militated against the "goal of functional data privacy harmonization.").

¹⁴⁰ See *id.* at 936 (asserting that the divergences in implementation were partially due to laggard member states that failed to implement the Directive by 2002).

¹⁴¹ See *id.* at 932-33 (suggesting that because the Directive was drafted and made effective before "'e-commerce,' and 'portals' were common parlance [and] . . . the increasing popularity of free trade [also transformed] business practices . . . [in which] . . . 'remote processing'" or BPO outsourcing was embraced, the Directive's language and conceptualization of privacy became outdated and irreconcilable with practical business interests).

¹⁴² Commission of the European Communities, *Communication on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive*, at 3, COM (2007) 87 final (Mar. 7, 2007), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf.

have since monitored the status of member state implementation, studied the commercial and privacy dimensions of new technologies such as RFID, and issued guidelines and supplementary materials clarifying the public interest requirement and simplified the requirements for data transfer outside of the EU.¹⁴³

Further, given that a number of non-member states have successfully secured adequacy findings after 2003 for their data protection practices under the Directive, the Directive clearly has some merit, at least as a practical solution. Non-member states would be less likely to seek approval in accordance with an “untenable” standard.¹⁴⁴ The Commission’s dedication to monitor member state compliance with the Directive and its commitment to fine-tune the implementation and (if necessary) the substance of the Directive itself, also indicate that the Directive will evolve to meet the demands of new technology and business practices.

5.3. Sovereignty Considerations in Holding the EU Data Directive as the De Facto Global Standard

One salient argument against setting the EU Data Directive as the benchmark for sufficient cross-border data protection is that it constitutes “regulatory imperialism”¹⁴⁵ and treads on national sovereignty.¹⁴⁶ Regulatory imperialism is a particularly acute issue in the context of data transfers because information flow is “more likely to proceed from the agencies of developed countries to the agencies of developing countries, [which] creates a notable asymmetry and raises the question of external accountability of one

¹⁴³ *Id.* at 3-10 (summarizing the work undertaken in ten targeted “action areas” such as investigation efforts in data processing in the healthcare sector, issuing comparative studies on notice-of-data-processing procedures and recognizing additional contractual clauses as adequate safeguards for external-EU data transfer).

¹⁴⁴ *Id.* at 4 (naming Argentina, Guernsey, and the Isle of Man as non-member states with adequacy findings).

¹⁴⁵ See Jonathan R. Macey, *Regulatory Globalization as a Response to Regulatory Competition*, 52 Emory L.J. 1353, 1353-55 (2003) (explaining that regulatory imperialism occurs when “governmental actors or regulators can increase their power by persuading or forcing other countries to adopt regulations favored by the first country”); Anu Piilola, *Assessing Theories of Global Governance: A Case Study of International Antitrust Regulation*, 39 Stan. J. Int’l L. 207, 220-21 (2003) (“The notion of regulatory imperialism suggests that powerful parties like the European Union and United States have managed to institutionalize their joint preferences and incorporate their concerns within the international trading system by means of their relative power advantage.”).

¹⁴⁶ See generally Daniel W. Drezner, *On the Balance Between International Law and Democratic Sovereignty*, 2 Chi. J. Int’l L. 321, 321-23 (2001) (identifying the question for democratic governments as “how to balance serving the national will . . . with meeting international obligations that may be objectionable at points but are believed to advance the national interest in the long run”).

nation to another.”¹⁴⁷ By adhering to the Directive, countries are essentially signing onto Euro-centric conceptions of privacy and acknowledging a Euro-centric system as the global approach to data protection. Critics claim that adopting the Euro-centric system as the global standard overlooks the reality that cultural conceptions of data privacy are shaped by the diverse linguistic heritages and histories of people from different countries.¹⁴⁸ For instance, the “European legal regime’s *omnibus* (comprehensive) approach to data protection is rooted in their cultural belief that data privacy is a fundamental human right”¹⁴⁹ In contrast, U.S. culture places freedom of speech over individual privacy rights; the lack of a comprehensive federal data privacy law is a legacy of “Americans’ fundamental distrust of government intervention into the private sphere.”¹⁵⁰ India’s “reluctance” to adopt comprehensive data protection legislation stems from a combination of high population density, a history of overregulation of private entities, and few records of privacy abuses or identity theft.¹⁵¹

Although cultural differences must be respected in the creation of an international data privacy standard, “the term ‘regulatory imperialism’ overstates the negative aspects of international regulatory cooperation.”¹⁵² Instead, the decision to conform to international standards is an exercise of national sovereignty. Economically, there is

¹⁴⁷ Piilola, *supra* note 145, at 221.

¹⁴⁸ See Anita L. Allen, *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723, 728-29 (1999) (“‘Coercing privacy’ – imposing privacy norms to make sure everyone lives in accordance with a particular vision of privacy – would be problematic.”).

¹⁴⁹ George & Gaut, *supra* note 35, at 39. However, the OECD Privacy Framework, which is enshrined in and made binding on EU nations by the EU Data Directive, acknowledges that:

[I]t is probably not possible to identify a set of data which are universally regarded as being sensitive. . . . For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth.

OECD Privacy Guidelines, *supra* note 25. *But see* U.S. Civil Society Organizations, Comments Submitted to the Department of Commerce on the Development and Implementation of Cross-Border Privacy Rules in the Asia Pacific Economic Cooperation Group 2-3 (2006), http://www.worldprivacyforum.org/pdf/APEC_Privacy_CSO_Comments.pdf (pointing out that the OECD’s privacy principles are “sensitive and flexible to ‘cultural and other diversities that exist within’ [APEC] member economies” because North American, European, and Asian countries collaborated in the creation of the principles (brackets in original)).

¹⁵⁰ George & Gaut, *supra* note 35, at 41.

¹⁵¹ *Id.* at 42.

¹⁵² Piilola, *supra* note 145, at 221.

much to gain. Countries that bring their national data privacy laws into compliance with the EU Directive gain market access to information transactions with EU members, increased protection for the information of their own data subjects, and reduced transaction costs (a by-product of fewer barriers to trade since there is a single regulatory standard).¹⁵³

Countries that wish to avoid making tradeoffs between preserving cultural norms about privacy and capturing the economic gains from cross-border information transactions with EU members could resort to negotiating individual “safe harbor” approaches. However, even if these countries succeed in negotiating such agreements (and success will be difficult as these countries lack the bargaining of the United States) the potential economic gains will be lower. Search and information costs associated with uncertainty about compliance with multiple standards will still exist.¹⁵⁴ Hence, transaction costs will not be reduced to the extent they would be under a uniform regulatory regime.¹⁵⁵ Moreover, the traditions of different regulatory systems may present a credible commitment problem that will frustrate the implementation and enforcement of such agreements.¹⁵⁶

¹⁵³ Within the context of technical standards, one survey of businesses indicates that “[h]armonized European and International Standards result in businesses reducing their trading costs . . . [because] [n]ational standards can be used as non-tariff trade barriers against economic regions with different standards.” Beuth Verlag, *Economic Benefits of Standardization* 12 (2000), http://www.din.de/sixcms_upload/media/2896/Economic%20benefits%20of%20standardization.pdf. The reasoning behind and benefits of standards are not limited to the technical arena. See David Zaring, *Informal Procedure, Hard and Soft, in International Administration*, 5 Chi J. Int’l L. 547, 549-50 (2005) (“[R]egulatory cooperation in antitrust, food and drug regulation, telecommunications, aviation and other areas has resulted in an epidemic of standardization.” (footnotes omitted)); see, e.g., John Braithwaite & Peter Drahos, *Global Business Regulation* 520 (2000) (“Standard-setting bodies like ISO have taken . . . [the] principle [of continuous improvement in technical standards] to environmental standards.”). This means that the standardization of data privacy rules can likewise “lead to lower transaction costs in the economy as a whole, as well as to savings for individual businesses” because of reduced trade barriers and simplified contractual agreements. Verlag, *supra* at 12 (reporting that “62% of the businesses surveyed stated that European and International Standards simplified contractual agreements [and] 54% of the businesses surveyed stated that European and International Standards had lowered trade barriers in their sector”).

¹⁵⁴ Firms would have to navigate the complex web of several separately negotiated bilateral data transfer agreements, a situation discussed *supra* section 4.2.

¹⁵⁵ See Braithwaite & Drahos, *supra* note 153, at 520 (“Transaction cost analysis helps to explain the desire of TNCs [trans-national corporations] for one global standard rather than many different national ones.”).

¹⁵⁶ For example, if India were to enter into several separate bilateral data transfer agreements with countries with varying data protection laws and conceptualizations of privacy rights, it is unclear how India would be able to credibly commit to these agreements, given the country’s deep-seeded aversion to burdensome regulations tying up private companies and limited experience with identity theft. See George & Gaut, *supra* note 35, at 42 (explaining that India has

The difficult decision of weighing cultural considerations against economic ones is not unique to the data privacy context; such decisions also surface in the context of securities and antitrust regulation.¹⁵⁷ Indeed, the hard choice that countries face in making tradeoffs between economic gains and cultural sovereignty appears to be an inevitable by-product of technology and globalization.¹⁵⁸ Though there is a general consensus that some degree of cultural sensitivity should be exercised in crafting and implementing any globalized regulation,¹⁵⁹ questions of “how much sensitivity is necessary” and “how to achieve this” continue to be discussed.¹⁶⁰

Yet despite the concern about cultural sovereignty, the convergence of national laws to an international standard predicated on the EU regulatory model has already been demonstrated as practicable. In the antitrust arena, the EU regulations¹⁶¹ are a driving influence in the harmonization of competition laws of both member and non-member

no national identity numbers, no social security numbers, few drivers licenses and few bank account PIN numbers).

¹⁵⁷ See, e.g., Macey, *supra* note 145, at 1367-68 (describing how the “SEC . . . succeeded in . . . export[ing] U.S. insider trading laws to Switzerland” even though Swiss laws and customs did not regard insider trading as a crime and strictly protected the secrecy of bank account holders); Hannah L. Buxbaum, *German Legal Culture & the Globalization of Competition Law: A Historical Perspective on the Expansion of Private Antitrust Enforcement*, 23 Berkeley J. Int’l L. 474, 475 (2005) (describing Germany’s strong protests against the “potential undermining of its local competition enforcement philosophy” when faced with a “new European Council Regulation modernizing competition law enforcement” and the expansion of the jurisdiction of US courts over “extraterritorial anticompetitive conduct”).

¹⁵⁸ See Macey, *supra* note 145, at 1357 (“[R]egulators do not respond to globalization passively. And, consistent with this theory, there has been an explosion in the quantity and scope of regulatory globalization in those areas that have experienced the most private-sector globalization. For example as capital markets and currency markets have become more globalized, the ability of regulators in a particular country to regulate domestic firms has declined significantly.”). But see Paul Schiff Berman, *From International Law to Law & Globalization*, 43 Colum. J. Transnat’l L. 485, 553-55 (2005) (explaining that “while hegemonic power is always present, law and globalization can also be counter-hegemonic, at least at times” since “norms cross borders in both directions”).

¹⁵⁹ See Buxbaum, *supra* note 157, at 494 (suggesting that a “truly global competition law regime” may be attained by identifying shared core policies, which reflect congruent historical and cultural conditions, and “building a harmonized system outward from that base”).

¹⁶⁰ Although this subject is beyond the scope of this paper, there is extensive literature addressing it. See generally Jagdish Bhagwati, *In Defense of Globalization* (2004); Ralph E. Gomory & William J. Baumol, *Global Trade and Conflicting National Interests* (2000); Joseph Stiglitz, *Globalization and Its Discontents* (2002).

¹⁶¹ Treaty Establishing the European Community art. 82, Dec. 24, 2002, 2002 O.J. (C 325) 65.

states.¹⁶² That harmonization movement encountered the same objections about regulatory imperialism intruding on national sovereignty.¹⁶³ In the antitrust context, EU politicians assert that “the goal [of harmonization] is to encourage countries to implement [their own] rules and enforce them on a domestic level”¹⁶⁴ with the EU judging whether such rules and enforcement comply with its standard. Thus, the EU assumes the role of an evaluator as to compliance with “agreed upon rules, principles, and commitments”¹⁶⁵ while countries still maintain their sovereign powers. The result is an “international framework through which each member’s rules can be applied[,]” as opposed to a substitution of domestic rules with international ones.¹⁶⁶

Although the EU’s role as “evaluator for compliance” indicates that the competition regulatory system is ultimately Euro-centric, Professors John Braithwaite and Peter Drahos argue that the system stems more from “globalization modeling” than from economic coercion.¹⁶⁷ Modeling, defined as “observational learning with a symbolic content, [and] not just the simple response mimicry implied by the term ‘imitation,’”¹⁶⁸ occurs when:

[N]ations have been persuaded to set up competition law authorities through a belief that this is something economies do when they want to become more efficient, internationally competitive and give better value to their consumers. Typically, they then look at the competition laws of other countries, modeling some elements of one country’s law, other elements of a different nation’s statutes.¹⁶⁹

¹⁶² See Sharon E. Foster, *While America Slept: the Harmonization of Competition Laws Based Upon the European Union Model*, 15 Emory Int’l L. Rev. 467, 467 (2001) (“The European Union (E.U.) has harmonized competition laws and is influencing other states to adopt competition laws based upon the E.U. model.”).

¹⁶³ See *id.* (The United States was particularly vocal in its resistance to the EU model, asserting that “we live in a system of nation states, [and] not a global state devoid of national sovereignty concerns”).

¹⁶⁴ *Id.* at 495.

¹⁶⁵ *Id.* at 496.

¹⁶⁶ *Id.*

¹⁶⁷ Braithwaite & Drahos, *supra* note 153, at 215 (“Economic coercion is the most important mechanism of trade policy globalization, but in regard to competition policy globalization modelling has been more important.”).

¹⁶⁸ *Id.* at 580 (citing Albert Bandura, *Social Foundations of Thought & Action: A Social Cognitive Theory* 47-49 (1986)).

¹⁶⁹ *Id.* at 216.

For example, after the World Bank persuaded Czech regulators that a competition regulatory system was necessary for privatization, the regulators, collaborating with US consultants, adopted the substance of German competition law. As a result, the Czech Republic's "new competition authority . . . [forged] close contacts with the OECD."¹⁷⁰ Thus, the modeling mechanism often leads to the crafting and implementing of competition regulatory systems with multi-national (and therefore multi-cultural) elements.

By analogy,¹⁷¹ the EU could also act as an evaluator for compliance in an international data privacy system modeled on the Directive. Given that some countries have already implemented personal data protection legislation that reflects the Directive¹⁷² as well as aspects of non-EU privacy rules,¹⁷³ the globalization modeling mechanism appears to also drive the development of a global data privacy scheme. This suggests that the convergence towards an international data privacy system does not occur in isolation of non-EU cultural influences. Rather, the resulting system has a "genetic fingerprint" including various legal and cultural elements. With a substantial number of countries enacting data protection regulations that *model* the principles of the EU Data Directive, it is both practical and efficient to make the Directive the *de facto* global benchmark for cross-border data transfer rules.

¹⁷⁰ *Id.*

¹⁷¹ It makes sense to analogize the EU antitrust regulations to the EU data privacy regulations. The antitrust provisions in the European Community Treaty operate in a similar fashion to the "adequacy" provision of the EU Data Directive, in terms of their extra-territorial application in situations where the EU will be affected (economically or socially). Just as the Directive protects personal information arising from data subjects in the EU, EU antitrust regulations grant the European Commission power to apply Article 81 of the Treaty of Rome to any anti-competitive conduct that causes an effect in the EU, even if the conduct actually occurred outside the EU. *See, e.g.,* Case 89/85, *A. Ahlstrom Osakeyhtio v. Comm'n*, 1988 E.C.R. 5193, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61985J0089:EN:HTML> (finding that pricing agreements amongst wood pulp producers outside the EU impacts the EU because the pulp could be resold within the Union); Commission Decision IV/M.920, *Samsung/AST*, 1999 O.J. (L 225) 12, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_225/l_22519990826en00120019.pdf (finding that Samsung's acquisition of California-based AST Research Inc. would have an impact on the EU market, i.e., constitute a concentration with a Community dimension under the Merger Regulation, although neither company is based in the EU).

¹⁷² *See generally* discussion *supra* section 5.1.

¹⁷³ Canada's privacy laws, for instance, have been "largely influenced by two radically different approaches within the [International Data Privacy] regime - the strict, protectionist EU approach, and the targeted, sectoral U.S. approach." Jennifer McClennan & Vadim Schick, "O, Privacy" *Canada's Importance in the Development of the International Data Privacy Regime*, 38 *Geo. J. Int'l L.* 669, 671 (2007).

6. AUDITED SELF-REGULATION OF THE TRUSTMARK INDUSTRY THROUGH AN AGENCY
ADMINISTERED BY THE EU AS A SOLUTION TO UNIFORM CROSS-BORDER DATA PROTECTION

This Article proposes that audited self-regulation¹⁷⁴ (also known as co-regulation) over the existing trustmark industry will be a viable means of implementing a strong data protection standard around the world with minimal interference in the market and with existing legislation. By regulating the trustmark industry, this approach recognizes the potential value of privacy seals “as a powerful facilitator of [the] globalization of consumer transactions if indeed they are able to provide acceptable and enforceable privacy protection across jurisdictions.”¹⁷⁵ Similar to the way certification marks identify goods or services meeting specified qualifications,¹⁷⁶ trustmarks identify firms that meet specified data protection standards – that is, trustmarks are a simple (and often) visual¹⁷⁷ way of putting potential and existing consumers on-notice as to a firm’s data privacy integrity.¹⁷⁸ The key advantage to regulating trustmarks under the proposed scheme is that consumers need only familiarize themselves with one clear standard of data protection (the one linked to the trustmark), thereby lowering the costs for firms with tarnished privacy reputations and new smaller firms of (re)establishing their data privacy credibility.¹⁷⁹

¹⁷⁴ See Michael, *supra* note 22, at 176-77 (“‘Audited self-regulation’ is . . . the delegation by Congress or a federal agency to a nongovernmental entity the power to implement laws or agency regulations, with powers of review and independent action retained by a federal agency.”).

¹⁷⁵ Holcombe, *supra* note 44, at 569 (quoting a report by Privacy Commissioners in Australia and Ontario, Ann Cavoukian, Office of the Info. & Privacy Comm’r Ontario, & Malcolm Compton, Office of the Fed. Privacy Comm’r of Austl., Web Seals: A Review of Online Privacy Programs § 5.2 (2000), available at <http://www.privacy.gov.au/publications/seals.html>).

¹⁷⁶ See Trademark and Unfair Competition Law: Cases and Materials 57 (Jane C. Ginsburg et al. eds., 4th ed. 2001) (naming as examples, geographic certification marks like “ROQUEFORT” for cheese from Roquefort, France and “UL” from Underwriter’s Laboratory for goods that meet safety standards).

¹⁷⁷ Much like stamping food products with a “kosher mark”, firms can display a graphical seal on their promotional materials and website.

¹⁷⁸ Cf. Holcombe, *supra* note 44, at 570 (“Labeling principles are closely tied to those of trade marks: to be non deceiving, informative and to allow for the identification of the producer of a product” (quoting Jorge Larson Guerra, Labels that Tell Stories: Building Bridges Between Producers and Consumers 1 (June 2003), available at http://www.wto.org/english/tratop_e/dda_e/symp03_larson_e.pdf)).

¹⁷⁹ New and smaller firms likely face greater costs in convincing consumers of their data privacy practices since, unlike large established organizations, they often do not have sophisticated marketing and customer relations departments through which the assurances can be channeled. However, even big established firms that suffer a data privacy breach face a considerable expense in fixing “brand impairment” and undertaking customer assurance

Audited self-regulation of the trustmark industry can most effectively coordinate and induce the commercial adoption of the EU Data Directive's principles, without impinging on national sovereignty, for the following reasons: (1) self-regulation is more easily accepted by the regulatory entities, which translates into better compliance with rules; (2) as a result of the trustmark providers' superior knowledge of data transactions in the outsourcing business, self-regulation permits more diversity (and flexibility) with respect to the methods of compliance with legal rules;¹⁸⁰ and (3) self-regulation may be characterized as a "retreat from bureaucratic 'command and control' methods of regulation"¹⁸¹ which are more likely to constitute regulatory imperialism in the international context.

With expertise in the field concentrated in the trustmark industry and the agency overseeing it, audited self-regulation functions by engaging the trustmark providers' incentives for compliance.¹⁸² The basic structure of this regulatory apparatus consists of two tiers of regulation. The first tier is comprised of trustmark providers, which monitor firms engaging in cross-border data transfers for compliance to the Directive, while the second tier consists of the agency regulating those trustmark providers. Thus, the parties to offshore BPO contracts will be audited by trustmark providers, which in turn will be audited by the agency. In other words, trustmark providers will self-report to an agency charged with oversight over the world-wide trustmark industry, and the aforementioned agency will operate under the administration of the European Union.

6.1. Process of Audited Self-regulation of the Trustmark Industry

The agency will issue a license that grants authority to trustmark providers to issue certificates of compliance as to the firms' outsourcing practices with the EU Data Directive. Trustmark providers will require both firms and their BPO service providers to submit (1) a privacy impact assessment by the firms' Chief Information Officer,¹⁸³ or equivalent, of their current and projected cross-border data protection practices and (2)

measures. *See, e.g.*, Sharon Gaudin, *T.J. Maxx Breach Costs Hit \$17 Million*, InformationWeek, May 17, 2007, <http://www.informationweek.com/security/showArticle.jhtml?articleID=199601551> (describing breach-related costs of fines, legal fees, notification expenses, security upgrades, investigation and containment expenses and exposure to payment card companies and banks).

¹⁸⁰ *See* Michael, *supra* note 22, at 181.

¹⁸¹ *Id.* (identifying an additional two distinct advantages of audited self-regulation over other regulatory techniques that are more relevant to the federal context).

¹⁸² *See id.* at 183 (explaining that there are stronger incentives to comply because the rules are more tailored to the outsourcing business and thereby perceived as more "reasonable" from the outset and thereby less costly to adhere to).

¹⁸³ The Chief Information Officer would fulfill the role of the personal data controller specified in the EU Data Directive.

their proposed and final outsourcing contracts for evaluation as to whether the cross-border data protection provisions are adequate and will comply with the EU Data Directive.

The trustmark providers will follow agency stipulated guidelines or procedures to assess whether the proposed and current data practices and outsourcing contractual provisions are adequate and comply with the EU Data Directive. Firms deemed to comply will receive a trustmark, or a certificate of compliance with a date stamp¹⁸⁴ that they may publicize in their promotional materials. However, approval of the use of the trustmark is contingent on the firm maintaining adequate data protection practices. Trustmark providers will monitor firms by requiring them to submit privacy impact assessments on a regular basis (at least every 45 days), or else the trustmark will “expire.” Firms also must submit privacy impact assessments to the trustmark providers at least 30 days before modifying or terminating any existing approved data protection practices or outsourcing contractual provisions. If the firm is amending a provision in the outsourcing contract, it must also submit the proposed changes to the trustmark provider for re-evaluation of compliance. A firm’s failure to submit to this regular monitoring and self-reporting will result in an “expiration” or suspension of the trustmark. Should a firm use an expired trustmark in a manner misleading to consumers, the trustmark provider should revoke the certification completely and impose punitive fines on the firm. The agency should also create a central database containing all the evaluations of firms’ cross-border data protection practices issued by the trustmark providers, and updates as to the status of the firms’ trustmarks.

To ensure that this firm process-oriented system functions properly, the agency will require trustmark providers to randomly audit, on a regular basis, firms that have procured trustmarks, and to take timely punitive action for lack of compliance.¹⁸⁵ These audits will be submitted to the agency for its records. If the agency determines that a trustmark provider is not performing satisfactorily (i.e., by improperly issuing a certificate, failing to properly monitor compliance, complete audits or impose punitive measures on firms that don’t comply), the agency may revoke the trustmark provider’s right to issue accreditation for compliance with the EU Data Directive.

Of course, since the agency only directly regulates trustmark providers and not the firms themselves, trustmark providers can only “require” action by firms insofar as the firms elect to participate. Firms that were not initially persuaded by the benefits of acquiring a certification of compliance can be incentivized to register and participate through the agency’s coordination of public relations efforts with the trustmark providers. For instance, the agency can maintain a website where individuals can check the

¹⁸⁴ A useful analogy is the “best before date” stamped on food products.

¹⁸⁵ These audits will be similar to the financial ones conducted by accountants to assess whether financial statements of publicly registered companies and charities accord with the International Financial Reporting Standards or the Generally Accepted Accounting Principles. *See generally* Fed. Accounting Standards Advisory Bd., *Statements of Federal Financial Accounting Concepts and Standards (2007)*, available at http://www.fasab.gov/pdffiles/codification_report2007.pdf; Int’l Accounting Standards Bd., *International Financial Reporting Standards (2006)*.

certification status of a firm and read the trustmark providers' evaluations of the firms,¹⁸⁶ as well as alert individuals about firms with expired or revoked certificates of compliance in press releases and monthly newsletters. The agency may also maintain a blacklist of non-participant firms and outsourcing service providers with poor data protection practices or major breaches and thus generate bad publicity that warns off existing and potential customers. Further, the agency can maintain profiles and assign rankings for good data integrity to BPO service providers. As a result, both public and private firms seeking to outsource can browse the accreditation history of the BPO service providers in the profiles and rankings, which can inform their choice of service provider (and thereby reduce search costs). By permeating the public consciousness with the accreditation model as an assurance of data integrity and protection, firms will seek to participate in co-regulation with the trustmark providers.

6.2. Administrative and Cost Considerations of an Audited Self-regulated Trustmark Industry

This form of audited self-regulation is not without drawbacks. Trustmark providers will bear significant costs in complying with agency regulations. Collecting registration and auditing fees from firms is unlikely to be profitable in its early stages. Until the public trusts and relies on this accreditation process, trustmark providers will be reluctant to charge higher fees as they seek to attract firms and BPO providers. It is not clear how the EU would administer the agency, although it is likely that the European Commission, already charged with assessing the adequacy of the data privacy laws of outside countries, would play a role. Moreover, the existence of bilateral agreements such as the U.S.-EU Safe Harbor Agreement means that there may be overlap in obtaining certified data protection compliance for certain firms and BPO service providers. It may well be that, in order to run smoothly, this system needs an international regulation that requires all firms wishing to outsource and transfer data abroad to obtain trustmarks before doing so.

However, audited self-regulation of the trustmark industry with oversight provided by an agency under the European Union's administration is likely the best way to ensure a strong level of protection for personal information transferred across borders. Setting an instrument of the European Union as the international standard for data protection is not a novel solution. As discussed earlier, the European Union's governance of outsourcing information practices is no different from its governance of anti-competitive practices, due to the manner in which the EU Data Directive applies to firms wishing to enter the European Union BPO market and transact in the personal information of European Union member state subjects.

Setting up this two-tier form of data protection regulation does not impinge on the legislative affairs of sovereign nations or the free market. Nor does it necessarily create a regulatory regime with a purely European make-up. By holding the EU Data Directive provisions as the bar for data protection, the agency will meet the need for a regulatory

¹⁸⁶ The agency can require the trustmark providers to enter status information and their evaluations of registered or participating firms in a central database.

apparatus that reduces the transaction costs incurred by outsourcing firms¹⁸⁷ as they search for and negotiate with suitable BPO providers. Further, this form of audited self-regulation preserves the flexibility of both outsourcing contract details and the new market for private trustmark certification companies. This approach also enhances the credibility of the trustmark organizations themselves since they will all be required to measure and regularly monitor the conduct of the outsourcing firms and BPO providers against a single stringent data protection standard.¹⁸⁸ Otherwise, they risk losing the authority to issue the trustmarks or compliance certificates. This eliminates the problems of variable standards for measuring compliance and inconsistent policing that plague the existing trustmark industry.¹⁸⁹

7. CONCLUSION

Data flows in offshore outsourcing transactions currently operate under a complex web of private contract, in-house or industry codes of conduct monitored by trustmark companies, sectoral and comprehensive national laws, and international organizational governance. The EU Data Directive, with its enforcement mechanisms reaching both Member States and outside countries, is increasingly emerging as the preferred transnational standard for data protection. However, it can take years for bilateral negotiations between the European Commission and outside countries seeking to obtain “adequacy” findings under the Directive (for their data protection laws) to be successfully realized in national laws. Setting up an agency under the administration of the European Union that oversees trustmark providers and holds the EU Data Directive as the standard for compliance is a practical and efficient solution. This form of audited self-regulation gives credibility to the trustmark industry by holding the trustmark providers accountable to a strong data protection standard and thereby increases consumer confidence.

¹⁸⁷ There are no transaction costs for individuals in overseeing the use of their data because consumers do not enforce the EU Data Directive (data protection regulation). Under this model, firms will presumably consider and come to value a trustmark as an asset essential for business, similar to accurate financial statements subject to public scrutiny. That way, the costs of purchasing the services of a trustmark provider will not be passed on to consumers.

¹⁸⁸ According to Professor Braithwaite and Professor Drahos, “[a]ccreditation and certification bodies monitoring for continuous improvement are one way in which a feedback loop between a principle of innovation and a minimum standard can be created . . . [which] ensures that the institutionalized standard continues being raised or lowered.” Braithwaite & Drahos, *supra* note 153, at 520.

¹⁸⁹ See Paul Boutin, *Just How Trusty is Truste?*, Wired News, Apr. 9, 2002, <http://www.wired.com/techbiz/media/news/2002/04/51624> (concluding that the TRUSTe web seal was rendered meaningless, if not misleading, after news broke out about how Yahoo! and Real Networks were permitted to continue displaying the seal even after making sweeping changes to their policies on personal information collection, storage and use, and as Seth Ross, chief strategy officer of PC Guardian explains, “a meaningless logo may induce people to make information disclosures they would otherwise avoid”).

Moreover, it accomplishes this through the use of incentives that encourage BPO providers and firms seeking to outsource to register for accreditation, thereby submitting their data transfer practices and contracts to scrutiny.

APPENDIX A: DATA PROTECTION LEGISLATION IN THE UNITED STATES RELEVANT TO OFFSHORE OUTSOURCING

The Health Insurance Portability and Accountability Act (“HIPAA”)¹⁹⁰ contains a Privacy Rule,¹⁹¹ which covers personal health information and requires disclosures only to the individual and the “Secretary of Health and Human Services for the purpose of enforcement.”¹⁹² The HIPAA Privacy Rule requires covered entities – hospitals, nursing facilities, outpatient rehabilitation facilities – to appoint a Privacy Officer and person in charge of responding to complaints, notify individuals of uses of their personal health information, track disclosures, and document privacy policies and procedures.¹⁹³ The Privacy Rule sports civil penalties for noncompliance, and criminal penalties for malicious misappropriation and misuse of health information, which are enforced by the Department of Health and Human Services’ Office for Civil Rights and the Department of Justice respectively.¹⁹⁴ The Privacy Rule does not preempt state laws providing stronger protection for health and medical information.

The Financial Services Modernization Act¹⁹⁵ (also known as The Gramm-Leach-Bliley Act, or “GLBA”) governs personal financial information through its Financial Privacy and Safeguards rules by requiring financial institutions to: 1) provide each consumer with a privacy notice disclosing the collection, security and use of personal information; and opt-out options at the beginning of the relationship, whenever the privacy policy is modified, and annually; 2) develop an information safeguards policy that includes risk management assessment *vis-à-vis* private client information; and 3) undertake protections against pretexting.¹⁹⁶ The GLBA prohibits financial institutions

¹⁹⁰ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

¹⁹¹ Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164 (2006).

¹⁹² Privacy & Human Rights, *supra* note 57, at 738.

¹⁹³ *See id.* at 1068.

¹⁹⁴ Privacy & Human Rights, *supra* note 57, at 739.

¹⁹⁵ Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

¹⁹⁶ Fed. Trade Comm’n, Privacy Initiatives: Financial Privacy, <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> (last visited Nov. 6, 2007) (summarizing the Gramm-Leach-Bliley Act).

from sharing nonpublic information, such as account numbers and access codes of any consumer to “any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.”¹⁹⁷ However, the GLBA does not require financial institutions to refrain from selling, leasing or otherwise disclosing information to non-affiliates so long as they believe the information is “lawfully made available to the general public.”¹⁹⁸ The GLBA does not grant to consumers, a private right of action if a financial institution violates the Act. Instead, consumers may file complaints to the following seven federal agencies charged with jurisdiction and enforcement authority over the financial institutions: the Federal Deposit Insurance Corporation, the Federal Reserve, the Office of Thrift Supervision, the Office of Comptroller of the Currency, the National Credit Union Administration, the Securities and Exchange Commission and the Federal Trade Commission.¹⁹⁹ The enforcing agency will then investigate the complaint, and may impose fines and injunctive relief through the administrative law system or court action.²⁰⁰

Under the Fair Credit Reporting Act (“FCRA”)²⁰¹ as it stands today,²⁰² private sector credit reporting agencies must follow the Act’s guidelines for information that can be gathered and ensure consumer access to their information. Moreover, private action may be brought “for any violation of the act, regardless of damages.”²⁰³

Some states have also enacted data privacy protection laws of general applicability (within the state). California, for instance, introduced a Mandatory Disclosure Law in 2003, which requires an organization to inform its California resident customers if their “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”²⁰⁴

¹⁹⁷ 15 U.S.C. § 6802(d) (2006).

¹⁹⁸ Privacy Sourcebook, *supra* note 55, at 286.

¹⁹⁹ *Id.*

²⁰⁰ *Id.*

²⁰¹ Fair Credit Reporting Act, Pub. L. No. 90-321, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681).

²⁰² In 1996, Congress enacted the Consumer Credit Reporting Reform Act which amended the FCRA. Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, 119 Stat. 3009-426 (codified at 15 U.S.C. § 1681s-2). The FCRA was further amended by the Fair and Accurate Credit Transactions Act in 2003. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-59, 117 Stat. 1952 (codified at 15 U.S.C. § 1681 and 20 U.S.C. § 9701-9708). The amendments imposed “new obligations on businesses to ensure the accuracy of reports, and increase[d] civil and criminal penalties . . . [and] establish[ed] remedial rights for identity theft[s] . . . [such as introducing] new document destruction procedures for personal information.” Privacy Sourcebook, *supra* note 55, at 1.

²⁰³ *Id.*

²⁰⁴ Cal. Civ. Code § 1798.82 (West 2006).

APPENDIX B: APEC PRIVACY PRINCIPLES

The nine principles consist of:

- I) 'Preventing Harm' – harm ensuing from wrongful collection or misuse of personal information may necessitate remedies for privacy infringements that are proportionate to the likelihood and severity of the harm threatened;²⁰⁵
- II) 'Notice' – personal information controllers should give notice before or at the time of data collection on the scope, purposes, types of persons to whom the information may be disclosed, any controls individuals have to access, correct and limit the use of their information, as well as the controller's contact information;²⁰⁶
- III) 'Collection Limitation' – only information relevant to the purposes of collection should be collected and the information should be procured in a lawful and fair manner, and where appropriate, with notice or consent of the individual concerned;²⁰⁷
- IV) 'Uses of Personal Information' – unless the consent of the individual data subject is procured or as required by law, information collected should be used only to fulfill the purposes for which it was collected and compatible or related purposes;²⁰⁸
- V) 'Choice' – individuals should be provided, where appropriate, with "clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure";²⁰⁹
- VI) 'Integrity of Personal Information' – the personal information controller has an obligation to maintain accurate, updated and complete records to "the extent necessary for the purposes of use";²¹⁰
- VII) 'Security Safeguards' – personal information controllers should implement "appropriate safeguards" proportional to the likelihood and severity of harm threatened by risks including loss of or unauthorized access, destruction, use modification or disclosure of information;²¹¹
- VIII) 'Access and Correction' – individuals should be able to obtain confirmation as whether their information has been collected, and have the ability to challenge

²⁰⁵ APEC Privacy Principles, *supra* note 83, at 11.

²⁰⁶ *Id.* at 12-14.

²⁰⁷ *Id.* at 15-16.

²⁰⁸ *Id.* at 16-17.

²⁰⁹ *Id.* at 17-20.

²¹⁰ *Id.* at 20-21.

²¹¹ *Id.* at 21.

the accuracy of the records, which may include, “as appropriate” rectifying, completing, amending or deleting and;²¹²

- IX) ‘Accountability’ – the personal information controller should be held accountable for complying with the Principles, as well as for exercising due diligence where the personal information will be transferred to another recipient person organization.²¹³

²¹² *Id.* at 22-28.

²¹³ *Id.* at 28-29.