Towards Understanding the Factors and Their Effect on Offshored Data Privacy

Anupam Kumar Nath

Offshoring of services has become an integral part of business strategy. While businesses are deploying service offshoring for quite some time now, preserving the privacy of the sensitive information of offshored data remains as one of the major challenges and concerns. In this paper, we identify factors that affect the privacy-preservation of the offshored data and the conduct of the offshore vendors and their employees towards clients' data. We deploy a positivist case study method to examine the proposed relationships. We collected qualitative data through semi-structured interviews with the project managers of client organizations as well as from the project managers of vendor organizations to test our proposed model. The result shows that the code of conduct set by the vendor organizations plays the most effective role in the privacy-preserving behavior of the vendors' employees.

Keywords: Offshoring, data privacy, positivist case study.

Reference to this paper should be made as follows: Nath, A. K. (2018). Towards understanding the factors and their effect on offshored data privacy. *Journal of Business and Management*, 24(2), September, 1-18. DOI: 10.6347/JBM.201809_24(2).0001.

Introduction

Information Technology (IT) service offshoring has emerged as a viable strategic option for many Western firms. However, these firms looking to offshore their services face several risks (Polak & Wójcik, 2015). One of the most prominent risks of IT offshore outsourcing is that it often involves transferring various sensitive and propriety data overseas and authorizing service providers located in different

countries to access and use that data (Palvia & Jain, 2017). There have been several allegations that employees based in foreign countries have stolen data outsourced to the service providers (Polak & Przemyslaw, 2015)) . Due to difficulties related to enforcing privacy laws in foreign countries' courts, privacy has been a major concern in offshore outsourcing decisions. Offshore outsourcing might cause political, reputation, and even financial risks because of the misuse of the offshored data (Overby, 2010). For example, recently a US-based organization's breach took place through the employee(s) of its outsourcing partner in an offshore law firm (Zelijka, 2017). Such incidents refer to the underlying importance of offshore vendors' employees' role in the privacy preservation of the offshored data. Hence, in this paper, we essentially identify the factors that affect the conduct of the employees who handle the offshored data.

Preserving the privacy of data is a major challenge for the offshoring practice. However, in the extant literature, we found diminutive instances of comprehensive empirical investigation of the factors that affect privacy preservation of behavior of the vendors' employees and overall privacy preservation, especially from both client and vendor's perspective in the same study. We address this gap in the literature through the following research question that guides our research: *What are the factors that affect the privacy-preservation of the offshored client data?*

In this research, based on the existing literature we develop a model by identifying the potential variables that affect privacy preservation of the offshored data. Then we adopt a qualitative positivist case study to confirm the relationship between different identified factors and the privacy preservation of the offshored data. We adopt the guidelines suggested by Dubé & Paré (2003) and Shanks (2002) in conducting the positivist case study.

The findings of the research will help to understand the relative effectiveness of different factors which affect the privacy preservation of the offshored data. We believe that with our findings client company t would be able to identify the important factors in privacy preservation behavior of the offshore vendors and their employees. Consequently, this can help them to make the necessary adjustments in offshore arrangements. An important and unique aspect of our research is that we study the effects of different factors from both clients' and vendors' perspective. Having both perspectives give us an opportunity to attain a holistic picture of privacy preservation in offshoring arrangements.

Theoretical Development and Hypothesis

Offshoring is a type of outsourcing (Swartz, 2004). Offshoring simply means having the outsourced business functions done in another country. In the extant literature, authors used different theoretical lenses to describe the offshoring

phenomenon and different aspects of it. Among them, Institutional Theory is one of the most frequently used theoretical lenses (Tate, Ellram, & Bals, 2009). Institutional theory concerns the study of organizational isomorphism, i.e., the process by which certain processes or routines are adopted by all organizations and therefore gradually attain legitimacy in that field. Unlike decision-making models that focus mainly on economic motivations, institutional theory hypothesizes that organizations might adopt certain practices for legitimacy even in the absence of any economic benefit (DiMaggio & Powell, 1983; Meyer & Rowan, 1977). This premise is important for our study as it helps us to find out the factors outside the economic factors that influence the behavior of the offshore vendors and their employees.

With the widespread illegal use of intellectual property, violation of privacy, and breaches in security, ethical issues are particularly important in IT today. Interestingly, according to the 2003 CSI/FBI Computer Crime and Security Survey report, employees ranked just below independent hackers and above competitors as likely sources of attack. A recent FBI Cyber Security Report also reiterates the employee as a potential threat to data security (Audit of FBI's, 2016). Moreover, in the current state of IT offshoring, in many IT projects people from different parts of the world who belong to different cultural dimensions are participating. A client company in most cases does not have direct control over the privacy preservation behavior of such workforce (Nath & Bejou, 2012; Overby, 2010). Consequently, how these employees themselves make their ethical judgment regarding issues like Intellectual Property Law or privacy preservation, and their consequent behavior is very important factors in preserving the privacy of the data (Culnan & Williams, 2009; Moores & Chang, 2006). Hence, the way we develop our hypothesis includes employee behavior towards client data as part of the hypothesis.

Code of Conduct and Other Requirements Set By the Client

In an outsourcing arrangement, regulatory controls such as legal documents, policies, formal systems, standards, and procedures establish the relationship between the client and the vendor as well as specify boundaries (Bender, 2007; Das & Teng 2001). One of the most important components of any outsourcing deal is the contract which describes the services that a vendor is to provide, discusses financial and legal issues, and essentially becomes the blueprint for the lifespan of an outsourcing arrangement (Tafti, 2005). One of the major steps that might affect the privacy preservation of the offshored data is the code of conduct set by the client on the vendors, mostly through these contracts. (Internet Business Law Service). The contracts with the vendors should and can include requirements mentioning that the offshore vendor adheres to policies and standards for protecting data to which the outsourcing firm is itself subject. In addition, the contract includes procedures for the offshore provider to follow for notifying the outsourcing firm of privacy breaches, controls to help prevent certain employees and third parties from obtaining access to

certain confidential customer data, and language requiring the vendor to conduct regular privacy audits and report the findings to the company. As per suggested by the Internet Business Law services, the agreement should require the vendor to educate employees about the outsourcing company's data protection and privacy policies, and require the vendor to have employees with access to sensitive data sign confidentiality agreements. Moreover, as there is a trend of subcontracting projects in the several offshore clients to an even cheaper location such contract should also include that the vendor may not subcontract in the absence of outsourcer approval of the subcontract and should give the outsourcing company a right to have the subcontract terminated for inadequate privacy. According to a panel of Internet Business Law lawyers, these clauses in the contract will play an important role in the privacy preservation of the offshored client data.

Moreover, as suggested by Ferrell and Gresham (1985) the rule, regulations or guideline such as code of conducts is one of the major factors that affect the ethical behavior of the employees. Hence, we posit:

H1a: Code of conducts and other requirements for data protection set by the clients positively affects the privacy-preserving behaviors of the offshore vendors' employees.

H1b: Code of conducts and other requirements for data protection set by the clients positively affects the privacy preservation of the offshored data.

Code of Conduct and Other Requirements Set by the Vendor Company

An offshoring arrangement requires a huge investment of resources from both the client and the vendor company. To justify the level of investment both parties normally look towards a long-term contract (Nath & Bejou, 2012). Therefore, realizing privacy preservation of the offshored data is a major concern for the client company, the vendor companies place rules, regulations, and code of conduct for their employees to preserve the privacy of the client data. These rules, regulations, and code of conducts might include additional ones in addition to what is required by the client in the contract (Barney, 1991). Vendor companies have direct control over the people handling the client data and are the authority responsible for enforcing the rule, regulations, and code of conducts to preserve the privacy of data. Therefore, we assert that a vendor company placed rules, regulations, code of conduct and other requirements will positively affect the privacy-preserving behavior of the workforce.

H2a: Code of Conduct and other requirements for data protection set by the vendors positively affects the privacy-preserving behaviors of the offshore vendors' employees.

H2b: Code of Conduct and other requirements for data protection set by the vendors positively affects the privacy preservation of the offshored data.

Code of Conduct and Other Requirements Set by the Professional Organizations

If the vendor country does not have a "strong" rule of law, then it could be inferred that the existing institutions are not effective enough to implement and exercise laws like Intellectual Property Right effectively to ensure the protection of the foreign clients' data. In that scenario, formal rules, regulations, guidelines, as well as a code of conducts placed by a higher authority, will affect the conduct of the employees of the vendors and overall privacy of the clients' data. As there is increasing concerns around data security and privacy in India NASSCOM, one of the most recognized and vocal trade organizations in the information technology (IT) software and services industry in India, has put in place several measures to address data security concerns regarding service provider employees. Many of NASSCOM's roles to an extent reflects India's weak regulatory environment. (Trombly & Yu, 2006). India does not have a strong law in place requiring the protection of personal data. Therefore, NASSCOM has introduced "assessment and certification" programs for the new employees in an attempt to fill the regulatory lacking and to discourage illegal and unethical behaviors (The Economist, 2006). In addition to these efforts, NASSCOM has also launched an independent self-regulatory agency to improve privacy and data protection standards for the country's offshore IT services and BPO clients.

Kshetri and Dholakia(2009) suggested that in a developing country where the rule of law is "week" or "ignored with impunities" (Bratton, 2007), the professional associations can become more effective in shaping the members' behavior. The effectiveness and the "*success*" of India's National Associations of Software and Service Companies (NASSCOM) in preserving the privacy of the offshored data in India is an example of such a phenomenon.

Hence, we posit the following:

H3a: Code of conducts and other requirements for data protection suggested by the professional associations in the vendor country will positively affect the privacy-preserving behaviors of the offshore vendors' employees.

H3b: Code of conducts and other requirements for data protection suggested by the professional associations in the vendor country will positively affect the privacy preservation of the offshored data.

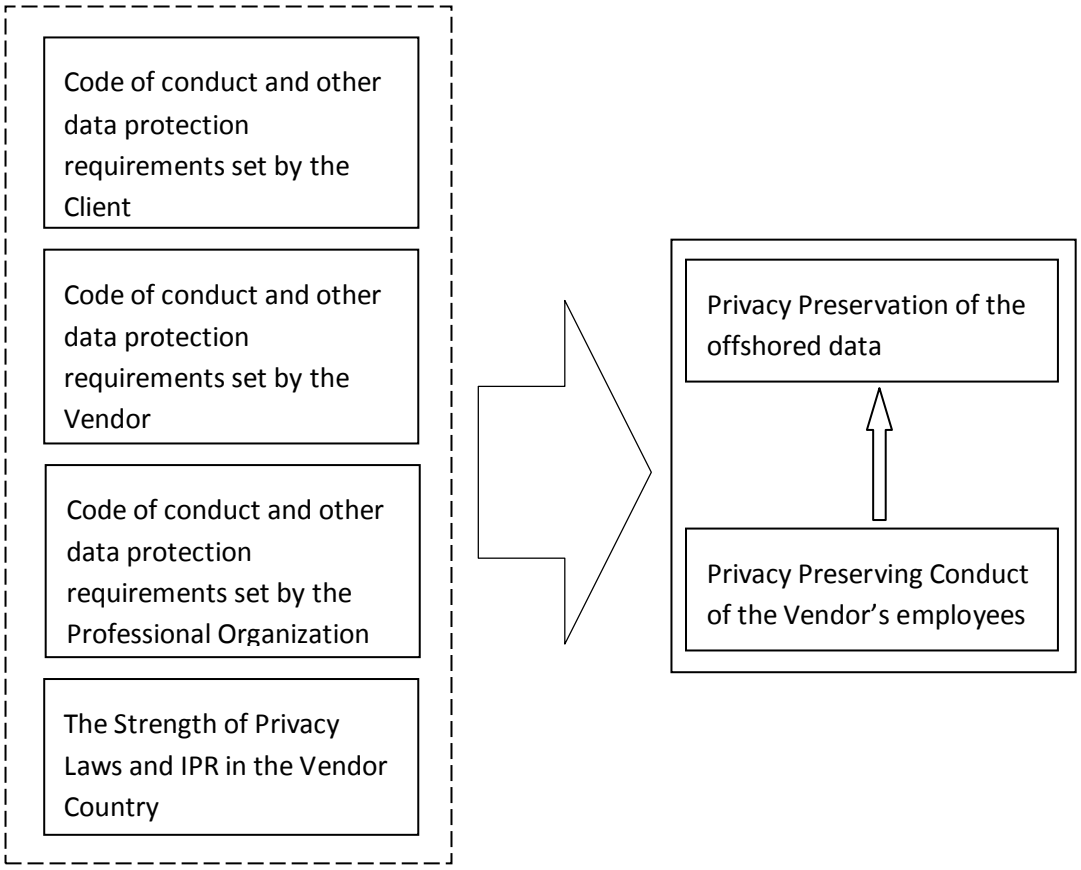

Figure 1. Research Model

The Strength of Privacy Laws and IPR in the Vendor Country

Every country governs Intellectual property and privacy of Data based on own distinct national law. These laws vary from one country to another. Many US and Europe-based companies are concerned about privacy preservation of the offshored data as in many of those countries there is a weak legislative environment and is difficult to enforce privacy (Engardio, Puliyenthuruthel, & Kripalani, 2004; Ravindran, 2004). In outsourcing, USA's privacy legislation is quite a lenient comparison to European Union (EU) regulations. U.S. privacy protections effectively end at the border, placing the obligation directly and solely on the shoulders of the U.S. client company if there is any privacy breach offshore. However, European consumers are afforded considerably greater protection by an EU law that permits personal data to be sent offshore only to countries whose privacy laws are perceived to provide equivalent privacy protection and that have been found to have strong enforcement capabilities. Essentially as perceived by the EU law, the Privacy Protection law and Intellectual property law in the vendors' country will help them to protect the privacy of the offshored data. Hence, we posit:

H4a: The strength of Privacy preservation law in the vendor country will positively affect the privacy-preserving conducts of the offshore vendors' employees.

H4b: The strength of Privacy preservation law in the vendor country will positively affect the privacy preservation of the offshored data.

Research Approach and Methodology

The use of case study research to test theory requires the specification of theoretical hypothesiss and related testable hypothesiss derived from existing theory. The results of case study data collection and analysis are used to compare the case study findings with the expected outcomes predicted by the hypothesis (Cavaye, 1996). The positivist studies are epistemologically premised on the existence of prior fixed relationships within phenomena which could be identified and tested using "hypothetico-deductive" logic and analysis (Dubé & Paré, 2003). Hypotheses are tested by comparing their predictions with observed data. To test the hypotheses through deductive testing, as per suggestion by Lee (1989), we look for observations that confirm a prediction to establish the truth of a hypothesis as well as we involve looking for disconfirming evidence to falsify the hypothesis. Falsified hypotheses might need to be refined based on the reasons for falsification and subjected to further empirical testing (Shank, 2002).

We deploy a qualitative positivist case-study approach to test the hypotheses. Our adoption of positivism is consistent with the views that are held by scholars in the fields of organizational studies (Eisenhardt, 1989), and information systems (Sarker & Lee, 2002; Lee, 1989; Orlikowski & Baroudi, 1991; Orlikowski,1993), and follows a similar path. "Hypothetico-deductive logic" is central to the world of positivist research today, which essentially is a synthesis of three traditions: empiricist, rationalist, and critical rationalist (Sarker & Lee, 2002). There is an empiricist influence in our positivist approach that is reflected in the rigor of our research process, drawing mainly on Yin (1994). The rationalist and the critical-rationalist traditions are reflected in the use of pattern matching to deductively test falsifiable statements derived from the literature (Sarker & Lee, 2002).

As this research is principally positivist in nature, using clearly defined methodological guidelines we satisfy the four criteria of rigor (Shanks, 2002): construct validity, internal validity, external validity, and reliability (Lee, 1989; Yin, 1994). In table 1, we summarize how we address the requirements of the positivist case-study method.

Table1. Steps to Achieve Rigor of the Study as Per Qualitative Case-Research Criteria

Rigor Criterion	**Guidelines to achieve rigor based on Lee (1989), Yin (1994) and Sarker and Lee (2002)**
Construct validity	Use of multiple sources of evidence Review of the report by the key informants Chain of evidence
Internal validity	Pattern matching
Reliability	Case-study database (consists of case-study notes, documents, and narratives) creation and maintenance Case-study protocol
External validity	Increased degree of freedom Replication logic

Based on this plan, we collect data to test the proposed hypotheses.

Case Selection

Case selection is a critical aspect of conducting a case study. Not only does the population define the set of entities from which the research sample is to be drawn, but the selection of an appropriate population also controls extraneous variation and helps to define the limits for generalizing the findings (Eisenhardt, 1989). According to the recommendations by Yin (2003), and Eisenhardt (1989) we based the case selection for our study on two factors - theoretical background and feasibility.

The first factor includes theoretical relevance, purpose, similarities, and differences across data sources with regard to the data sources' appropriateness for the study. In our case, we want to study the uses and effects of Web 2.0 based KM at the group levels. Hence, we selected two organizations which have been part of the offshore arrangement for a sufficient length of time to identify and understand the effects of different factors related to privacy preservation of data. Both organizations are leading firms in their respective fields in the IT industry and have branches or offices in many countries. However, they are different regarding the role they play in an offshoring arrangement. While organization A is an offshore vendor dealing with client data, organization C is the client. The second factor, feasibility, was largely determined by each organization's willingness to participate in the study and to

provide the required information. In our research, the organizations we selected had to be willing to provide us the necessary information and share their experience so that we could study the effects of different factors regarding privacy preservation.

Organization A is an information technology Services Company in India with more than 100 thousand professionals. It has offices in 22 countries and development centers in India, China, Australia, UK, Canada, and Japan. In 2009, organization A was recognized as one of the best performing and innovative companies in the software and services sector in the world by Forbes and Business Week.

Organization C is an American multinational corporation that designs and sells consumer electronics, networking and communications technology and services. C has more than 65,000 employees and annual revenue of more than 36 billion dollars. C has more than 190 branches worldwide.

Organizations A and C are in different offshoring arrangements for various IT services, C as a client and A as an offshore vendor, for more than a decade.

We interviewed three managerial level persons from organization C. All these managers been overseeing IT offshored projects for several years and working extensively with the vendor organizations in India. While one of them no longer are responsible for overseeing offshore projects because of his recent promotion and change in job description, others are still managing and overseeing more than one ongoing offshored projects with Indian vendors.

On the vendor side, we could also include three managerial level individuals from organization A. All of them are involved in managing US-based clients' IT projects and have worked on such a project in different capacities. The interviewees have worked on different sorts of offshored IT projects such as product development, testing, and sales management.

Data Collection and Analysis

Our principal data collection method is semi-structured interviews. Each of the interviews lasted around 25-50 minutes on an average. We recorded the interviews whenever possible and transcribed before starting the data analysis. To enhance the validity of the answers, wherever possible, we verified summaries of the major findings with the interviewee after the end of each interview session. Furthermore, to ensure consistency and reliability, we used structured interview guides for all interviews. The interview guide includes several open format questions based on our research model which is based on existing literature. However, to allow the participants flexibility in their responses, we used open-ended questions.

As a second data source, wherever possible, we also investigated the internal documents (e.g., draft of contracts) which the organizations use in an offshoring arrangement. Existing literature suggests that it is preferable to have multiple investigators in such case studies. Hence, wherever possible, we made sure that at least two researchers were present for the interviews. A significant characteristic of our research is the overlap of data analysis and collection, and we achieve this through field notes. Overall, we followed the same guidelines we followed in phase1 which was provided by Lee (1989), Yin (2003) and Sarker and Lee (2002) to achieve rigor in our case study.

Hypotheses Testing Results and Discussion

We present the results of propositions testing in the following section, and summary of the results in table 1.

Hypotheses 1s:

We have some interesting conflicting findings on these propositions. While we found strong support for this hypothesis from the client's perspective, we did not get ample support from the vendors' point of view. The managers of the client organizations thought that the requirements such as code of conducts for employees they impose on the vendor side through the contract they sign with the vendors play the most important part in protecting their data from any misuse when they offshore them. The managers identified three major aspects of any contract that they thought plays the most important role in protecting their data as follows.

First, as per the contract, if a vendor organization fails to protect the client organization's data, then the vendor will pay a large monetary penalty to the client organization. A project manager from the client organization mentions:

> *"If somehow, they (the vendor organization) fail to meet the requirements mentioned in the contract, they have to pay us (the client organization) a huge amount of fine."*

Second, the client organization ultimately has the authority to decide who will work on the project and who from the vendor organization will have access to the data. As a project manager mentions,

> *"The contract requires them (i.e., vendor organization) to have clearance for every employee they use in my project from me."*

Third, most of the contracts are short term. Hence, to keep on renewing the contract, the vendor organization has to keep the client data safe which is one of the requirements of the clients. A project manager mentions,

> *"Most of our contracts are only three months long initially. The contract gets renewed for another 3-6 months based on the performance in those three months. So, if I am not convinced of the safety of my data, then I will not renew the contract."*

On the other hand, the management of the vendor organization thought that the aspects mentioned by the clients are important. But what matters most is the guidelines, code of conduct, rules and regulations they have in place to protect any sensitive data. Interestingly, it appeared to us that the managers of the client organization felt almost offended when we emphasized the importance of clients' suggested guidelines and code of conducts for protecting data. According to the vendor organization, they have enough sensitive data of their own, and they need to protect that from competitors or any other unauthorized users and uses. Hence, to protect data, they make sure all the employees working for them abide by the code of conduct and other rules and regulations. As a manager explains,

> *"We have to eat our own dog food you know. We have those data security and privacy measures in place for our information too as we need to protect the sensitive information from the outsiders."*

They also thought that their employees do not interact with the client organizations' representatives frequently enough to be driven by their code of conducts. However, they admitted that the manager who is working on behalf of the vendor organization might take extra effort to convince the clients about the integrity of their (client's) data. To do so, as one of the managers from the client side has described, it can become *"sand is hotter than the sun"* scenario. One of the examples a manager provided is like this:

> *"When one of the employees working with the client's data ran a query who is not supposed to run by mistake, that employee got fired immediately. Finding no other way, that employee contacted the manager from the client organization, describing the scenario and how he did it by mistake and not with any bad intention. Under the circumstances, the manager from the client company thought it was little "too harsh" and recommended giving back his job."*

Examples like these lead us to conclude that guidelines and code of conduct set by a client are important for the vendor organization to an extent. However, they are not the most influential factor in the privacy-preserving behavior of the employees as the client organizations do not or cannot implement those directly in most cases.

Hypotheses 2s:

We found the strongest support for this hypothesis. Both client and vendor organizations thought that code of conducts set by the vendor organizations is the most influential factor. From vendor's point of view, they thought as they are the party who is responsible for enforcing any code of conduct as well as rules and regulations, they are the most influential factor no matter whether those rules have been proposed by a client or a professional organization or vendor country. They emphasized that their employees mostly are not aware or concerned about from whom the guideline, code of conduct or rules and regulations have been originated. What matters to them most is that to work for that vendor organization (and in some cases in certain projects), they have to abide by those rules, regulations, and code of conducts. Otherwise, the employee(s) sees job loss or another type of punishment carried out by the organization they are working for as the immediate effect.

The client organization to a large extent had a similar opinion. They emphasized that while based on the nature of the project and the sensitivity of the data, they might want the offshore vendor to take additional measures to protect their data, the vendors are responsible for putting them in place. The representatives from client organizations also mention that the code of conduct for employees and other rules and regulations they want to be placed are through the contract they sign, and, in most cases, they are not involved in the micro-management of actually making sure they are implemented and followed properly. However, they have emphasized that it is because they have been working with a specific offshore vendor(s) for a long time and they have mostly positive experience up to that point. But, for an entirely unknown offshore vendor, this scenario could be different.

Hypotheses 3s:

We did not find ample evidence to support this hypothesis. Neither the client side nor the vendor organization thought that professional organizations have a very strong role to play in the privacy preservation in the current state of the offshoring arrangements between USA and India. Surprisingly, it appeared to us that client organization has very little awareness of the role of the most prominent professional organization of India NASSCOM. They know that it is a there and it plays a certain role internally. However, interviewees from the client side did not think that professional organization would play a significant role in preserving the privacy of their data. As a project manager from client organization mentions,

> *"Yes. I know about NASSCOM. However, I am not so sure how effective they are in preserving the privacy of our data."*

On the other hand, the interviewees from the vendor organization had an interesting perspective. They thought a professional organization like NASSCOM could play an important role in privacy preservation of the client data. However, they did not think it plays a significant role in affecting the privacy-preserving behavior of their employees and their organization as they thought they already had strong rules and regulations to protect their data as well as client data.

The managers of vendor organizations provided examples regarding employee screening process and the behavioral guideline they had in place claiming that these processes are stronger than what a professional organization suggests. However, they thought it might help relatively newer organizations to shape up rules and regulations in a way that would help them to protect client data. Not only that, they thought the professional organizations could play a very important role in protecting client data.

Table2. Summary of the hypotheses testing

Hypotheses	**From Clients' Perspective**	**From Vendors' Perspective**
P1: Rules by Client	Supported	Moderate Support
P2: Rules by Vendor	Supported	Supported
P3: Rules by professional organization	Moderate Support	Moderate Support
P4: The strength of privacy preservation law in the vendor's country	Moderate Support	Supported

Hypotheses 4s:

We found fairly strong support for this hypothesis regarding the role of privacy preservation law. The client organization's management thought having a strong privacy preservation law strongly affects the privacy-preserving conducts of the offshore vendors and their employees. As mentioned by a project manager from client organization,

> *"It certainly makes us feel more comfortable if we know that there is strong privacy preservation law in that (i.e., vendor's) country."*

One thing was quite apparent that the client organizations thought that having strong privacy preserving law would help and that was somewhat a concern at the beginning of the offshoring arrangements. However, over the time as they had worked with the certain offshore vendor(s) and had mostly positive experience with

the vendor(s), the strength of privacy preservation law in the vendor country has become less concern for them. A project manager from client organization mentions

> *"… over the time we have come to know some key persons in vendor organization, and we rely on them."*

On a similar note, we asked them about their Indian offshore vendor's practice of offshoring to China where arguably privacy preserving laws is weaker than India and whether that concerns them or not. They responded that they trust their offshore vendor and rely on the contract that they had with them. Therefore, no matter where their Indian offshore vendors send their works to get it done, they are the responsible party and will be held accountable for any misuse of data. However, as per their contract, the offshore vendors must get clearance from their client for each of the team members who will have access to their sensitive data. Hence, if a vendor organization in India wants to involve team members from China, then they are required to get clearance from their clients. But as a project manager mentions,

> *"The contract requires them (i.e., vendor organization) to have clearance for every employee they use in my project from me. However, in most cases, it becomes merely a formality as I know him (i.e., the project manager/representative on vendor's side) and sort of think that he will make a right judgment. In any case, if anything goes wrong, they would be held responsible."*

The vendor organizations thought that having a strong privacy preservation law is a big help. Most of the employees in a vendor 's organization have a very vague or no idea about what conduct would be an invasion of privacy as they grow up in society and earns an education in a system where sensitive things like intellectual property law and privacy preservation law either do not exist or not practiced properly. Therefore, the management of the vendor organization thought that it becomes a quite steep learning curve for the newly hired workforce to get accustomed to the all the new rules and regulations they should follow to preserve the integrity of any data they would handle. The vendor organization from India mention that they face the similar change when they hire people from China as they also grow up in a weaker "rule of law" country. Hence, having an environment where there is a strong "Rule of Law" to protect data or any intellectual property positively affects the privacy-preserving behavior of the people they would hire to work in projects and that in turn will increase the safety of data.

Conclusion

Offshore outsourcing certainly has its benefits. However, it comes with a risk of misuse of sensitive information. Different institutional factors might affect the privacy preservation of the offshored data. In our study, we identified the mimetic, coercive, and normative institutional factors that would affect the privacy preservation of the sensitive offshored data and empirically tested their effectiveness. The findings show that the code of conduct set by the offshore vendors plays the most important role followed by the code of conduct set by the clients and the strength of privacy preservation law in the vendor's country.

The findings of our research shed light on an important aspect of the literature as we included both client and vendor managements' perspective to verify the effects. However, one limitation of our finding is that the client and vendor organizations in our case study are industry leaders and very well reputed firms and have been in offshoring arrangement with each other for at least last ten odd years. Hence, it appeared to us that the response from client management is mostly based on the trust they have in the vendor organization, and it might change if they get into an offshoring arrangement with a relatively new company. Hence, to address this limitation, we intend to have more than one vendor organization with a varied level of reputation in the market.

References

Audit of the Federal Bureau of Investigation's Cyber Threat Prioritization. Retrieved from https://oig.justice.gov/reports/2016/a1620.pdf .

Barney, J.B. (1991), Firm Resources and Sustained Competitive Advantage, *Journal of Management*, 17(1), 99-120.

Bender, D. (2007) Internet Law- Outsourcing Offshore May Pose Problems for Protecting Data. Retrieved from http://www.ibIs.com/internet_law_news_portal _view.aspx?s=latestnews &id=1635.

Bratton, M. (2007) Formal Versus Informal Institutions in Africa, Journal of Democracy 18(3), 96-110.

Cavaye, A. L. M. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal*, 6, 227-242.

Culnan, M. J., & Williams, C. (2009) How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches, *MIS Quarterly*, 33(4), 673-687.

Das, T. K., & Teng, B. (2001) Instabilities of Strategic Alliances: An International Tensions Perspective, *Organization Science* 11(1), 77-101.

DiMaggio.J., & Powell. W. (1983) The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality Organizational Fields, *American Sociological Review* 48(2), 147-160.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly*, 27(4), 597-634.

Eisenhardt, K. (1989) Building Theories from Case Study Research, *The Academy of Management Review*, 1(4), 532-550.

Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004). Fortress India? *Business Week* (3896), 42-43.

Ferrell, O.C., & Gresham, G. L. (1985) A Contingency Framework for Understanding Ethical Decision Making in Marketing, *Journal of Marketing*, 49(3), 87-96.

Kshetri, N. & Dholakia, N. (2009). Professional and trade associations in a nascent and form ative sector of a developing economy: a case study of the NASSCOM effect on the Indian offshoring industry. *Journal of International Management*. 15(2), 225–239.

Palvia, S., & Jain. C. (2017) Global Sourcing of Services: A Two-Stage Model for Selecting a Vendor. Global Sourcing of Services: Strategies, Issues, and Challenges, 407.

Polak, J. & Przemyslaw, W. (2015) Knowledge management in IT Outsourcing/Offshoring Projects, *PM World Journal*, 4(8).

Lee, A. (1989) A Scientific Methodology for MIS Case Studies, *MIS Quarterly,* 13(1), 33-50.

Meyer, J.W., & Rowan, B. (1977) Institutionalized Organizations: Formal Structure as Myth and Ceremony, *American Journal of Sociology*, 83(2).

Moores, T.T., & Chang, J.C.J. (2006) Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model, *MIS Quarterly*,30(1), 167-180.

Nath, A. & Bejou, A. (2012). Offshored Data Privacy: Determining the factors and their relative effect, Proceedings of the 18th Americas Conference on In-formation Systems (AMCIS), Seattle, USA, 2012.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, 2(1), 1-8.

Orlikowski, W., (1993), Case Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development, *MIS Quarterly*, 17(3), 309-340.

Overby, S. (2010), Offshoring: The 25 Most Dangerous Cities for Outsourcing in 2010. Retrieved from CIO.com http://www.cio.com/article/596533/offshoring_ The_25_Most_Dangerous _Cities_For_Outsourching_in_2010.

Polak, J., & Wójcik, P. (2015, August). Knowledge management in IT outsourcing/offshoring projects (2nd ed.). *PM World Journal*, 4(8), 1-10.

Ravindran, P. (2004) Factors That Are Worrisome For BPO Sector., Business Line. Retrieved from http://www.thehindubusinessline.com/2004/04/03/stories/2004040302210300.htm

Sarker, S. & Lee, A. (2002) Using Positivist Case Research Methodology to Test Three Competing Theories-In-Use of Business Process Redesign, *Journal of AIS*, 2(7), 1-72.

Shanks, G. (2002, November). Guidelines for conducting positivist case study research in information systems. *Australasian Journal of Information Systems*, 10(1), 76-86.

Special report: watch out, India-outsourcing to China. Outsourcing to China, *The Economist*, 379(8476), 80, 2006. Retrieved from http://www.economist.com/node/6878397.

Swartz, N., (2004), Offshoring Privacy, *Information Management Journal*, 38(5), 24-26.

Tafti, M. H. A., (2005) Risks factors associated with offshore IT outsourcing, *Industrial Management & Data Systems*, 105(5), 549-560.

Tate, W., Ellram, L., & Bals, L. (2009) Offshore Outsourcing of Services: An Evolutionary Perspective, *International Journal of Production Economics*, 120(2), 512-524.

Trombly, M., & Yu, W. (2006) Outsourcing resilient in India, *Securities Industry News*, 18(26), 1-21.

Yin, R. K. (1994). Case study research: Design and methods (2nd ed.). Thousand Oaks, C. A.: Sage.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, C. A.: Sage.

Zelijka, (2017) Offshore Law Firm Appleby Confirms Data Breach. Retrieved from https://www.helpnetsecurity.com/2017/10/26/appleby-confirms-data-breach/.

About the Author

Anupam Kumar Nath*
3893 Lost Oak Drive,
Buford, GA 30519,
USA
Tel.: +1(919)-274-9339
E-mail: anupamknath@gmail.com

*Corresponding author

Anupam Kumar Nath is an assistant professor in the School of Business at Georgia Gwinnett College. He received a Ph.D. degree in Information Systems from The University of North Carolina at Greensboro. His research interests include Outsourcing, Knowledge Management., Social Computing, E-Government, and Data Privacy. Nath's research has been published in several journals, including Journal of Information and Knowledge Management Systems, Journal of Accounting, Business & Management and e-Service Journal. His research has also been presented at national and international conferences, including America's Conference on Information Systems (AMCIS) and Decision Sciences Institute (DSI).