Communications of the Association for Information Systems

Volume 42 Article 4

2-2018

Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies

V S Prakash Attili
Infosys Ltd, PrakashV_S@infosys.com

Saji K. Mathew
IIT Madras

Vijayan Sugumaran
Oakland University

Recommended Citation

Attili, V S Prakash; Mathew, Saji K.; and Sugumaran, Vijayan (2018) "Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies," *Communications of the Association for Information Systems*: Vol. 42 , Article 4.
DOI: 10.17705/1CAIS.04204
Available at: http://aisel.aisnet.org/cais/vol42/iss1/4

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04204 ISSN: 1529-3181

Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies

V. S. Prakash Attili
Education Training and Assessment
Infosys Ltd
India
prakashv_s@infosys.com

Saji K Mathew
Department of Management Studies
IIT Madras
India

Vijayan Sugumaran
Decision and Information Sciences
Oakland University
USA

Abstract:

We develop a framework for understanding the mechanisms of information privacy assimilation in information technology (IT) organizations. Following neo-institutional theory, we develop a broad conceptual model and further build a detailed theory based on a multi-site, multi-case study of 18 organizations. We treat information privacy as a distinct dimension separate from information security. As in the case of information security, senior management support emerged as a mediator between the external influences of coercive, mimetic, and normative forces and information privacy assimilation. Privacy capability emerged as a distinct construct that had a moderating effect on the influence of coercive and normative forces on privacy assimilation. Similarly, cultural acceptability also moderated the effect of external forces on privacy assimilation. We produce a theoretical model that future research can empirically test. The findings would enable senior managers identify and respond to institutional pressures by focusing on appropriate factors in the organizations.

Keywords: Information Privacy, Privacy Assimilation In Organizations, Neo-institutional Theory, Synergy Between Privacy and Security.

This manuscript underwent peer review. It was received 01/28/2017 and was with the authors for 6 months for 2 revisions. Alvin Leung served as Associate Editor.

1 Introduction

Data supports management decisions in the 21st century more than ever in the past, which leaves data vulnerable to privacy breaches. The Privacy Rights Clearinghouse has reported that, since January 2005, in the US, 912 million records that contain sensitive personal information have been exposed due to 5,436 data breaches (Privacy Rights Clearinghouse, 2017; DSCI, 2016b), which may be the tip of the iceberg. Notwithstanding the cost of data breaches suggested in research, management attention still remains wanting, and organizations' management approaches to information privacy protection show a high level of variance (Acquisti, Friedman, & Telang, 2006; IAAP, 2014; TRUSTe, 2015).

What are the external forces that organizations respond to in defining privacy policies? How do organizations respond to external information to shape their privacy practice? Does organizational adoption of privacy practice get translated into strategic actions? Although research on data security has examined such enquiries (Armstrong & Sambamurthy, 1999; Hsu, Lee, & Straub, 2012), we still do not understand information privacy well at institutional level. Surprisingly, in the Ernst & Young (2015) Global Information Security Survey (GISS) privacy questionnaire, 38 percent of respondents admitted that they addressed security in new business processes and technologies but not privacy specifically.

Recent studies have also reported a scarcity of privacy studies at the organizational level compared to the individual level (Belanger & Crossler, 2011). On the other hand, academic studies have analyzed the interplay between the external institutional forces and internal factors at an organizational level with reference to information security assimilation (Hsu et al., 2012; Tejay & Barton, 2013). However, we still do not clearly know how institutional forces influence information privacy assimilation and the factors that drive this assimilation in organizations. As such, we have gaps in our current understanding of "privacy assimilation" at the "organizational level", which forms the focus of our current study. We address this research gap and follow a multi-case, multi-site approach to first identify the institutional forces specific to information privacy and posit potential relationships among the concepts identified.

2 Literature Review

2.1 Information Privacy in IS Literature

As computers, networks, and the Internet continue to influence social, political, and business activities in many ways, information privacy has received a distinct and significant attention in recent times. Westin (2003) tracks this distinct evolution of information privacy through four eras: 1) privacy baseline (1945-1960), 2) first era of privacy (1961-1979), 3) second era of privacy (1980-1989), and 4) third era of privacy (1990-2002). A parallel stream of research and practice evolved around data security, and the terms security and privacy have often been used synonymously, which has caused confusion (Belanger et al., 2002). However, information privacy in the current and future world of technology stands out as a distinct phenomenon from security.

Ackerman (2004, p. 432) suggests that "security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of…disclosure, or to reassure users". In e-commerce, for example, online shoppers are interested in knowing not only whether the online transactions are secure but also the vendor's information privacy policies in terms of how their personal information is/will be used (Kim, Yim, Sugumaran, & Rao, 2016). In analyzing the literature, we found three reasons that pertain to business, legal-regulatory, and academic research imperatives that suggest the need for a separate and distinct focus on information privacy research.

First, the issue of privacy has already posed a significant challenge to many reputed and large organizations such as Google (Hansell, 2008) and Facebook (Stone & Stelter, 2009), ChoicePoint and TJMax (Culnan & Williams, 2009), which have faced privacy-related backlash in recent years (Xu, Dinev, Smith, & Hart, 2008). In particular, organizations often lack clarity about dealing with privacy in that they often face ethical and moral dilemmas when dealing with customers' data. Culnan and Williams (2009) investigated major privacy-related incidents that led to substantial financial losses at ChoicePoint and TJMax (TJX). In their paper, they provide recommendations on dealing with privacy-related incidents that hurt organizations and argue that organizations can successfully secure stored personal information but still make bad decisions about the subsequent use of it, which can result in information privacy problems. Chan et al. (2005) and Greenaway, Chan, and Crossler (2015) highlight the organizational imperative to address privacy as distinct from security.

Second, the 9/11 terrorist attack has significantly impacted “privacy concepts” and dramatically changed the landscape of information exchange in that it has set the bar higher for privacy concerns (Westin, 2003). Chan et al. (2005) reported analysis by expert panelists on privacy disasters, and they identified an array of challenges that governmental policies or self-regulatory approaches could address. Over 80 countries and independent territories have now adopted comprehensive data-protection laws including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa. Recently, the General Data Protection Regulation (GDPR) (Regulation 2016/679) has focused on strengthening and unifying data protection for individuals in the European Union (EU). A country-level focus on privacy (separate from security) became a new direction of thought in the 21st century (Gupta, 2014).

Third, the growing emphasis on information privacy has resulted in a stream of research focused on privacy-related issues at different levels. Belanger and Crossler (2011) review over 500 papers and 102 conference proceedings that study information privacy at individual, group, and organizational levels. However, they note that that bulk of privacy research pertains to individual level of analysis and that privacy at organizational level remained less explored. Hu et al. (2007) conceptualize security as an administrative innovation and address it at the organizational level. Smith et al. (2011) indicate that “it’s impossible to develop a one size fits all” for privacy policies and suggest that further research needs to conceptualize information privacy through exhaustive interviews with an organization’s members and stakeholders. This approach would uncover subtle organizational dynamics that drive privacy policies and practices (Pavlou, 2011; Smith, Dinev, & Hu, 2011).

The privacy research panel at the 2013 IEEE Symposium on Security and Privacy (NITRD Program, 2013) discussed privacy not as a subset of security. The panel delineated the difference between privacy and security in layman’s terms as follows: privacy is characterized as pink (i.e., soft with complicated laws and people involved) and security as blue (i.e., hard with more systems involvement). With this backdrop in the evolution of information privacy as a distinctly different phenomenon, which research has scarcely addressed at the organizational level, we focus on information privacy at organizational level.

2.2 Theoretical Foundations: Institutional Theory

In reviewing the broader literature in relation to privacy, we found: a) reforming laws related to privacy, b) contribution to reform the policies related to privacy by auditing firms, and c) an increasing focus on privacy training to minimize uncertainty in the technology landscape. These drivers resemble coercive, normative, and mimetic forces that respectively make up the institutional theory (Attili, Mathew, & Sugumaran, 2015). Robey and Boudreau (1999, p. 177) suggest that the institutional approach is particularly well suited to addressing the “question of information technology and organizational change, conflicts among external pressures (efficiency, rights to privacy, autonomy) and deeply embedded notions of bureaucratic and hierarchical structure”. Greenaway et al. (2015) highlight the strategic implications of privacy, which makes an institutional-level understanding of information privacy imperative. Considering the strategic dimension of privacy, we propose a model for assimilation (strategy + value added activities) instead of compliance like in other studies. Previous studies in information systems have used neo-institutional theory (Liang, Saraf, Hu, & Xue, 2007; Saraf, Liang, Xue, & Hu, 2013; Tejay & Barton, 2013) to explain how organizations respond to external pressures for institutional change. Interplay between the external pressures and internal organizational factors can have strategic implications at the organizational level (Armstrong & Sambamurthy, 1999; Hsu et al., 2012). We further review the concept of assimilation in organizational context before we arrive at a framework for our study on privacy.

2.3 Assimilation

Meyer and Goes (1988) define assimilation as an “organizational process that 1) is set in motion when individual organization members first hear of an innovation’s development, 2) can lead to the acquisition of innovation, and 3) sometimes come to fruition in the innovations full acceptance, utilization, and institutionalization”. From a technological view, it also refers to the extent to which the use of technology diffuses across organizational work processes to become routinized in the activities associated with those processes (Armstrong & Sambamurthy, 1999; Chatterjee, Grewal, & Sambamurthy, 2002; Fichman & Kemerer, 1997; Gallivan, 2001). Researchers have studied assimilation in IT-related fields such as software process innovations (Fichman & Kemerer, 1997), IT innovations (Fichman, 2000), knowledge platforms (Purvis et al., 2001), complex technological innovations (Gallivan, 2001), Web technology (Chatterjee et al., 2002), ERP (Liang et al., 2007), and, recently, security-related policies (Gallagher, Zhang, & Gallagher, 2012).

3 A Priori Framework

Here, we focus on the concept of assimilation that pertains to information privacy in IT organizations. Building on prior literature, we regard information privacy assimilation as an important outcome in organizations' efforts to leverage the potential of information privacy practices in their business activities and strategies (Armstrong & Sambamurthy, 1999).

Drawing on the concepts of neo-institutional theory, we developed a broad framework (see Figure 1) to better initially understand the interplay between the external and internal factors that influence information privacy assimilation.

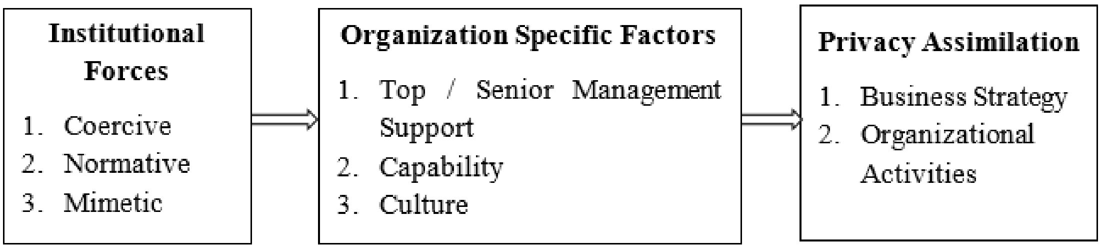

Figure 1. Privacy Assimilation Framework in IT Organizations

Following the neo-institutional theory as used in IS research, (DiMaggio & Powell, 1982; DiMaggio & Powell, 1991; Powell & DiMaggio, 2012), we anticipate that coercive forces such as regulatory requirements (Johnson, 2009; Liang et al., 2007; Tejay & Barton, 2013), normative forces such as professionalization of work (Appari, Johnson, & Anthony, 2009; Bjorck, 2004; Liang et al., 2007; Teo, Wei, & Benbasat, 2003), and mimetic forces such as ambiguity about technology, environment, and peers (Johnson, 2009; Liang et al., 2007; Tejay & Barton, 2013; Teo et al., 2003) influence organizational assimilation of information privacy.

Prior studies on IT assimilation have identified top/senior management support (Chatterjee et al., 2002; Hsu et al., 2012; Liang et al., 2007; McFadzean, Ezingeard, & Birchall, 2011) as a critical factor influencing assimilation. Considering the organizational context, we also include capability (Bharadwaj, 2000; Ernest Chang & Ho, 2006; Hsu et al., 2012) and cultural acceptability (Gallivan, 2001; Hsu et al., 2012; Hu et al., 2007) as other critical factors in the model.

4 Research Methodology

4.1 Approach

In order to validate our broad framework developed from literature, we followed a multi-case, multi-site approach and used a combination of inductive and deductive principles (Davis & Eisenhardt, 2011). Although theory building research often starts with an ideal clean theoretical slate of "no theory under consideration" and "no hypothesis to test" (Eisenhardt, 1989, p. 536), we chose to formulate the research problem with some potentially important variables from neo-institutional theory. Doing so helped us draft the initial semi-structured interview questions (Refer Appendix-A) similar to the ones that researchers have followed earlier (Ali & Birley, 1999; Braun & Clarke, 2006). The approach of starting with an a priori research framework for theory building follows the "retroduction" strategy, which captures the interplay between deductive and inductive research, referred to as a "reality check" (Harrison, 2002). Dibbern, Winkler, and Heinzl (2008) used a similar approach to specify their model a priori.

Further, "a priori specification of constructs [is] a recommended approach in shaping an initial design in case study research" (Eisenhardt, 1989). We do not test a theory; rather, we build a theory of information privacy for organizations by referring to similar theories while also observing industry practice. Yin (2013) highlights that "multiple-case studies typically provide a stronger base for theory building". We followed Eisenhardt and Graebner's (2007) guidelines, which focus on the research strategy of theory building from (particularly multiple) cases. Because privacy is an emerging topic, we followed the case study approach for understanding the real-world context based on multiple considerations. Here, multiple cases permit replication logic, and we treat the cases as discrete experiments that confirm, contrast, or extend emerging conceptual insights. Also, emergent theory from multiple-case research is typically more analytically generalizable and better grounded than theory from a single case study (Davis, Eisenhardt, & Bingham, 2007). Further, because privacy is a multidimensional concept (Hong & Thong, 2013), case research strategy suits efforts to understand its nature and complexity.

4.2 Data Sources and Sampling

We studied 18 IT organizations in India and USA, and our sample comprised respondents from these organizations. Tables 1 and 2 provide the characteristics of our sample organizations.

Table 1. Characteristics of the Organizations

Geography (significant presence)	Sample Count
India and USA	11
India	3
USA	4

Table 2. Classification of Organizations

Classification	Revenue (INR crores)	Sample count
Large	> 200	9
Medium	50 - 200	5
Small	< 50	4

Some of the identified IT companies operated across domains such as banking, insurance, healthcare, retail, telecommunications, manufacturing, human resource management, and consulting. Most of our participants had experience in more than one domain. We interviewed respondents with a minimum of 10 years' experience in their organizations (Fichman & Kemerer, 1997). Table 3 lists respondents' roles and their average experience.

Table 3. Classification of Organizations

Respondent category	Count	Average experience (years)
Leadership (senior management)	5	23
Director	3	
Associate information officer	1	
Vice president	1	
Practitioners (seniors + experts)	13	13
Senior managers (mid-level)	6	
Information/solution architects	5	
Principal consultants	2	

While interviewing the above sample, we asked mostly atheoretical questions (Ali & Birley, 1999) with an open mind. After two months of preparatory work (June and July in 2015) to identify the respondents and obtain their consent for the interviews, we conducted the actual interviews between August and November, 2015, telephonically for respondents from USA and in-person for Indian locations. Each interview lasted about 40 minutes on average. To triangulate the data, we extensively referred to the websites of the companies, industry bodies, and reports of consulting companies such as Ernst & Young, Deloitte, and Forrester.

4.3 Data Analysis Procedure

As part of the data analysis, we followed the six-phased thematic analysis that Braun and Clarke (2006) provide; these authors argue that it is a flexible method for qualitative research. During the course of the thematic analysis, we referred to existing literature to better identify subtle features of the data (Tuckett, 2005). We had also considered the caution from Eisenhardt (1989, p. 536) that researchers should avoid "thinking about specific relationships between variables and theories".

The first author fully transcribed the interview data. We did not use any tool for extracting themes as privacy is context specific. We analyzed and coded more than 25,000 words transcribed from interviews following the thematic analysis. After identifying 40 major themes, we extracted 287 quotations that best represented the identified themes. We provided two independent coders with a list of codes, an explanation of each code, and a sample chunk for each code. We instructed them to use the list to become familiar with the codes. We then provided them with a test set of quotations (287) from the interviews. The external coders and the lead author independently coded these chunks. We calculated inter-coder reliability using Holsti's (1969) code of reliability (CR). The coefficient of reliability for the test set was 0.78, which supports the reliability of the coding.

We used extensive tables and other visual devices that summarize the related case evidence to signal the depth and detail of empirical grounding. To do so, we referred to Gilbert (2005), Graebner (2004), and Zott and Huy (2007), which served as examples of blending construct tables with selected text descriptions. The strength of the quotations was indicated by A+, A, B, and C by all three coders; A+ was the highest and C was the lowest. In all, 115 out of 287 quotations (40%) emerged under A and A+. The second and third authors—academics with wide experience—analyzed the 115 quotations and selected 55 (19%) to present in the current manuscript. We used 39 of these quotations while discussing the thematic analysis and future scale development, and we present the remaining 16 in the manuscript to discuss the propositions of the model.

Here, we quantify the responses that came from key statements of 18 cases into three labels (Y++, Y+ or Y). "Y++" represents that two-thirds (or more) of participants supported the theme, and "Y+" denotes that more than one-third of participants supported the theme (Meehan, Vermeer, & Windsor, 2000; Reicher & Taylor, 2005). If two or more participants responded in support of a theme, we used "Y" to denote such a scenario. If only one participant responded in support of a theme, we duly checked for the possibility of an emergent theme and rechecked with participants.

5 Analysis and Results

We focused on identifying and examining the themes related to privacy in the context of IT organizations. We examined various themes that emerged under the three broad categories of institutional forces (coercive, normative, mimetic), organizational influencers (senior management support, culture, privacy capability), and assimilation (strategy, organizational activities).

5.1 Institutional Lens: Three External Forces

Themes that pertain to institutional forces that act on the organizations emerged from our coding procedure and fit with our a priori framework.

5.1.1 Coercive

Table 4 depicts the themes that pertain to coercive forces as specific to the organizational privacy.

Table 4. Themes that Pertain to Coercive Force

Tag	Themes	Label
COER1	Government/regulatory influence	Y++
COER2	Industry associations' encouragement	Y
COER3	Competitive conditions	Y+
COER4	Contracts with other businesses	Y
COER5	Customer expectations	Y+

COER1: the majority of the participants echoed the theme about regulatory requirements.

> *Most of the organizations the number one motivating factor is regulation, especially working with US clients. This is also mandatory and must rule [sic].* (Senior manager, medium-scale U.S. company (MSU-2))

Existing reports advocate more proactive forward-thinking privacy management strategies that balance existing regulatory requirements against technological development (Ernst & Young, 2012). The leading response for reasons to fund privacy remained "regulatory compliance" even in our study similar to the earlier reports (International Association of Privacy Professionals, 2012).

COER2: the theme related to "industry associations' encouragement" emerged as a mandate force with relatively less support in the interviews.

> *There is more and more emphasis on privacy and security every year. What I believe it's because of market trend and encouragement from industry forces.* (Vice president, large-scale multi-national company (LSM-5))

COER3: many respondents felt the impact of "competitive conditions" influence level of privacy funding.

> *As an organization, I would base regulation as my lower cut point; that is, it should be the minimum I should follow. Regulation is always a catch-up based on the experience. So, I feel organizations should follow regulations as minimum, but go with trends around privacy & security incidents to be on the top of game.* (Information architect, small-scale U.S. company (SSU-1))

This observation is interesting considering the nature of Indian IT industry—a dominant, competitive, service-oriented industry. Of late, the industry has begun to appreciate and adopt privacy in its various verticals such as the Internet of things (IoT) and big data analytics as recent conferences evidence (John & Ian, 2016). One Forrester report found that executives fund privacy initiatives more due to (among other reasons) competitive differentiation (Heidi Shey & Mak, 2012).

COER4: contracts with other businesses emerged as another theme.

> *Whenever we go for a contract, we need to follow all measures. For example, we can't take a mobile, recorder, Bluetooth device, memory card etc., to work area. This helps protect customer data in their data-bases.* (Senior manager, large-scale multi-national company (LSM-4))

In recent times, the Indian IT services provider Tata Consultancy Services (TCS) was fined US$940 million for privacy-breach allegations: accessing the documentation and process flow from one of their service providers (Kaiser Foundation Hospitals) for in-house software development (Dissent, 2016). In this context, law enforcement claimed that TCS performed a "breach of contract".

COER5: many participants emphasized "customer expectations" as an important influence for building and sustaining the trust.

> *Motivation comes from clients in terms of the trust to "hold and process data" in secured way; that is, to meet the expectation of keeping it safe end to end. Here maintaining the trust is the key factor.* (Information architect, large-scale multi-national company (LSM-1))

A Forrester report has highlighted the negative impact of data misuse on profitability and consumer trust. Growing awareness among consumers has led to higher expectations around privacy standards and policies (Shey, Mak, Balaouras, & Luu, 2013). Furthermore, among the executive reasons for funding privacy, "meeting business clients and partners expectations" stood among the top-three reasons.

5.1.2 Normative

Table 5 depicts the themes that pertain to normative forces that emerged from the interviews.

Table 5. Themes that Pertain to Normative Force

Tag	Themes	Label
NORM1	Formal education	Y
NORM2	Participating in conferences, forums	Y
NORM3	Journal subscriptions	Y(Limited)
NORM4	Presence of external consultants	Y
NORM5	Dedicated privacy certified employees	Y

NORM1: formal education was a key theme.

> *Ten years back, we didn't hear about data privacy and security and used to play with data a bit without knowing much of its consequences. But, recently, education and clear-cut understanding at each role playing a critical role.* (Information architect, large-scale multi-national company (LSM-1))

Professional networks such as the Data Security Council of India (DSCI), established in 2008, have played a pivotal role in spreading formal education through alignment programs with SANS, (ISC)^2, and some premier universities such as the Indian Institutes of Technology (DSCI, 2016b).

NORM2: participation in conferences and forums was the second leading influencer.

> *I am also Board of advisors of Cyber Security and Privacy Foundation, a non-profit organization that conducts trainings on security and privacy.* (Director, small-scale Indian company (SSI-2))

The chapters from DSCI, the Information Systems Audit and Control Association (ISACA), and the Cyber Security & Privacy Foundation (CSPF) are engaged with the IT and business process outsourcing (BPO) industry through a number of security and privacy awareness seminars and workshops across major cities (DSCI, 2016b).

NORM3: journal subscriptions.

Participants did not explicitly mention subscriptions to journals, though they did hint to them as an extension to participation in conferences. One practitioner explicitly mentioned the same. Considering the strong literature support (Liang et al., 2007; Tejay & Barton, 2013; Teo et al., 2003), we retained this theme.

NORM4: presence of external consultants also indicated the normative forces.

> *We believe on expert's opinion. It will have better value addition than who is working in the system. So, a third party evaluation is always gives us insight.* (Director, small-scale Indian company (SSI-1))

The complex nature of privacy compliance has led to an increase in privacy consultation opportunities for IT consulting companies (Ernst & Young, 2016; Shey et al., 2013).

NORM5: participants echoed the need for domain experts' going through the certifications and their dedicated presence in the teams.

> *There is a group that is responsible for standards. We reach out to this group to go over the plan. We will explain the initiative and privacy related aspects in it. They have to approve, then only we can go forward with initiative.* (Vice president, large-scale multi-national company (LSM-5))

Dedicated privacy-certified employees also indicated the professionalization and influence of normative forces. Various certification programs are being organized with special focus on privacy preservation (DSCI, 2016a; International Association of Privacy Professionals, 2016).

5.1.3 Mimetic

Mimetic forces come from peer organizations when individuals perceive these organizations' rules and practices as better in response to uncertain environments. When we asked interviewees if the actions of other companies influenced their privacy compliance and behavior, we received mixed responses. Table 6 depicts the themes that pertain to mimetic forces that emerged from our interviews.

Table 6. Themes that Pertain to Mimetic Force

Tag	Themes	Label
MIM1	Competitors' successes or failures	Y
MIM2	Perceptions of competitors in industry	Y+
MIM3	Adoption by successful peer firms	Y
MIM4	Following successful peer firms	Y+
MIM5	Absence of peer influence	Y+

MIM1: participants saw competitors' successes or failures as one of the influencing themes.

> *Peer organizations will also influence the privacy and security practices. In banking industry, if something happened to one bank wrongly, other banks will ensure to avoid similar incidents. This is to mitigate the domino effect.* (Senior manager, large-scale multi-national company (LSM-4))

More than competitors' successes, failure due to non-implementation of privacy practices can have an effect on peer firms. Participants expressed that privacy breaches have the potential to impact not only organizations but also their industries. Indeed, Target's data breach in 2013 and Home Depot's data Breach in 2014 alerted retail companies to strengthen their privacy and security practices.

MIM2: participants also saw perception of competitors in the same industry as a theme.

> *If somebody/origination is not there on protecting privacy, they should jump on to it. That way, they can secure their business for next decade…. Implementing the privacy frame work, it will give additional trust to the customers—to give their data, process their data. So, it helps.* (Principal consultant, large-scale multi-national company (LSM-7))

Participants favorably viewed competitors with strong privacy practices in the same industry. One recent example that concerns competitive pressures involves Microsoft and Google, which have recently argued about browser privacy settings and online advertising companies' ability to work around the settings to collect data on users (Hachamovitch, 2012).

MIM3: adoption by successful firms also emerged as a theme.

> *If we see as example, Fortune-500 companies – they take data security/privacy as highest concern. This reflects the immediacy of this measure.* (Information architect, large-scale multi-national company (LSM-6))

In the Indian context, employees had low awareness of information privacy and misconstrued it as a subset of security. As a result, many organizations included this as a part of chief information security officer's (CISO) function. Information privacy is emerging as an independent function and not considered as a subset of CISO, and it is being adopted by successful peers (Poorsarla, 2016).

MIM4: interviewees did express their interest in following their successful peer firms to mitigate risk.

> *Peer pressure is just to catch-up with others...but regulatory and client pressures are significant. But we do look out for what peers are doing—especially from an implementation point of view.* (Executive director, large-scale multi-national company (LSM-9))

With emerging technologies such as big data and the cloud, uncertainty and ambiguity related to information privacy has arisen. A report from ISACA that features interviews with cloud security alliance members has also highlighted that data privacy and security is one of the top 10 challenges and the challenge is related to big data privacy—"scalable and compassable privacy preserving data mining and analytics" (ISACA, 2012).

MIM5: some participants mentioned no peer influence when it came to privacy. The discussion concerned building privacy awareness as built in culture in the organization and not looking into peers.

> *Privacy will start from you; that is, within organization [sic]. That's how I feel. If I am working on a project, I see myself—can I disclose this. Privacy is always assumed by keeping the person himself in that situation. So, it's more about organizational ethics and not to get influenced by other organizations.* (Principal consultant, large-scale multi-national company (LSM-7))

Early studies have also observed the expression of "mimetic" views as "normative" (Hu, Hart, & Cooke, 2007). Thus, we can conclude that organizations may not mimic other organizations, but conferences and education might set the best practices as norm.

5.2 Organizational: Three Internal Influencers

5.2.1 Senior Management Support

Table 7 shows the key themes that pertain to senior management support. Though the literature prominently features the construct, we contextualized the themes to privacy.

Table 7. Themes that Pertain to Senior Management Support

Tag	Themes	Label
SMS1	Tone at the top	Y
SMS2	Strategy formulation	Y
SMS3	Decision making support	Y
SMS4	Establishing processes and standards	Y+
SMS5	Providing resources and assigning responsibilities	Y

SMS1: participants saw privacy compliance as a top-down approach, which indicates that senior management directly influences privacy assimilation.

> *We will need that support from senior management to emphasize, it is of concern, great deal for the company. That message should be clear and loud till the bottom.* (Information architect, medium-scale US company (MSU-1))

The theme “tone at the top” highlights the importance of senior management participation. Even a recent Ernst & Young (2016) report highlights the “lack of tone from the top” as very important, leading to a gap in privacy awareness, which many respondents emphasized in its global survey.

SMS2: participants also highlighted the formulation of strategy for actual implementation.

> *[My] current organization has invested a lot in privacy and security framework both from competitive plus strategic view [sic]. Here you might be competing with competitors who are also playing with same data, but strategic envisioning is what probably data exploitation in future.* (Information architect, large-scale multi-national company (LSM-1))

Note that, as Shey et al. (2013) found, organizations can run into trouble when they think of preventing data leaks as a product instead of a function and do not have a holistic data-protection strategy in place.

SMS3: we found evidence for decision making support as key aspect of senior management.

> *I am trying to work on projects like analytics by reusing the data and get insights…. Because of privacy/security policies it becomes so difficult to do this work. Though we appreciate the need for security, sometimes getting a role or authorization to get a data is very difficult…. At some time, these two interests work against each other. That is where we need senior management support to understand what’s okay what is not okay as per company strategy.* (Information architect, large-scale multi-national company (LSM-6))

Industry reports show that, for accountability to be successful, leadership and management need to be aligned in terms of both priorities and culture when it came to managing privacy (Ernst & Young, 2016).

SMS4: establishing processes and standards was another important theme we identified. Our participants noted that it helped their organizations achieve compliance.

> *In my area, since it deals with customer and account information—our estimation also includes privacy, security aspects. Any added routines for new initiatives etc…. So process/budgeting is covered for that and had never issue with privacy & security.* (Vice president, large-scale multi-national company (LSM-5))

Based on the comment from the participants, it’s important to concentrate on the process and best practices from forums such as DSCI (2016c). These best practices ensure a significant level of detailing done while designing a process or deploying a technology solution for privacy implementation and creating a catalogue of processes that are deployed for privacy.

SMS5: participants distinctly identified providing resources and assigning responsibilities apart from establishing the standard processes.

> *From resource view, we need investment (from senior management) in terms of a dedicated data person in teams, Due diligence given for the data and also support for periodic re-visits of current frame works….* (Information Architect, large-scale multi-national company (LSM-1))

One industry report has highlighted that organizations focus more on people and their roles (data creators, owners, users, and auditors) to protect their data and limit employees to use the data appropriately (Shey et al., 2013).

5.2.2 Cultural Acceptability

Though one can quantify organizational culture, the level of quantification remains a question (Denison, 1996). In our study, we focused on "cultural acceptability" because almost all participants mentioned it in some way as a key factor in their organizations. Table 8 shows the key themes that pertain to it.

Table 8. Themes that Pertain to Cultural Acceptability

Tag	Themes	Label
CULT1	Company value and ethics	Y
CULT2	Dynamic / first with competitive actions	Y+
CULT3	Swift in changing formal rules and policies	Y
CULT4	Workforce in various geographic regions	Y++
CULT5	Focus on learning, awareness	Y+

CULT1: company values and ethics emerged as a key organizational influencer of privacy compliance.

> *Like quality is a practice and not a goal, similarly, privacy/security is a practice and not a one-time setup. So, the culture and values will come with the way how we approach it.* (Senior manager, large-scale multi-national company (LSM-8))

An Ernst & Young (2016) report has highlighted that, in a world where laws and regulations cannot keep pace with digital change, the onus of accountability shifts from regulators to organizations.

CULT2: participants also saw organizational culture in terms of "dynamic / first with competitive actions" as an influencing factor of organizational privacy compliance.

> *Culture of organization plays a far big role in investing what is the risk and compliance mechanism…. In my organization there is huge investment in that side—privacy/security and compliance measures.* (Senior manager, large-scale multi-national company (LSM-8))

Many participants mentioned Microsoft's initiative from a decade ago. To retain customers and keeping customer trust as their single greatest asset, Microsoft set out to make privacy deeply embedded into everything it did (product development, customer service, and operations) and allow customers to access their 10+ year track record on privacy (PwC, 2014).

CULT3: another theme concerned swiftness in changing formal rules and policies.

> *Off late with the change in the leadership, culture of the organization what we see is "breaches are treated with high criticality" and dedicated (account specific) HR policy on how these need to be handled.... Overall it's much opened and accepted that these kind of things do happen and seeking help from outside group to mitigate these risks than handling internally like years back.* (Senior manager, large-scale multi-national company (LSM-3))

A recent study published by Ernst & Young (2016) reports that many organizations have no formalized requirements and policies for using big data while addressing their privacy obligations. The reports were alarming and implied that organizations need to change formal rules and policies to comply with privacy requirements.

CULT4: participants also noted that a workforce in various geographic regions also makes privacy compliance a complex problem. However, they also saw this workforce diversity as facilitating quick learning in organizations.

> *In India, there is no proper/strong law to state about this privacy. Though section 43A, and amendment is there for IT law. But it doesn't talk as much as EU / US emphasis from legal point of view.* (Principal consultant, large-scale multi-national company (LSM-7))

Supporting the above view, a report from Ernst & Young (2016) has noted that "data flows across regions and continents, where different players are subject to different laws and users can access the services anywhere", which makes privacy compliance more complex.

CULT5: focus on learning and awareness emerged as another important theme.

> *Basic level training will avoid involuntary mistakes/gaps from privacy standpoint.* (Information architect, large-scale multi-national company (LSM-6))

According to Unilever's chief privacy officer, "we want to test the awareness level of our employees through surveying, to measure the effectiveness of our controls to raise awareness" (Ernst & Young, 2016).

5.2.3 Privacy Capability

In our study, "privacy capability"—similar to "IT capability" in the literature—evolved as a new concept (Bharadwaj, 2000). Further, research shows senior management want a security and privacy capability similar to their competitors (Johnson, 2009). Table 9 shows the key themes that pertain to privacy capability.

Table 9. Themes that Pertain to Privacy Capability

Tag	Themes	Label
PCAP1	Subject matter expertise (SME)	Y
PCAP2	Training opportunities (regular / on-demand basis)	Y++
PCAP3	Process planning and execution capability	Y++
PCAP4	Infrastructure capability	Y+
PCAP5	"Go to teams" for problem solving	Y+

PCAP1: participants mentioned the need for IT organizations to have people with both technical and subject matter expertise (SME).

> *We don't operate on sensitive information with more people. Its small group of trusted expert people and that's how we ensure data is private and secured.* (Director, small-scale Indian company (SSI-1))

Participants saw employees' technical expertise in IT organizations as very critical and important in the domain of privacy and security. In addition to technical skills, when it came to privacy, they mentioned employees needed subject matter expertise.

PCAP2: participants saw training opportunities (regular/on-demand) to enhance employees' skills as critical to enhance IT organizations' privacy capability.

> *Organizations should invest a lot to train their employees on data privacy and security…. How to deal with privacy and security has to be taken forward as we are gaining new business.... I wouldn't think that one size kind of an approach will fit considering the kind of data we handle. We should have trainings to people based on different kind of data they deal with.* (Information architect, small-scale U.S. company (SSU-1))

Insiders continue to cause a fair share of data breaches. According to Shey et al. (2013), inadvertent misuse of data from insiders topped the list of breach causes in 2013. As for why, Forrester notes that many organizations undervalued security-awareness training; thus, employees had access to data but did not understand data-use policies and used and stored data across a variety of devices (Shey et al., 2013).

PCAP3: process planning and execution capability also emerged as a theme.

> *Say, beyond these many transactions, we need to follow next certification process…. We have lately realized that we are growing business and the number of transactions are exceeding certain limit. That means it's time for next level of certification or process.* (Senior manager, medium-scale U.S. company (MSU-2))

As per the industry reports, after most serious breaches, organizations tend to update their technologies, improve their processes, and train their people. Multiple weaknesses across people, processes, and technology have triggered the worst organizational breaches. Based on the participant's comments, we can conclude that, apart from training people, IT organizations have to focus on the processes related to privacy preservation (PwC, 2014).

PCAP4: participants also considered IT organizations' infrastructure (hardware and software) to play a critical role in ensuring privacy compliance.

> *I worked with an organization where they do a "Key stroke capture mechanism"; if they match with critical and classified information, people would get alert.* (Information architect, small-scale U.S. company (SSU-1))

A recent market study reports that "use of encryption software will continue to increase to protect consumer privacy. Malware (malicious software) will increasingly hide behind encryption to evade detection by most enterprises that are struggling to balance employee privacy with attacks hiding behind encryption" (McLellan, 2015).

PCAP5: dedicated "go to teams" for problem solving also emerged an emerging theme.

> *My team will come to me whenever they identify a potential segment for privacy/security solutions that is need of the hour. We have some team of people who have domain expertise in that area. We form as a team and get best output out of the meeting…. So, we will approach as expert team to address security related needs coming and always will be priority. (*Director, small-scale Indian company (SSI-1))

Establishing dedicated information privacy office in organizations has been a trend in the last decade in Indian IT organizations. For example, Infosys announced its privacy and data protection office and chief data privacy officer in 2010 with an established governance structure (Infosys, 2011).

5.3 Organizational Assimilation

5.3.1 Business Strategy

Table 10 shows the themes that pertain to business strategy.

Table 10. Themes that Pertain to Business Strategy

Tag	Themes	Label
BST1	Enhancing company image	Y
BST2	Attracting new customers	Y+
BST3	Offering new, value added customer services	Y
BST4	Protecting company assets and intellectual property (IP)	Y
BST5	Enhancing effectiveness of data handling	Y

BST1: enhancing company image and reputation emerged as a theme.

> *Any privacy compromise will impact both the customer and organization. It's both in terms of revenues and reputation.* (Associate information officer, medium-scale U.S. company (MSU-4))

Indeed, Bracey (2012), who discusses organizations' seeking to build their reputation and image, states that organizations need to "be sensitive to privacy—with rampant identity theft and hacking, being aware of the sensitive nature of financial information is more important than ever". Further, in surveying executives about why they allocated funds to preserve privacy, Heidi Shey and Mak (2012) found that they did so to enhance their organizations' brands, to enhance public trust in their organizations, to meet regulatory compliance, and to reduce the risk of data breaches.

BST2: attracting new customers through differentiation in privacy practices also emerged as a theme.

> *There is a huge competitive advantage [sic]. The cost of not doing this is much much higher. If I am the customer sitting in USA and selecting a vendor from India, "Given all standard core parameters" the clear decision making influencer is "Vendor with proven data privacy & security capability".* (Director, small-scale Indian company (SSI-2))

Some of the observations we found also match executives' thoughts that strengthening the privacy practices in the organization would enable them to establish global presence in the market and get new business avenues (Heidi Shey & Mak, 2012).

BST3: some participants also mentioned the offering of new, value-added customer services as a key advantage of strengthening privacy practices.

> *We also add value added services to expand business. Privacy related are one of it.* (Director, small-scale Indian company (SSI-1))

Recent industry reports have highlighted that opportunities that digital technologies offer also come with an abundance of new, unforeseen risks and complexity when dealing with personal information (Ernst & Young, 2016). Approaches to mitigate these risks would also have a huge market. We also see that products such as Infosys Enterprise Data Privacy Suite (iEDPS) and TCS MasterCraft data privacy suite from large IT organizations have provided new, value-added services to their existing customers (Infosys, 2016b; TCS, 2016).

BST4: participants also mentioned protecting company assets and intellectual property (IP) as a reason to invest in privacy- and security-related measures in organizations.

> *As we are looking organizational privacy/security as foundation stones to IP, there is a definite strategic advantage with this IP. So, every company spends energy—money, resources to protect this.* (Senior manager, small-scale multi-national company (SSM-1))

Recent industry reports state that personally identifiable information (PII) and intellectual property (IP) are the types of data that cybercriminals or unwitting employees are most likely to compromise. For instance, Heidi Shey and Mak (2012) found that PII and IP topped the list of data types that individuals could potentially compromise.

BST5: Participants saw enhancing data handling effectiveness as a business strategy by leading organizations.

> *If we delve deeper into organizations, we have reports going on daily and also hourly basis. Information is going on how some of the risks are happening and organizations are dealing with it [sic]. So, this is real and important to enhance organizational effectiveness.* (Associate information officer, medium-scale U.S. company (MSU-4))

According to the chief privacy officer of Unilever, “when we embarked on a cross-enterprise, cross geography privacy program in 2013, we were interested not only in developing and implementing a robust global privacy program, but also in monitoring and measuring its success” (Ernst & Young, 2016). This quotation illustrates how organizations look forward to improving how effectively they handle data.

5.3.2 Organizational Activities

Table 11 lists themes that pertain to various activities in IT organizations that demand attention from the information privacy front as part of the organization’s activities.

Table 11. Themes that Pertain to Organizational Activities

Tag	Themes	Label
OAT1	Proposing and initiating new projects	Y+
OAT2	Development life cycle phases	Y+
OAT3	Audit phase	Y+
OAT4	Third party vendors	Y+
OAT5	Incident management	Y+

OAT1: the focus on privacy starts from proposing and initiating new projects.

> *Ten years back we have not seen much emphasis on privacy/security. If we see a business requirement document, security might be in the last item. But these days, one of the first point will be privacy/security for new project implementations—with spelled requirements.* (Information architect, small-scale U.S. company (SSU-1))

Proposing and initiating new projects are critical stages in the IT industry. Among the vendor-selection criteria, participants considered information-privacy capabilities as an important parameter. Indeed, many IT organizations have built in-house frameworks such as enterprise information security (EIS) by Wipro and business risk intelligence and compliance solutions (BRiCS) by HCL, which highlight the capabilities needed at the proposal phase (HCL, 2016; Wipro, 2016).

OAT2: software development lifecycle (SDLC) processes cover various phases of software development in IT organizations. Participants mentioned that the organizations paid important attention to privacy throughout these lifecycle processes.

> *At design phase we have some ambiguity on which role is eligible to see sensitive information. After multiple discussions with experts, we defined the roles for accessing the information.* (Information architect, medium-scale multi-national company (MSM-1))

Further, privacy by design (PbD) policy states that, at a very early stage, privacy professionals need to be involved in the development of new features and apps. In addition, some of the tools (e.g., MasterCraft Data Privacy Suite) that IT organizations such as TCS showcase highlight how one can create a secured test environment and standardized test data-management process. Frameworks such as trusted application development and maintenance (ADM) from Infosys highlight the presence of privacy and security focus at every stage of the software-development process (Infosys, 2016a; TCS, 2016).

OAT3: audit emerged as a key phase in compliance- and assurance-related activities.

> *Recently customers came back asking this data could reside in your desktops/laptops on network [sic]. They were asking access to these networks for audits. So, this is very tricky situation – as its opening doors to one vendor's infrastructure for audit purposes.* (Senior manager, large-scale multi-national company (LSM-3))

Standards such as ISO 27001:2013 mandate audits related to security and cover some of the privacy aspects as well. In 2011, AICPA issued a new framework for controls in a service organization relevant to security, availability, processing integrity, confidentiality, and privacy (SOC 2). They enable service providers to be transparent and accountable to their clients.

OAT4: participants also highlighted aspects related to third party vendors.

> *We as company follow the process of privacy & security, also work with many vendors (30-40 vendors) in IT companies [sic]. If we deal with vendors to manage with some part of business, then you along with vendors need to follow the privacy and security practices.* (Senior manager, medium-scale U.S. company (MSU-2))

According to Ernst & Young (2016), one-third of the respondents in their survey indicated that their organizations did not control what vendors did with the personal information they had access to. At the same time, Shey et al. (2013) found that inadvertent misuse by business partner/third-party supplier was the most common way in which a data breaches have occurred.

OAT5: participants also mentioned that their organizations have paid attention to incident management-related items to effectively manage privacy.

> *There was a demo…. [An] employee was running short of time, he sent document across his personal ID. This was brought to my attention in compliance team asking what could be breach to customer's data…. It comes with high priority.... I noticed there is no wrong intent, but vulnerability we are exercising is high…. As a leader, I better be serious than sorry. I revoked the access and have a process in place. It's to do with additional investment and also efforts—collaboration with security team—post a potential incident.* (Senior manager, large-scale multi-national company (LSM-8))

Incident management procedures are also a key part of ISO standards (ISO-IEC-27035, 2011). The White House (2015) has released a draft of the proposed Consumer Privacy Bill of Rights (2015) that requires organizations to disclose data breaches in a timely manner to mitigate the risk of identity theft. Also, the DSCI has included best practices related to privacy monitoring and incident management as a part of its privacy framework (DSCI, 2016c).

6 Propositions and Emergent Theoretical Model

Based on analyzing the data gathered from our interviews and reviewing the literature, we develop a set of propositions to show the interplay between external influencing forces, internal organizational parameters, and assimilation. These propositions constitute a part of this research's contribution. In Sections 6.1 to 6.4, we present the number of statements related to a specific theme (for supporting a proposition) as "Theme (#)". For example, government, regulatory influence (3) means we found three supportive statements for the "government, regulatory influence" theme in that context.

6.1 Institutional Forces and Senior Management

We analyzed the interplay between the external forces of influence and senior management support in achieving assimilation based on our interview data. We found that senior management plays a mediating role between external forces and organizational assimilation of privacy.

6.1.1 Coercive

Senior management support plays a role in dealing with mandatory and legal forces that impact an organization. The participants echoed that the themes related to government/regulatory influence (3), competitive conditions (3), and customer expectations (2) positively influenced senior management support and participation.

> *Sometimes the requirements might come from senior management or IT managers (mid-level). We usually need support from senior management, but it's easy to get support is it's related to data privacy & security as it's a "must rule" and "not nice to have".* (Senior manager, medium-scale U.S. company (MSU-2))

> *The current organization has invested a lot in privacy and security framework both from competitive plus strategic view. Here you might be competing with competitors who are also playing with same data, but Strategic in envisioning what probably data exploitation in future.* (Information architect, large-scale multi-national company (LSM-1))

Organizational studies related to security also suggest that coercive pressure from business partners and pressure from regulations positively influence investment in information security control resources (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Drawing on these consistent findings, we posit:

P1: Institutional forces that pertain to information privacy positively influence senior management support.

P1A: Coercive forces that pertain to information privacy positively influence senior management support.

6.1.2 Mimetic

Senior management support enables organizations to respond to the uncertainties and risks that impact them. Our data analysis suggests that the themes related to competitors' benefits or failures (2), competitors' perception in industry (1), and uncertainty while handling adoption of new technologies (3) influence senior management. Overall, we found that learning from peers, especially the challenges they face in privacy matters, is a very important force, and senior management involvement serves to translate the privacy policy into strategic initiatives.

> *If other organizations are investing significantly and current organization is not investing, focusing on strategic way, obviously there will be some pressure.* (Information architect, large-scale multi-national company (LSM-1))

> *If we can prove in the market that we have lot of security compliance, ethics and the privacy rules enabled to the highest level—it definitely keeps us ahead in market [sic]. Showcasing "how we value customer data holds a very important role. Lot of importance is attached to privacy/security. Lots of initiatives are running on this front…. I see privacy/security is 40-50% differentiating factor in any deal.* (Senior manager, large-scale multi-national company (LSM-8))

The above statements serve as examples for learning from peers (a mimetic force) and the role of senior management involvement in responding to the mimetic force and providing strategic direction to privacy practice. Further, unlike Cavusoglu et al.'s (2015) findings, we found many participants who emphasized the impact of mimetic pressure compared to normative pressures on senior management. Our findings are similar to the mimetic influences related to ERP and information system security studies (Liang et al., 2007; Tejay & Barton, 2013). These studies report that mimetic mechanisms could either change beliefs or directly influence action without affecting beliefs of senior management. Thus, we posit:

P1B: Mimetic forces that pertain to information privacy positively influence senior management support.

6.1.3 Normative

Participants noted that senior management support to "sponsor industry forums" facilitates learning and enhances organizational activities to ensure privacy compliance. The participants noted that the themes related to participating in conferences and forums (1), the value added from external consultants (1), and availability of dedicated and certified privacy experts (2) influenced senior management.

> *I expect unconditional support from senior management to implement the data privacy and security. Like other areas you can't be reactive in this case. You need to proactive and can't wait for something to happen to fix it…. You need to ahead of game, aware of privacy/security issues with new technologies. This requires lot of budget and support.* (Information architect, small-scale U.S. company (SSU-1))

> *Privacy is an ocean. Organizations don't know where to start and where to draw line. Definitely external help they (organization) seek with privacy, but may not be for security…. Mainly, they share complexity of laws and regulations. They don't want to be on wrong side of law.* (Executive director, large-scale multi-national company (LSM-9))

Prior information system security studies have reported low levels of normative influences on senior management (Tejay & Barton, 2013). Our findings provide similar insights in that we found few statements related to normative forces' influencing senior management. Further, we noted that normative pressures dominate in motivating organizational investments (senior management) in information security control resources (Cavusoglu et al., 2015). Thus, we posit:

P1C: Normative forces that pertain to information privacy positively influence senior management support.

6.2 Mediating Role of Senior Management

Our analysis showed that all themes identified under the "senior management support" construct (i.e., tone at the top (4), formulates a strategy (2), decision making support (2), establishes processes and standards (3), and provides the resources and assigns responsibilities (4)) points to senior management support's influence on privacy assimilation. Senior management support emerged as a significant mediating variable in the assimilation of privacy in response to external institutional forces.

> *It's the tone at the top matter.... How they posture and how they communicate to others that this is important exercise and people have to co-operate here. Unless it comes heavily from top, people take it lightly.... Senior management has to practice and evangelize it.* (Executive director, large-scale multi-national company (LSM-9))

> *Management put lot of practices in place and they hold the responsible of data (both internal / customer data). Lot of in-built tracking systems were in place…. Several mechanisms in which we track it…. Manager, super manager including HR manger—all getting into place. They review the case and take corrective action.* (Senior manager, large-scale multi-national company (LSM-8))

Previous studies also report a significant relationship between senior management and IT assimilation. For example, Hsu et al. (2012) conceptualize information security management as an administrative innovation. Further, Purvis, Sambamurthy, and Zmud (2001) found management championship (i.e., the extent to which an organization's senior management advocates the use of an innovation) to impact assimilation. In the broader IT context, Armstrong and Sambamurthy (1999) report that the business and strategic IT knowledge of senior leadership teams significantly enhances a firm's IT assimilation. Other studies also report that senior management championship in terms of managerial belief and participation positively influences the extent of organizational assimilation (Chatterjee et al., 2002; Liang et al., 2007; Tejay & Barton, 2013). Liang et al. (2007) extend the institutional model of Teo et al. (2003) by examining the mediating role of senior management between institutional forces and enterprise system assimilation in organizations. Tejay and Barton (2013) empirically investigate how external influences motivate senior management to commit to information system security by examining the mediating role of senior management. In light of the qualitative evidence of senior management's mediating role that emerges from our analysis and based on support from prior literature, we posit.

P2: Greater support of senior management results in higher levels of information privacy assimilation.

6.3 Moderating Role of Cultural Acceptability

As part of this qualitative study, cultural acceptability emerged as a moderating variable that influences the relationship of institutional (normative and mimetic) forces on privacy assimilation.

From analyzing the data, we could see that the theme related to company value and ethics (5) positively influences the normative forces (formal education, participation in external forums, and external consultant inputs) and results in privacy assimilation. Also, cultural aspects such as swift in changing formal rules and policies (1) and focus on learning, awareness (1) helps organizations to learn about privacy practices from external conferences and forums and, thereby, assimilate privacy practices.

> *Regulations are a guidelines to meet. Beyond which it's to organizations to better in them. On this basic guidelines, the organization based on their culture need to build on the top of the regulation guidelines. Organizations should think beyond regulations.* (Senior manager, small-scale multi-national company (SSM-1))

> *If you take some of the Indian companies, though there is no government law, still they are trying to implement the privacy and build some ethical standards. Here it's like a healthy competition.* (Principal consultant, large-scale multi-national company (LSM-7))

The literature indicates that culture shapes and guides behavior via shared values among individuals (Smircich, 1983). Further, researchers have argued that security policies must be instilled into organizational culture to be effective (Von Solms & Von Solms, 2004). Information security cultures have been studied across various professions in organizations (Ramachandran, Rao, Goles, & Dhillon, 2013), and a recent study has reported that the higher the cultural acceptability of innovation, the stronger the relationship between institutional influences and assimilation (Hsu et al., 2012). Thus, we posit.

> **P3A:** Greater cultural acceptability in an organization results in a stronger positive relationship between normative forces and privacy assimilation.

Here, we found slightly different results compared to Hsu et al. (2012) in terms of the influence of normative forces. In our study, which we conducted predominantly in the Indian context, normative influence had a greater role than regulatory authorities (unlike South Korea).

We also found that the themes dynamic / first with competitive actions (1) and swift in changing formal rules and policies (1) positively enable mimetic forces (adoption by successful peer and following successful peer), which results in privacy assimilation.

> *Technology goes forward first and privacy will catch up.... When we built AML application on Teradata, we just built it and then fix privacy issues around it. Hadoop is coming next. Though we are talking about privacy, we don't know how to do that.... If someone comes with best practice—others to follow*. (Vice president, large-scale multi-national company (LSM-5))

> *Innovations are not organization bound. If we see some best security/privacy standards…, organizations should embrace it and learn from the peers.* (Senior manager, large-scale multi-national company (LSM-8))

The above statements highlight that an organization's cultural acceptability affects whether it assimilates best practices from another organization (a peer). Based on the consistency of these observations with previous studies (Hsu et al., 2012; Ramachandran et al., 2013; Smircich, 1983; Von Solms & Von Solms, 2004), we posit.

> **P3B:** Greater cultural acceptability in an organization results in a stronger positive relationship between mimetic forces and privacy assimilation.

6.4 Moderating Role of Privacy Capability

Privacy-related capability emerged as another moderating variable in strengthening privacy assimilation in response to coercive and normative forces. From analyzing our data, we noticed that several themes that related to privacy capability such as process planning and execution (2), infrastructure (2), and known contacts for problem solving (1) helped to moderate the effect of mandatory forces such as regulatory influence and contracts on information privacy assimilation.

> *Whenever we encounter new customers OR existing customers for a new project…. We consider privacy/security aspects. As IT companies works across customers, so these conflicts*

> *will come. We will resolve these with the help of contract team (By looking at Master Service Contract and Legal help). (Director, small-scale Indian company (SSI-2))*
>
> *Within our organization, we have a strong compliance team that do audits for every application. They ensure any of the confidential information is not leaked out and also ensure customer information is kept confidential. So, we have this capability with support from internal teams.* (Information architect, medium-scale multi-national company (MSM-1))

Previous studies have shown that organizations that maintain a strong security capability but do not focus on privacy itself could suffer significant impact (Choobineh, Dhillon, Grimaila, & Rees, 2007). Under the privacy capability construct, certain concepts related to learning capabilities of an organization show some similarities of this construct with that of absorptive capacity (ACAP). Prior research has shown that IT-related assimilation in organizations is not only a response to external institutional pressures but also subject to moderation by an organization's absorptive capacity (Liang et al., 2007; Saraf, Liang, Xue, & Hu, 2006, 2013). Thus, we posit:

P4A: Greater privacy capability in an organization results in a stronger positive relationship between coercive forces and privacy assimilation.

This observation differs slightly compared to Saraf et al. (2013) and highlights the influence of coercive forces in the case of information privacy. In the Indian context, privacy capability moderated the coercive pressure in that customer expectations (3).

Privacy-related capability also emerged as having a moderating role in response to normative forces. We found several themes that facilitate normative forces (norms through education, conferences, and privacy experts) to differentially impact privacy assimilation: subject matter expert support (1), training opportunities for employees (3), infrastructure capability (2), and known contacts for problem solving (3).

> *More the employees know about privacy/security…the more compliance. It's achieved through training. "Why we need to do, how we need to do—the way". In our organization, we have every year we have to get certified on privacy & security…. We keep tab on market trends. Have technologies in place like masking to complement audit findings and early closure.* (Vice president, large-scale multi-national company (LSM-5))
>
> *I was part of account setup for big auditing industry. This auditing company has data coming from multiple other worldwide organizations. When we are setting up this data, rules around who can see the data…. We involved the "privacy, security and risk management team" of my organization…. Got best practices to be followed before we negotiate with customer.* (Senior manager, large-scale multi-national company (LSM-8))

The above quotes represent privacy's capability to moderate the effect of normative forces on privacy assimilation. Indeed, Saraf et al. (2013) show that absorptive capacity moderates the effect of normative forces on assimilation, which is very similar to our finding. Thus, we posit:

P4B: Greater privacy capability in an organization results in a stronger positive relationship between normative forces and privacy assimilation.

7 Discussion

Figure 2 presents our model and all propositions. With this study, we contribute to identifying relevant constructs and positing potential relationships that pertain to information privacy assimilation in organizations. We found that business strategy and organizational activities reflect the level of importance of information privacy in an organization. This finding is similar to assimilation strategies and value chain activities as Armstrong and Sambamurthy (1999) and Chatterjee et al. (2002) highlight in their studies on IT assimilation. We also found that "enhancing company image" (BST1), "attracting new customers" (BST2), and "offering new, value-added customer services" (BST3) are consistent with constructs and measures that Johnson (2009) and Cavusoglu et al. (2015) provide.

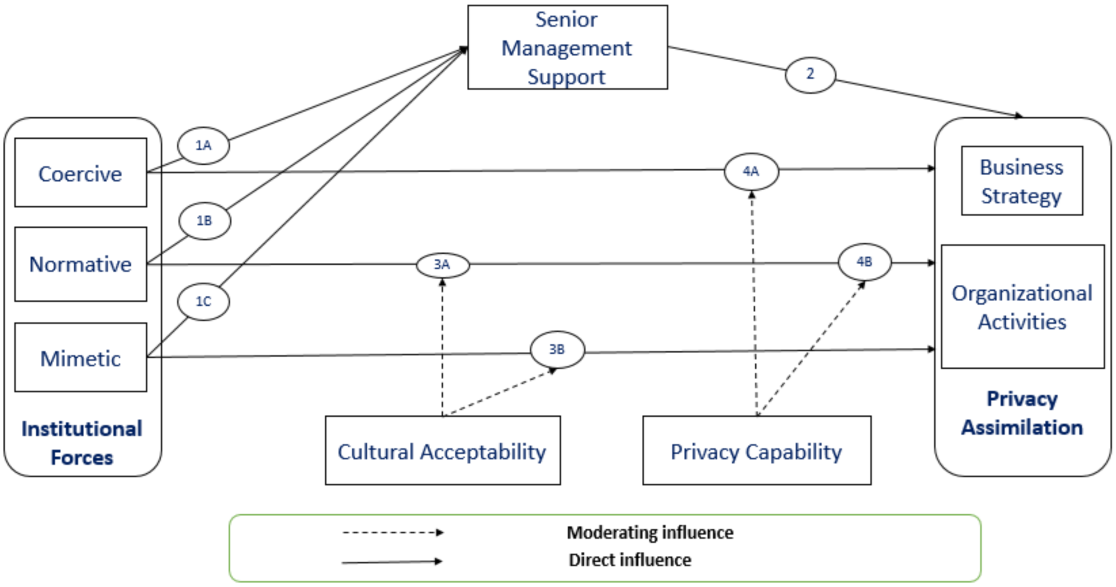

Figure 2. Privacy Assimilation in IT Organizations: Proposed Model

We considered institutional forces, which are coercive, normative, and mimetic in nature. Most participants emphasized the influence of government and regulations (COER1) on privacy assimilation, which also aligns with Cavusoglu et al. (2015), Liang et al. (2007), and Tejay and Barton (2013). Industry associations' encouragement (COER2) emerged as a strong theme with few participants, who highlighted its specific influence in the Indian context. Liang et al. (2007) and Tejay and Barton (2013) also touch on this theme under the coercive forces category. They also highlight the theme related to competitive conditions (COER3).

Surprisingly, normative forces did not receive strong support (less than one-third of our participants mentioned it) in our study contrary to prior studies. The themes related to formal education (NORM1), participation in forums (NORM2), and journals subscriptions (NORM3) as highlighted by Liang et al. (2007), Tejay and Barton (2013), and Teo et al. (2003) did not have the anticipated relevance in our findings. The presence of external consultants (NORM4) is in line with the work of Appari et al. (2009). Furthermore, and specific to the Indian context, the theme (NORM5) "dedicated privacy certified employees" emerged as an important influencing factor for privacy assimilation and compliance—similar to results that Bjorck (2004) and Johnson (2009) report.

We found a mixed result for mimetic forces. Though we found good support for the influence of peers, many participants also mentioned the non-existence of peer pressure. The expression of "mimetic" views as "normative" could explain why as earlier studies have observed (Hu et al., 2007).

Our findings show that senior management support is a key internal factor that mediates the impact of external forces on privacy assimilation in organizations. We did not differentiate between senior management beliefs versus participation/support unlike in prior literature (Chatterjee et al., 2002; Liang et al., 2007; Tejay & Barton, 2013).

Cultural acceptability also emerged as another influencing factor for privacy assimilation. In our study, most of the participants highlighted the workforce's geographic origin as an influencing factor. Prior literature has also used themes such as company value and ethics that we identified in our study (Chan & Greenaway, 2005; Culnan & Williams, 2009; Smith, 1993). For example, Altman (1977) and Newell (1998) discuss the themes of workforce in various geographic regions (CULT4) and focus on learning, awareness (CULT5) under the broad construct of culture. Themes such as "dynamic, first with competitive actions" and "swift in changing formal rules and policies" had a moderating effect in our study unlike in Gallivan (2001) and Hsu et al. (2012).

The privacy capability construct that emerged from our study has some similarity to absorptive capacity that prior literature has discussed (Cohen & Levinthal, 1990; Saraf et al., 2006, 2013). Our themes “training opportunities, regular basis, on-demand basis” (PCAP2), “process planning and execution capability” (PCAP3), and “go to teams for problem solving” (PCAP5) have been elaborated in the work of Liang et al. (2007), Saraf et al. (2013) and Tejay and Barton (2013). We also found that higher levels of privacy capability lead to a more positive influence of coercive and normative forces on privacy assimilation.

8 Conclusion

8.1 Contributions

In this paper, we develop a conceptual model to understand information privacy in organizations and validate the model analytically. We contribute to the literature primarily by developing a theory for information privacy assimilation. To do so, we build on concepts derived from neo-institutional theory using primary data collected through case studies. As information privacy stands out as a distinctly different phenomenon that affects organizations at a strategic level, we add to the body of knowledge that concerns information privacy. In particular, we make four important contributions.

First, we address information privacy as a separate phenomenon from data security and develop conceptual elements and relationships specific to information privacy. Several studies have mixed privacy with security, and some have addressed security separately at organizational level (Hu et al., 2007; Pavlou, 2011; Smith, et al., 2011). However, extent literature has not adequately developed the interplay of external and internal factors that help evolve information privacy-related strategies in organizations. We address this gap, which is critical to organizations in the information age.

Second, we followed a novel methodological approach in privacy studies that is most suitable for building a theory. We followed a combination of inductive (qualitative data analysis) and deductive (a priori framework) approaches. We employed a multi-case, multi-site approach with a rigorous data-analysis procedure (Davis & Eisenhardt, 2011). This emergent theory from multiple-case research is typically more analytically generalizable and better grounded than the theory from a single-case study (Davis et al., 2007). Further, we extensively triangulated our data by corroborating findings from interview data with observations from secondary sources such as industry reports and trade and academic journals. Such data triangulation strengthens the validity of the emergent theory.

Third, we produce a theory that will guide future research for theory testing (Colquitt & Zapata-Phelan, 2007). The identified constructs and inter-relationships are specific to organizational information privacy. For example, “privacy capability” evolved as a new construct from our significantly re-conceptualizing an existing IT-capability/absorptive capacity construct. Similarly, the new role and relationship of “culture as moderating factor” specific to the context of privacy evolved from our analysis.

Fourth, our findings have implications for practice within the constraints of a qualitative study. For example, some of the themes that evolved from the study serve to enhance a company’s image with strong privacy policies as a market differentiator. The right-hand side of the present model goes beyond compliance and practices to assimilation, which adapts the subconstructs strategy and activity. In contrast, most existing studies have focused on the awareness and enforcement of security policies (Hu et al., 2007; Kam, Katarattanakul, & Gogolin, 2013). Senior management emerged as a mediator between external forces and information privacy assimilation. Such insights would be useful for policy makers. Our findings also enable senior managers to identify and respond to institutional pressures by focusing on appropriate factors in their organizations and, thus, help them to invest in the right focus areas. Another benefit of the study for practice is in developing a better understanding of which aspects of privacy goes in line with security and which aspects need distinct attention compared to security.

8.2 Limitations and Future Study

Notwithstanding the insights we found, our study has some limitations. We followed a qualitative approach suitable for theory building and, as such, we cannot generalize the findings without further support from a quantitative study for testing and validation. Though our study helps to identify appropriate privacy measures from an IT organization’s view point, we did not focus on the business domain’s (healthcare, banking etc.,) influence. Finally, our sample includes only U.S. organizations with operations that expand to India and Indian organizations that predominantly work win US regions. Lack of organizations from the European region in our sample geographically limits the study.

Future work should develop our scale and instrument, administer the survey to large samples with different geographic regions and types of industries, and empirically validate the proposed research model. Doing so would yield statistically significant and generalizable results that managers would find useful.

Acknowledgments

We thank all the industry participants in the study for their help and cooperation. We owe a special debt of gratitude to two independent coders Jefrin and Bhaskar for their painstaking support in coding. We thank the two anonymous reviewers for their thoughtful comments and suggestions, which have led to a higher quality paper. We thank the associate editor for the clear directions concerning the revisions needed. We also thank the chief editor for the thoughtful guidance given. This research was supported by Infosys higher education policy partnership with IIT Madras. Dr. Sugumaran's research was supported by a 2017 School of Business Administration Spring/Summer Research Fellowship from Oakland University

References

Ackerman, M. S. (2004). Privacy in pervasive environments: Next generation labeling protocols. *Personal and Ubiquitous Computing, 8*(6), 430-439.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the International Conference on Information Systems.*

Ali, H., & Birley, S. (1999). Integrating deductive and inductive approaches in a study of new ventures and customer perceived risk. *Qualitative Market Research: An International Journal, 2*(2), 103-110.

Altman, I. (1977). Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66-84.

Appari, A., Johnson, M. E., & Anthony, D. L. (2009). HIPAA compliance: An institutional theory perspective. In *Proceedings of the Americas Conference on Information Systems.*

Armstrong, C. P., & Sambamurthy, V. (1999). Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Information Systems Research, 10*(4), 304-327.

Attili, V., Mathew, S., & Sugumaran, V. (2015). Information privacy assimilation in organizations–a neo institutional approach. In *Proceedings of the Americas Conference on Information Systems.*

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1042.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, *24*(1), 169-196.

Bjorck, F. (2004). *Institutional theory: A new perspective for research into IS/IT security in organisations.* In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*.

Bracey, L. (2012). The importance of business reputation. *Business in Focus Magazine*. Retrieved from http://www.businessinfocusmagazine.com/2012/10/the-importance-of-business-reputation/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400.

Chan, Y. E., Culnan, M. J., Greenaway, K., Laden, G., Levin, T., & Smith, H. J. (2005). Information privacy: Management, marketplace, and legal challenges. *Communications of the Association for Information Systems, 16*, 270-298.

Chan, Y. E., & Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems, 6*(6), 171-198.

Chatterjee, D., Grewal, R., & Sambamurthy, V. (2002). Shaping up for e-commerce: Institutional enablers of the organizational assimilation of Web technologies. *MIS Quarterly*, *26*(2), 65-89.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems, 20*, 958- 971.

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, *35*(1), 128-152.

Colquitt, J. A., & Zapata-Phelan, C. P. (2007). Trends in theory building and theory testing: A five-decade study of the academy of management journal. *Academy of Management Journal, 50*(6), 1281-1303.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673-687.

Davis, J. P., & Eisenhardt, K. M. (2011). Rotating leadership and collaborative innovation recombination processes in symbiotic relationships. *Administrative Science Quarterly, 56*(2), 159-201.

Davis, J. P., Eisenhardt, K. M., & Bingham, C. B. (2007). Developing theory through simulation methods. *Academy of Management Review, 32*(2), 480-499.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *Academy of Management Review, 21*(3), 619-654.

Dibbern, J., Winkler, J., & Heinzl, A. (2008). Explaining variations in client extra costs between software projects offshored to India. *MIS Quarterly, 32*(2), 333-366.

DiMaggio, P., & Powell, W. W. (1982). *The iron cage revisited: Conformity and diversity in organizational fields* (vol. 52). Institution for Social and Policy Studies, Yale University.

DiMaggio, P. J., & Powell, W. W. (1991). *The new institutionalism in organizational analysis* (vol. 17). Chicago, IL: University of Chicago Press.

Dissent. (2016). *US jury fines Tata Consultancy Services $940m for healthcare software "theft".* Retrieved from https://www.databreaches.net/us-jury-fines-tata-consultancy-services-940m-for-healthcare-software-theft/

DSCI. (2016a). *Certifications: DSCI certified privacy professional (DCPP).* Retrieved from https://www.dsci.in/taxonomypage/1287

DSCI. (2016b). *Data protection: Organization roles.* Retrieved from https://www.dsci.in/

DSCI. (2016c). *DSCI Privacy best practices: Privacy monitoring and incident management.* Retrieved from https://www.dsci.in/taxonomypage/101

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25-32.

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Ernst & Young. (2012). *Privacy trends 2012—the case for growing accountability*. Retrieved from http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2012_The_case_for_growing_accountability/$FILE/Insights%20on%20IT%20risk%20Privacy%20trends%202012.pdf

Ernst & Young. (2015). *Creating trust in the digital world: EY's global information security survey*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

Ernst & Young. (2016). *Privacy trends 2016—can privacy really be protected anymore?* Retrieved from http://www.ey.com/gl/en/services/advisory/ey-privacy-trends-2016

Fichman, R. G. (2000). The diffusion and assimilation of information technology innovations. In R. W. Zmud (Ed.), *Framing the domains of IT management* (pp. 105-128). Cincinnati, OH: Pinnaflex Educational Resources.

Fichman, R. G., & Kemerer, C. F. (1997). The assimilation of software process innovations: An organizational learning perspective. *Management Science, 43*(10), 1345-1363.

Gallagher, K. P., Zhang, X., & Gallagher, V. C. (2012). Assimilation of security-related policies in US firms: An empirical study of Web assimilation and related knowledge as antecedents. In *Proceedings of the 45th Hawaii International Conference System Science.*

Gallivan, M. J. (2001). Organizational adoption and assimilation of complex technological innovations: Development and application of a new framework. *ACM SIGMIS Database, 32*(3), 51-85.

Gilbert, C. G. (2005). Unbundling the structure of inertia: Resource versus routine rigidity. *Academy of Management Journal, 48*(5), 741-763.

Graebner, M. E. (2004). Momentum and serendipity: How acquired leaders create value in the integration of technology firms. *Strategic Management Journal, 25*(8-9), 751-777.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information Systems Journal, 25*(6), 579-606.

Gupta, M. (2014). *Handbook of research on emerging developments in data privacy*. Hershey, PA: IGI Global.

Hachamovitch, D. (2012). *Google bypassing user privacy settings. Microsoft.* Retrieved from https://blogs.msdn.microsoft.com/ie/2012/02/20/google-bypassing-user-privacy-settings/

Hansell, S. (2008). *Is Google violating a California privacy law? The New York Times.* Retrieved from http://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law/

Harrison, A. (2002), Case study research. In D. Partington (Ed.), *Essential skills for management research* (pp. 158-180). London: Sage.

HCL. (2016). *Business risk intelligence & compliance solutions.* Retrieved from http://www.hcltech.com/financial-services/risk-and-compliance-management

Heidi Shey, S. B., & Mak, K. (2012). *Understand the state of data security and privacy: 2012 to 2013.* Forrester Research.

Holsti, O. R. (1969). *Content analysis for the social sciences and humanities*. Reading, MA: Longman Higher Education.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research, 23*(3), 918-939.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153-172.

IAAP. (2014). *Benchmarking privacy management and investments of the Fortune 1000.* Retrieved from https://privacyassociation.org/resources/article/benchmarking-privacy-management-and-investments-of-the-fortune-1000-2/

Infosys. (2011). *Infosys sustainability report 2010-2011.* Retrieved from https://www.infosys.com/sustainability/Documents/infosys-sustainability-report-1011.pdf

Infosys. (2016a). *Trusted (secure) ADM Infosys*. Retrieved from www.infosys.com/richmedia/infosys-labs-areas.swf

Infosys. (2016b). *Infosys enterprise data privacy suite.* Retrieved from https://www.infosys.com/products-and-platforms/maskit/

International Association of Privacy Professionals. (2012). *Privacy professionals role, function and salary survey.* Retrieved from https://iapp.org/media/pdf/knowledge_center/IAPP_Salary_Survey_2012.pdf

International Association of Privacy Professionals. (2016). *IAPP certification*. Retrieved from https://iapp.org/certify/

ISACA. (2012). *Top ten big data security and privacy challenges.* Retrieved from https://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf

ISO-IEC-27035. (2011*). Information technology—security techniques—information security incident management*. Retrieved from https://www.iso.org/standard/44379.html

John, T., & Ian, F. (2016). *Privacy, the competitive advantage*. Retrieved from http://www.theprivacyadvantage.com/

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a Delphi study. *Journal of Information Privacy and Security, 5*(1), 3-27.

Kam, H.-J., Katerattanakul, P., & Gogolin, G. (2013). *A Cross industry study: Differences in information security policy compliance between the banking industry and higher education*. In *Proceedings of the 34th International Conference on Information Systems.*

Kim, D. J., Yim, M.-S., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: An investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems, 25*(3), 252-273.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59-87.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28*(2), 102-129.

McLellan, C. (2015). Cybersecurity in 2015: What to expect*. ZDNet.* Retrieved from http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

Meehan, T., Vermeer, C., & Windsor, C. (2000). Patients' perceptions of seclusion: A qualitative investigation. *Journal of Advanced Nursing, 31*(2), 370-377.

Meyer, A. D., & Goes, J. B. (1988). Organizational assimilation of innovations: A multilevel contextual analysis. *Academy of Management Journal, 31*(4), 897-923.

Newell, P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology, 18*(4), 357-371.

NITRD Program. (2013). *Privacy research panel, 2013 IEEE symposium on security and privacy.* Retrieved from https://www.youtube.com/watch?v=fzkAtfx6W-g

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Poosarla, S. (2016). Emerging digital landscape pushing data privacy quest. *EGov*. Retrieved from http://egov.eletsonline.com/2016/05/emerging-digital-landscape-pushing-data-privacy-quest/

Powell, W. W., & DiMaggio, P. J. (Eds.). (2012). *The new institutionalism in organizational analysis*. Chicago: University of Chicago Press.

Privacy Rights Clearinghouse. (2017). *Privacy data breaches.* Retrieved from https://www.privacyrights.org/data-breach

Purvis, R. L., Sambamurthy, V., & Zmud, R. W. (2001). The assimilation of knowledge platforms in organizations: An empirical investigation. *Organization Science, 12*(2), 117-135.

PwC. (2014). *10 Minutes on data privacy.* Retrieved from https://www.pwc.com/us/en/10minutes/assets/pwc-data-privacy.pdf

Ramachandran, S., Rao, V. S. C., Goles, T., & Dhillon, G. (2013). Variations in information security cultures across professions: A qualitative study. *Communications of the Association for Information Systems, 33*, 163-204.

Reicher, S., & Taylor, S. (2005). Similarities and differences between traditions. *Psychologist, 18*(9), 547-549.

Robey, D., & Boudreau, M.-C. (1999). Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. *Information Systems Research, 10*(2), 167-185.

Saraf, N., Liang, H., Xue, Y., & Hu, Q. (2006). The moderating role of absorptive capacity in the assimilation of enterprise information systems. In *Proceedings of the Americas Conference on Information Systems.*

Saraf, N., Liang, H., Xue, Y., & Hu, Q. (2013). How does organizational absorptive capacity matter in the assimilation of enterprise information systems? *Information Systems Journal, 23*(3), 245-267.

Shey, H., Mak, K., Balaouras, S., & Luu, B. (2013). Understand the state of data security and privacy: 2013 to 2014. *Forrester Research.* Retrieved from https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2013+To+2014/-/E-RES82021

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, *28*(3), 339-358.

Smith, H. J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*(12), 104-122.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Stone, B., & Stelter, B. (2009). Facebook withdraws changes in data use. *The New York Times*. Retrieved from http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html

TCS. (2016). *Data privacy suite.* Retrieved from http://www.tcs.com/offerings/mastercraft/test_data_environment_management_suite/Pages/default.aspx

Tejay, G. P., & Barton, K. A. (2013). *Information system security commitment: A pilot study of external influences on senior management.* In *Proceedings of the 46th Hawaii International Conference the System Sciences.*

Teo, H.-H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt inter organizational linkages: An institutional perspective. *MIS Quarterly*, *27*(1), 19-49.

TRUSTe. (2015). *Privacy priorities in 2015—privacy investment on the rise?* Retrieved from http://www.truste.com/blog/2014/12/11/privacy-priorities-in-2015/

Tuckett, A. G. (2005). Applying thematic analysis theory to practice: A researcher's experience. *Contemporary Nurse, 19*(1-2), 75-87.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

White House. (2015). *Administration discussion draft: Consumer privacy bill of rights act of 2015*. Retrieved from https://www.democraticmedia.org/sites/default/files/field/public/2015/draft_consumer_privacy_bill_of_rights_act.pdf

Wipro. (2016). *Enterprise information security.* Retrieved from http://www.wipro.com/india/products/infrastructure-technology-solutions/enterprise-information-security/

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the International Conference on Information Systems.*

Yin, R. K. (2013). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Zott, C., & Huy, Q. N. (2007). How entrepreneurs use symbolic management to acquire resources. *Administrative Science Quarterly, 52*(1), 70-105.

Appendix A: Interview Guidelines

1. What are the factors that motivate organizations to invest in data privacy?
2. How you see the difference between privacy and security in your business (unit) context?
3. How you foresee the perceived risks and actual risks of not being compliant with data privacy?
4. What do you think about strategic / competitive advantages – Ability of the firm to differentiate (In Global Delivery Model)
5. What kind of support from senior management is required for data privacy?
6. What kind of internal capability you possesses / look forward that facilitates compliance with data privacy?
7. How is organizational culture related to data privacy?
8. What is the role of regulations in the information-sharing, data privacy practices – with emerging technologies like big data, cloud, digital, mobility etc.?
9. How does the peer organizations pressure influence the data privacy practices in your organization?
10. Does organization believe in need to train employees on data privacy?
11. In which tasks and activities you/ your teams will encounter the need for decision making related to data privacy aspects?
12. Can you please share the data privacy concerns specific to your domain of the expertise?

Note: we started the initial enquiry with data privacy, but most of the experts noted that “information privacy is the more appropriate word in the organizational context”. Also, academic literature refers to information privacy similar to information security. Therefore, we referred to it as information privacy throughout the paper.

About the Authors

V. S. Prakash Attili is currently principal at Education and Training division of Infosys. He is an agile coach also offers trainings in the area of Information privacy and security. He has fifteen years of experience in the IT industry including program management, global delivery and business analysis. Prior to education division, He served as Senior Project Manager managing large multinational delivery teams over 10 years including six years in client facing role at USA. Since joining the education division in 2012, he has embarked on a research career from IIT Madras with presence in reputed conferences and Industry forums. His area of interest is digital data privacy and security in IT Organizations. He was one among the global experts on security and privacy from industry who were invited as part of Indian delegation for contributing in the ISO International Conference (ISO/IEC/JTC1 SC27) at Jaipur in October, 2015. He holds a Master's degree from IIT Bombay. He is currently a PhD candidate in information systems at Department of Management Studies, IIT Madras.

Saji K. Mathew is currently an Associate Professor at the Department of Management Studies, Indian Institute of Technology Madras. His doctoral research and subsequent academic work focused on the role of Information Technology in Business and Management. As a Fulbright Scholar, he did his post-doctoral research on risk mitigation in offshore IT outsourcing at the Goizueta Business School of Emory University, Atlanta (USA). His present research interests cover strategies in offshore IT outsourcing, issues in IT infrastructure management services, information privacy and data mining. His articles have been published in reputed international journals. He has about 10 years of work experience in the area of industrial automation in the Indian industry covering private and public sector companies. He has also provided industrial training and consulting for companies such as Exxon Mobile, Genpact, HP Globalsoft, Oracle India, Primus Retail, L&T and Hindustan Aeronautics Limited in addition to sponsored research projects for Nissan, Hand in Hand, Infosys DSIR and DFID. He teaches courses such as Management Information Systems, Data Warehousing and Data Mining, IT Services & Outsourcing, Information Systems Development and Research in IT and Organizations.

Vijayan Sugumaran is Professor of Management Information Systems and Chair of the Department of Decision and Information Sciences at Oakland University, Rochester, Michigan, USA. He was WCU Visiting Professor at Sogang University, Seoul, South Korea from 2010 to 2012. He received his Ph.D. in Information Technology from George Mason University, Fairfax, Virginia, USA. His research interests are in the areas of Intelligent Information Technologies, Ontologies and Semantic Web, Intelligent Agent and Multi-Agent Systems, and Component Based Software Development. He has published over 200 peer-reviewed articles in Journals, Conferences, and Books. He has edited twelve books and serves on the Editorial Board of numerous journals. He has published in top-tier journals such *as Information Systems Research*, *ACM Transactions on Database Systems*, *IEEE Transactions on Engineering Management*, *Communications of the ACM*, *IEEE Transactions on Education*, *IEEE Software,* and *Healthcare Management Science*. He is the editor-in-chief of the *International Journal of Intelligent Information Technologies*. He is the Chair of the Intelligent Agent and Multi-Agent Systems mini-track for Americas Conference on Information Systems (AMCIS 1999 - 2017). He has served as the program co-chair for the International Conference on Applications of Natural Language to Information Systems (NLDB 2008 and NLDB 2013). He also regularly serves as a program committee member for many national and international conferences.