IDIS (2010) 3:295–318
DOI 10.1007/s12394-010-0059-6

Extending the value chain to incorporate privacy by design principles

Julie Smith David · Marilyn Prosch

Received: 10 November 2009 / Accepted: 19 April 2010 / Published online: 18 May 2010

Abstract Morgan et al. (2009) examine the notion of corporate citizenship and suggest that for it to be effective companies need to minimize harm and maximize benefits through its activities and, in so doing, take account of and be responsive to a full range of stakeholders. Specifically, they call for a "next generation" approach to corporate citizenship that embeds structures, systems, processes and policies into and across the company's value chain. We take this notion of corporate citizenship and apply it to Privacy by Design concepts in a value chain model. Privacy by Design is comprised of Seven Foundational Principles (Cavoukian 2009), and as we develop the Privacy by Design Value Chain, those principles are incorporated. First, we examine the primary activities in the value chain and consider each of these seven principles, and then we extend the analysis to the support activities. Finally, we consider privacy implications and the challenges to be faced in supply chain and federated environments. Designing privacy into the value chain model is a practical, business view of organizational and privacy issues. This puts privacy where it belongs in an organization—everywhere personal information exists. We conclude that further research is needed to consider the internal stakeholders' communications among the various departments within an organization with the goal of better communications and shared values, and we believe the value chain approach helps to further this research agenda. Also, federated environments necessitate that organizations can "trust" their third parties providers. Research and case studies are needed regarding how these organizations can create value and competitive advantages by voluntarily providing their customers with privacy practice compliance reports. For the most part, the future is bright for the protection of personal information because solutions, not problems are being proposed, researched, developed and implemented.

Keywords Privacy by design · Value chain

J. S. David · M. Prosch (✉)
The Privacy by Design Research Lab, W.P. Carey School of Business, Arizona State University,
Tempe, AZ, USA
e-mail: marilyn.prosch@asu.edu

Introduction

Morgan et al. (2009) examine the notion of corporate citizenship and suggest that for it to be effective companies need to minimize harm and maximize benefits through its activities and, in so doing, take account of and be responsive to a full range of stakeholders. Specifically, they call for a "next generation" approach to corporate citizenship that embeds structures, systems, processes and policies into and across the company's value chain. We take this notion of corporate citizenship and apply it to Privacy by Design concepts in a value chain model. We consider the various stakeholders, both internally and externally, that potentially have any contact with personal information with the goal of better communication and designing privacy into all relevant activities. Privacy by Design is comprised of Seven Foundational Principles (Cavoukian 2009), and as we develop the Privacy by Design Value Chain, the following principles are incorporated:

a. Proactive not Reactive
b. Privacy as the Default
c. Privacy Embedded into the Design
d. Full-functionality—Positive Sum, not Zero-Sum
e. End-to-End Lifecycle Protection
f. Visibility and Transparency
g. Respect for User Privacy

First, we examine the primary activities in the value chain and consider each of these seven principles, and then we extend the analysis to the support activities. Finally, we consider privacy implications and the challenges to be faced in supply chain and federated environments.

Value chain analysis

Porter's (1985) Value Chain model has been used to analyze firm and inter-organizational activities with the goal of identifying configurations that add value or help to create competitive advantage. To model the value chain, organizations can focus on their internal operations or their complete supply chain. As illustrated in Fig. 1, internal operations include primary activities that are performed to add value to their customers' experiences and support activities that can span the organization to enable the successful execution of primary activities. Additionally, when considering supply chains and federated environments, each organization in the supply chain or federation must configure and execute their activities to best contribute to the overall system success.

Initial research focused exclusively on optimizing the flow of physical goods throughout the system and has been used extensively in practice (Supply-Chain Council 2008). Relatively recent work has recognized that information asymmetries are a major cause of inefficiencies, such as the bull whip effect (Lee et al. 1997), and the value chain concept has been extended to incorporate information and financial flows to further optimize operations (such as Patnayakuni et al. 2006). Additionally, since the internet has enabled more tightly integrated firms, research has shown that information technology has transformed the types of relationships

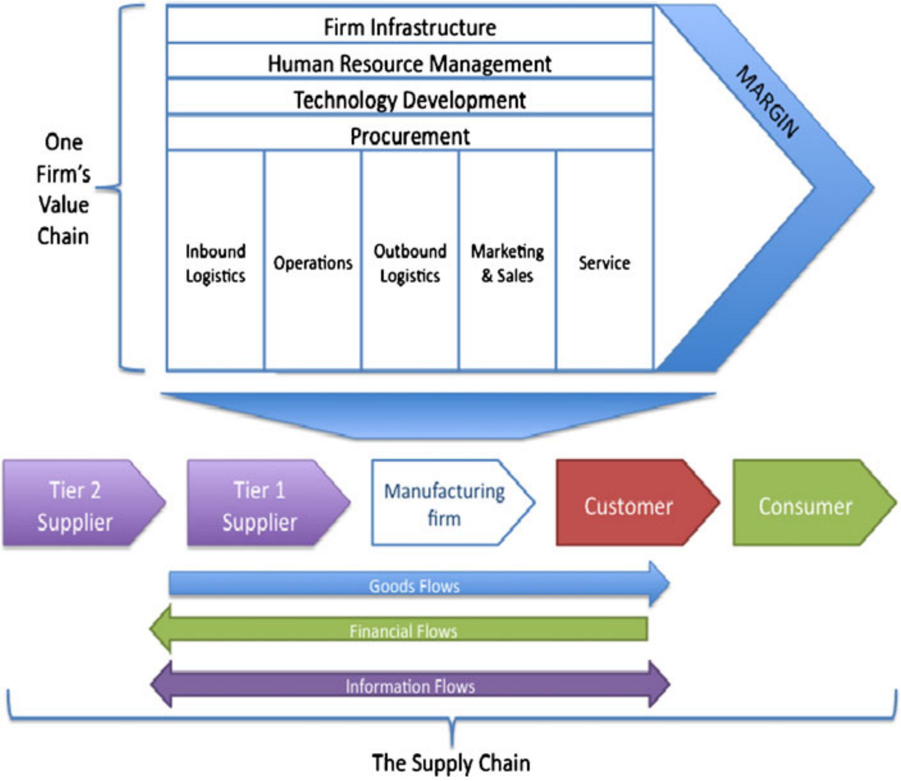

Fig. 1 The relationship between one firm's value chain and the inter-organizational supply chain (Adopted from Porter 1985)

between organizations (Porter 2001). Unfortunately, with enhanced technologies and communication between organizations, not only are efficiencies enabled, but additional opportunities arise for inappropriate use of personal information. In response, we extend this well-known model to incorporate the Privacy by Design principles. Therefore, the next section of this paper explores the privacy risks inherent in a firm's internal activities, and then the subsequent section expands the analysis to incorporate federated communities and discusses how the privacy risks flow throughout the supply chain. We argue that privacy has been an afterthought at best in this information-based society, and we propose that Privacy by Design principles should be embedded and operationalized in value chain activities to create both value and competitive advantage. To set the stage for the consideration of Privacy by Design concepts in today's digital business environment and federated communities, we consider the following quote by the creator of the initial value chain concepts:

> Many of the pioneers of Internet business, both dot coms and established companies, have competed in ways that violate nearly every precept of good strategy. Rather than focus on profits, they have sought to maximize revenue and market share at all costs, pursuing customers indiscriminately through

> discounting, giveaways, promotions, channel incentives, and heavy advertising. Rather than concentrate on delivering real value that earns an attractive price from customers, they have pursued indirect revenues from sources such as advertising and click through fees from Internet commerce partners. Rather than make trade-offs, they have rushed to offer every conceivable product, service, or type of information. Rather than tailor the value chain in a unique way, they have aped the activities of rivals. Rather than build and maintain control over proprietary assets and marketing channels, they have entered into a rash of partnerships and outsourcing relationships, further eroding their own distinctiveness. While it is true that some companies have avoided these mistakes, they are exceptions to the rule. (Porter 2001)

These thoughts directly relate to the lack of consideration of good privacy practices and the concept of a positive sum approach to privacy espoused by Cavoukian (2009). The importance of considering the payoff of good privacy practices and its impact of adding value to the customer was examined by Cavoukian and Hamilton (2002). Porter asserts, in the above quote, that businesses have rushed to implement technologies without considering the true value added of such technologies. Prosch (2009), in a similar vein, discusses how new technologies are typically implemented before their privacy impacts have been considered, as well as before the need for corresponding associated controls are developed and implemented. For example, firms that collect personal data for initial purposes may determine that selling this data is a new potential revenue stream; however, the privacy implications of such a decision are great. Therefore, this research considers why organizations need to design privacy into the value chain activities and build and maintain control over personal information, and how so doing can add value to the organization.

Internal privacy concerns

We have reviewed the literature for each of the primary and secondary (support) activities to identify potential areas for privacy concerns, and each of these are discussed in turn in this section.

Primary activities

Primary activities were defined by Porter (1985, p. 38) as those that “are involved in the physical creation of the product and its sale and transfer to the buyer as well as after-sale assistance.” As shown in Fig. 1, five broad categories of activities exist, and each can help the organization better meet its customers’ needs and add value. As such, customer data is likely captured, used or disseminated in one or more of these steps. The following sections highlight the general business models that have emerged and highlight their implications for privacy within their context of the Seven Foundational Principles.

Inbound logistics Inbound logistics encompasses the activities performed to receive materials into an organization. For production facilities, the materials are in “raw”

form, for merchandising organizations, they may be in semi-finished or finished goods form. For service organizations, the inbound materials may take many forms. Literally, in the medical profession, the intake would be the patients, and in the legal profession, the clients. For manufacturing facilities, these activities are performed by purchasing and receiving employees within the focal firm, and the sales and distribution employees at the seller's organization. Given that privacy concerns are generally about uncontrolled and/or improper use of personal data, usually either collected from or about customers or employees, no significant privacy concerns are identified in the manufacturing industry in the typical inbound logistics function.
For the service industry, however, the intake process can involve the collection of a significant amount of personal information, such as prior medical history, allergies, legal records, or financial information. In the service industry, designing privacy into the intake of personal information regarding customers is imperative. Policies, procedures and controls need to be put into place to ensure that only necessary data is collected during the intake process of service organizations, and that it is accurate, complete, and protected. Further customers must be given appropriate notice and asked for consent (only in special cases would this not be a requirement).

Referring back to the Seven Foundational Principles, we propose some guidelines for designing privacy into the inbound logistics phase of the value chain. In order to be proactive, organizations should engage in the process of clearly identifying what personal information is absolutely necessary for the establishment of the individual into the system, and only collect that data. If an organization has a true business need to collect certain pieces of personal information, then that data should be thought of as adding value to the experience of the customer. The positive sum approach necessitates that such value added as a result of collecting and possessing the data be explicitly identified and considered. Collecting data just because "you can" without an associated business need can actually result in the organization creating a potential liability (Prosch 2009). In order to set privacy as the default, the system should be set up with the assumption that the individual does not wish to have their information shared. In order to respect user privacy, the user should be given notice about all uses of their personal information at the point of collection and they should be given choices about how that data will be shared. All input screens and forms, as well as access to such data, should be designed with protection of the data in mind. For example, electronic clipboard use for collecting medical histories of new patients should have encryption embedded into the devices for data transmission, so that data cannot be transmitted any other way other than encrypted. Data that is collected at the intake does not magically self-destruct once its usefulness has expired (although that would be a nice Privacy by Design technique), so the consideration of when it should be destructed needs to be considered at the outset, as well as the method of destruction of all instances (replications) of the data. Table 1 summarizes privacy considerations across the Seven Foundational Principles for the input logistics activities of the value chain.

Operations Operation activities are the "production" activities a firm performs to create goods or services that are valued by their customers. Initially, operations research focused on manufacturing processes of made-to-stock physical goods. In this initial case, no privacy issues are readily apparent. However, as organizations

Table 1 Input logistics considerations by foundational principle

Proactive vs. Reactive	For each piece of data that is not required by law, assess the value of the data to the organization. If value is found, next assess the "cost" to the employee/ customer. Select privacy solutions that minimize identified costs.
Privacy as the Default	For the intake of new customers/ employees obtain explicit consent for uses of such data.
Privacy Embedded into the Design	Carefully design and protect input screens and forms with choice fields explicitly displayed and easy to find. Encrypt personal information.
Positive Sum not Zero-Sum	Consider the real business needs of all data collected during the intake process and do not collect any data that does not serve a real business purpose as it can potentially become a liability.
End to End Lifecycle	Protect all personal information collected during the intake process and during the entire life span of the data. Determine the retention period and destruction time *before* the data is initially collected.
Visibility & Transparency	Notify new customers of relevant privacy policies and procedures. Make all privacy policies and procedures readily available and easy to understand. Clearly conveyed to the customer/employee all uses of third parties.
Respect for User Privacy	Do not conduct unwarranted employee monitoring. Involve customers in privacy development practices.

have moved toward mass customization for their production processes, and as service delivery has become more important to the economy, privacy processes must be incorporated into these activities. When organizations adopt mass customization processes, they create products in response to specific customer desires. Firms may elect to customize the physical products as they are manufactured (or enable the customer to customize the product), but may also customize the sales processes or packaging variations. Research has found that organizations that adopt mass customization are often able to increase sales, and whenever the customization is being performed by the organization, the firm must collect customer preference information, and make it available to the operations team. (Da Silveira et al. 2001). If done successfully, research indicates that organizations adopting mass customization practices may be able to increase revenues through product differentiation, and customers are willing to share information and become "co-producers" of goods if they enjoy the co-production "experience" and receive a product that meets their needs (Fiore et al. 2004.).

Customization by nature requires customers to share their preferences which are transferred to the operations team. This practice, which is often enabled through information technology that supports a high volume of transactions, exposes the organization to potential privacy risks. For example, the internet has enabled organizations to easily collect customer preferences and personal information such as personal body measurements used to create customized Levi's jeans or personal messages engraved on customized products (Fiore et al. 2004). Processes should be designed so that a minimal number of employees have access to the personal information of customers during the operations processes. Further, logs of such access should be kept and monitored for compliance with privacy policies and procedures.

As mentioned in the inbound logistics section, privacy issues also exist for service providers. Similar to mass customized manufacturing, in most service organizations, customer requirements are collected and used to customize and deliver the service. In addition, many services have significant information content which results in firms having varying amounts of personal information, some of it highly sensitive. For example, health care providers engage in diagnostics, compile test results, provide treatments and prescriptions, and store diagnosis and treatment information. The protection of personal health information falls under the EU's Privacy Directive and Canada's PIPEDA laws, and in the US under HIPAA regulations. Likewise, the processing of financial data generally falls under the general privacy directives in the US and Canada and under the Gramm-Leach-Bliley Act and the FCRA in the US. Privacy is not regulated in the US for many other sectors, however, that collect, process and store personal information: accountants, lawyers, ISPs, social networking services, and many other online services, such as email providers, to name a few. In all of these cases, operations procedures must be designed with privacy practices at their core. If not, the organization will be exposed to security risks, and, as research has shown, if the customer no longer trusts the provider, they may reduce or eliminate future purchases from the supplier.

Again, referring back to the Seven Foundational Principles, we propose some guidelines for designing privacy into the operations phase of the value chain. Reactive systems are ones in which unnecessary personal information is collected and/or not appropriately protected or used. To be proactive in the operations phase of the value chain, organizations should clearly identify precisely what personal information is absolutely necessary for the delivery of the service or manufacturing of the good and only collect that data. Again, the data should add value to the experience of the customer or provide efficiencies to the organization that can result in savings that can be passed back to the customer. Consider rental car agencies that collect the whereabouts of their customers through GPS systems. Likely, little direct benefits pass to the customer from the collection of such data, but the car rental agency can use it to identify customers that drive the car into prohibited locations, such as a U.S. rental agency that prohibits taking the car into Mexico. The data can be used to fine such individuals and potentially charge them higher rates the next time they wish to rent a car, allowing potentially lower rates to be charged to other customers. The positive sum approach considers such value added activities, while at the same time protecting the privacy of the individual. In the case of the safe return of the vehicle with no prohibited activities having occurred, the personal information regarding the whereabouts of that customer should be destroyed because at that point they serve no business purpose and the data lifecycle should come to an end for those specific pieces of data.

Retaining data just because "you can" without an associated business need, can result in the organization facing undesirable situations, such as a law enforcement agency that subpoenas the records a later time. If the organization does not retain such data, then it does not have to deal with the administrative costs of complying with the subpoena and any potential press/media issues as well. In order to respect user privacy, the user should be given notice about all uses of their personal information before or at the point of collection and they should be given choices about how that data will be shared. In the case of the car rental agency, the customers should be made aware that their location whereabouts will be tracked. One option may be to give them the option to have future rates lowered if the organization is allowed, with their permission, to keep their location-based data for a specific period of time. If data is kept on improper use of the car, such as speeding or traveling to forbidden destinations, then the customer needs to be notified prior to renting the car. Again, personal information that is collected during the operations process should only be kept as long as a business purpose exists and appropriate destruction processes should be designed into the system. Additionally, uses of personal data identified after the initial data collection and notice must be very cautiously considered. For example, selling customer data without notice and consent can result in loss of trust at a minimum, and, in some jurisdictions, may result in legal action or regulatory sanctions.

Employee monitoring data may be collected during the operations phase and the legality of such monitoring varies widely internationally. Such data might be throughput rates, billable hours, wasted raw materials, and even mouse technology that records pulse rates and body temperatures of computer users. First, the local law must be researched and understood. Secondly, the real business need of such data should be identified and the effects on the morale of the employees should be carefully weighed, considered and documented. If employee monitoring is collected during the operations phase, it should be protected and periodically reviewed for appropriateness. Table 2 summarizes privacy considerations across the Seven Foundational Principles for the operations activities of the value chain.

Outbound logistics Porter (1985) defined outbound logistics as "activities associated with collecting, storing, and physically distributing the product to buyers". For most

Table 2 Operations considerations by foundational principle

Proactive vs. Reactive	For each piece of data that is not required by law, assess the value to the organization. If value is found, assess the "cost" to the employee/ customer. Select privacy solutions that minimize identified costs.
Privacy as the Default	Do not collect any operational monitoring data without giving notice, and if appropriate, give choices.
Privacy Embedded into the Design	Design processes so that a minimal number of employees have access to the customer data during operations and keep logs of such access.
	Securely collect and use employee monitoring data and periodically review for appropriateness.
Positive Sum not Zero-Sum	Foster co-producers philosophy of customization experience to enhance both product/service provider's and customer's value received from the relationship.
End to End Lifecycle	For all data collected that may be necessary to process the transaction consider how long it is really needed before collecting it. Destroy the data as soon as the business purpose no longer exists.
Visibility & Transparency	Notify customers/ employees of all uses of data collected during the operations processes.
	Clearly conveyed to the customer/employee all uses of third parties.
Respect for User Privacy	Appropriately train operations employees to respect the personal information necessary to make the good or perform the service.
	Give choices to customers about how their data is used. Protect employee monitoring data and use it with respect for the individual.

organizations, little additional customer information is collected during this phase relative to other primary activities. The extent of privacy exposure, therefore, is generally limited to the customer data that is used during this process, but many of the same concerns regarding the personal information of employees/customers are the same as during the inbound logistics and operations. For example, as goods are packed and shipped, customer addresses and buying behaviors are visible to warehouse and distribution employees. Referring back to the foundational principles, we propose some guidelines for designing privacy into the outbound logistics phase of the value chain. Organizations must proactively identify potential privacy risks in the outbound logistics activities and train employees about the appropriate and inappropriate use of personal information used during the packaging and delivery of goods and services. Consider the delivery function for a florist, the processes in place should ensure that the delivery staff cannot read messages (seal the envelope) nor should they talk about the contents of their deliveries to others. Oftentimes, when packages are delivered to homes, when an individual is not available, the delivery personnel will attempt to leave it with a neighbor, whose name gets added to the database for tracking purposes. The positive sum approach to this situation would cause the organization to consider how it can provide tracking details of the delivery without infringing upon the privacy of the neighbor. The delivery person should inform the neighbor that their address and name will be stored for tracking purposes and they should be given a choice whether to accept the delivery under those terms. Tracking numbers that can be used to gain access to the contents of packages should not be externally viewable. Further, packaging, to the extent possible, should not reveal the contents of the package. A reasonable time period for retention of such data should be identified and communicated to the individual.

Some organizations collect and sell data as their major primary activity. Such organizations face considerable privacy issues during their outbound logistics activities, i.e. when they are transferring data to their clients. Consider marketing information service organizations that aggregate consumer data to sell to retail organizations. They can potentially aggregate data in such a way that seemingly anonymous data becomes personally identifiable. We assert that leaders in the industry can potentially benefit from instituting privacy practices that protect individuals—whether data are further aggregated to show trends or the personal information is omitted. Failure to do so may result in deteriorating consumer confidence, or perhaps in more serious legal/regulatory challenges in certain jurisdictions.

Recently, much debate about the privacy issues surrounding RFID devices in consumer goods, such as tires, athletic shoes, razors, etc. has ensued (Shih et al. 2005). One well known example is how an RFID device was used in lipstick packaging and then subsequently used in a Wal-Mart store to monitor how consumers "handled" the product (Hildner 2006). The intended use of the RFID was to prevent against theft, not to track the actual "use" after it left the store. Cavoukian (2008), in conjunction with Hewlett-Packard, issued a set of guidelines for the use of RFID tags in the healthcare sector. The report highlights concerns over RFID and privacy issues, but suggests that the benefits of the technology are great enough to make it worth navigating the privacy risks. Two examples of privacy by Design regarding RFID devices is the ability to strip away the transmitting device (IBM's "clipped tag") and the creation of an "always off" RFID device (privacy by default) that can be turned on when necessary by squeezing the device to emit a signal (Cavoukian 2009). Table 3 summarizes privacy considerations across the Seven Foundational Principles for the outbound logistics activities of the value chain.

Marketing & sales Sales and marketing activities influence customers throughout the sales cycle: from initial contact with a potential customer through the execution of a sale. This process was historically based on personal relationships between firm personnel (often a sales person) and customers, and trust was built over time from repeated interactions. This relationship changed dramatically with the emergence of internet delivery channels. In this environment, supply chain efficiencies can be gained, but only if consumers are willing to use the internet-based order processing systems to execute their transactions. One important difference in the web-based era of sales and marketing is the technological ability to record browsing behavior that may or may not result in a sale. Many organizations even analyze abandoned online

Table 3 Outbound logistics considerations by foundational principle

Proactive vs. Reactive	For each piece of data that is not required by law, assess the value to the organization. If value is found, assess the "cost" to the employee/ customer. Select privacy solutions that minimize identified costs.
Privacy as the Default	Do not collect any operational monitoring data without giving notice, and if appropriate, give choices. Devices, such as RFID, should be "off" by default when possible.
Privacy Embedded into the Design	Designed processes so that a minimal number of employees have access to the customer data during outbound logistics and keep access logs. Securely collect and use employee monitoring data and periodically review for appropriateness. Consider RFID devices with the ability to disengage by the customer after the purchase and delivery is complete. Mask/hide tracking numbers that can be used to gain access to the contents of packages.
Positive Sum not Zero-Sum	Consider technologies that do not infringe on privacy, such as RFID devices for tracking that can be deactivated. Do not use delivery packaging data that contains personal information as a marketing tool at the expense of customer.
End to End Lifecycle	For all data collected that may be necessary to process the transaction, consider how long it is really needed before collecting it. Destroy the data as soon as the business purpose no longer exists.
Visibility & Transparency	Notify all customers/employees of all uses of data collected during the outbound logistics processes. Clearly convey to the customer/employee all uses of third parties.
Respect for User Privacy	Appropriately train outbound logistics employees to respect personal information. Give customers choices about how their data is used. Use and protect employee monitoring data with respect for the individual. Ensure that the contents of the packaging cannot be easily identified from the packaging.

shopping carts. Research has shown that consumers are less likely to shop online if they believe their personal data may be used inappropriately. Concerns arise that their personal information may result in interactions they do not desire (such as spam), may be sold to other organizations, or may be used inappropriately (such as inferring personal characteristics). Targeted behavioral advertising is a topic of hot debate where companies, such as Google, examine the contents of incoming/ outgoing email messages and deliver advertising content based on those messages. Since individuals cannot control what is sent to them in messages, a concern about the delivered advertisements has arisen. To overcome many of the privacy concerns surrounding sales and marketing, firms can implement policies and practices to gain customers' trust (Luo 2002). Again, we consider the Seven Foundational Principles, this time from a sales and marketing perspective. The Privacy by Design value chain can guide management to develop high quality privacy policies and procedures that are embedded into sales and marketing practices and where respect for the customer is at the core of such practices. In all sales and marketing databases, regardless of the source of collection of personal information, users should be allowed to access, correct and delete marketing data and object to behavioral inferences. To be successful in electronic commerce, organizations must convince their customers to trust the internet in general, as well as the vendor, and its specific web site (McKnight et al. 2002). Transparency needs to be designed into the systems and privacy as a default should guide businesses regarding their marketing opt-in, opt-out choices (Mine and Boza 1999). "Web signals" can be implemented to increase customer trust, and trustmarks have been shown to be the most influential (Aiken and Bousch 2006). "Trustmarks are defined as any third-party mark, logo, picture, or symbol that is presented in an effort to dispel consumers' concerns about Internet security and privacy and, therefore, to increase firm-specific trust levels." (Aiken et al. 2003). These trustmarks, however, should not be used to deceive consumers, they should be based on truly respectful, positive-sum approaches to privacy practices. Marketing departments need to devise mechanisms, such as anonymizing databases that will be kept for a long period of time for data mining purposes. Marketers have also come to learn that more is not always better and that a smaller set of permission-based customers can provide richer targeted customers sets than extremely large databases that only contain a small number of truly interested potential customers as evidenced by the relative purchasing prices of such lists (Hosford 2009). Table 4 summarizes privacy considerations across the Seven Foundational Principles for the marketing and sales activities of the value chain.

Service In Porter's initial value chain work, service refers to the post-sales service activities that enhance the customers' long-term experiences with the products they have purchased. Service may be needed on a scheduled basis (such as automobile service appointments or elevator maintenance) or may be in response to a product/ service problem (such as a product failure). These activities are critical to an organization's long term success because every service delivery event is an opportunity to collect product/customer information and to provide a service recovery experience. Additionally, research has shown that successful service recovery is dependent upon successful execution of the service recovery process and is especially reliant on having employees who deliver excellent service and who

Table 4 Marketing and sales considerations by foundational principle

Proactive vs. Reactive	For each piece of data that is not required by law, assess the value to the organization. If value is found, assess the "cost" to the employee/ customer. Select privacy solutions that minimize identified costs.
Privacy as the Default	Do not collect any marketing data without giving notice, and use the opt-in method of data collection. Do not use web beacons to capture or transfer data without notice and explicit consent.
Privacy Embedded into the Design	Develop high quality privacy policies and procedures into sales and marketing. Use permission based marketing and whenever possible anonymize personal information as soon as possible for data mining purposes. Design processes so that a minimal number of employees have access to sales and marketing data.
Positive Sum not Zero-Sum	Generally avoid unsolicited, direct marketing as permission based marketing has been shown to provide richer, more meaningful sets of potential customers.
End to End Lifecycle	Consider how long all marketing and sales data collected is really needed before collecting it. Destroy the data as soon as the business purpose no longer exists.
Visibility & Transparency	Notify customers/employees of all uses of data collected during the sales and marketing processes. Clearly convey to the customer all uses of third parties.
Respect for User Privacy	Appropriately train sales and marketing employees to respect personal information. Allow users to access, correct and delete marketing data and object to behavioral inferences. Give customers choices about how their data is used. Use and protect employee monitoring data with respect for the individual. Ensure that the contents of the packaging cannot be easily identified from the packaging.

are able to interact with customers (Spreng et al. 1995). However, in the delivery of this service interaction with the customers, much personal information may need to be accessed and additional personal information generated. Further the data collected in post-sales activities may be electronically gathered via sensors and other automated devices or by customer and service representative interactions. Given the level of interaction between the service personnel and the customer, significant privacy risks exist within this value chain activity. To prevent customer service representatives, especially from outsourced vendors, from downloading customers' personal information, thin-client environments with no client side electronic writing devices are preferred.

A primary concern in the service function where personal information is being accessed and shared with the customer or employee is the authentication of the individual. Privacy flies out the window if anyone can request and receive personal information on persons other than themselves. Authentication techniques for service purposes need to be embedded into the system, such as challenge-response questions, one-time password devices, and/or biometrics. Further, customer service representatives frequently rely on information technology to access customer, product, and sales information to better understand the customer's situation and respect for the customer needs to be embedded into the system as well. During such reviews, customer service representatives will likely see personal information that should remain protected. Therefore, the service interfaces must be designed to share appropriate data with the service representative - but not share unnecessary personal data. Additionally, service personnel will also collect product, service, and customer information during their post-sales service activities. Training these employees in the importance of maintaining confidentiality is critical. Incentives can help assure that the training and policies are followed.

Transparency of practices in customer service can be challenging as companies may not wish their customers to know the service call has been outsourced to another country. In the spirit of transparency and respect for the customers, full disclosure should be given the customer. If the customers are truly distraught, then the company should consider conducting additional value chain analysis for these activities. As organizations create self-service interfaces for their customers to use, a company's internet applications collect more granular data about the customer experience. These systems can track every click made by customers, capture all responses to posed questions. As a result, much personal information may be collected, and it needs to be protected. For example, if a patient returns to a hospital's patient portal to get information about on-going care of diseases and/or surgeries, the system needs to be adequately controlled (authentication of customer, well-designed screens, encrypted data) to keep such data confidential. The entering of response data into these systems needs to be considered in the privacy policies and practices, as well as the uses and retention. Table 5 summarizes privacy considerations across the Seven Foundational Principles for the marketing and sales activities of the value chain.

Support activities

Support activities are defined as those which "support the primary activities and each other by providing purchased inputs, technology, human resources, and various organization wide functions" (Porter 1985). As illustrated in Fig. 1, support activities can span the organization and will support and interact with the organization's primary business functions. Although not mentioned specifically in Porter's initial work, governance and reporting functions such as accounting, finance, and internal audit are performed to provide guidance to an organization's primary activities (such as how accounting can support value chain analysis as discussed in Hergert and Morris 1989), and can also be used to support inter-organizational value chain analysis (Dekker 2003). Therefore, these functions are also categorized as support activities. We examine Porter's four support activities, and expand some of the activities to incorporate relevant events and processes to further examine Privacy by Design opportunities. When considering these various support activities, different perspectives within an organization and amongst these various support groups may exist, and actually are quite normal; however, they can present challenges to organizations as they move forward in advancing privacy initiatives. Research is needed in this area to help identify situational and dialectic differences and to overcome such hurdles and advance positive-sum Privacy by Design strategies.

Table 5 Service considerations by foundational principle

Proactive vs. Reactive	For each piece of data that is not required by law, assess the value to the organization. If value is found, assess the "cost" to the employee/ customer. Select privacy solutions that minimize identified costs.
Privacy as the Default	Do not collect any service data without giving notice, and the opt-in method of data collection should be used. Do not use electronic sensors or program code to capture or transfer data without notice and explicit consent
Privacy Embedded into the Design	Develop high quality privacy policies and procedures into all service activities.
	Design processes so that a minimal number of service employees have access to personal information and only when servicing the employee or customer.
	Use strong authentication techniques, such as one-time passwords, biometrics or effective challenge-response systems, to authenticate users requesting account information.
Positive Sum not Zero-Sum	Carefully consider the value of the outsourcing partners used from a customer perspective, and consider more closely aligning the customer's desires with potential marketing advantages by choosing high-quality third parties with good reputations.
End to End Lifecycle	For all service data collected, consider how long it is really needed before collecting it. Destroy the data as soon as the business purpose no longer exists.
	Consider thin client-servers where service representatives are not allowed to download any data locally.
Visibility & Transparency	Notify customers/employees of all uses of data collected during the service processes.
	Clearly convey all uses of third parties, including their geographic location, to the customer.
Respect for User Privacy	Appropriately train service employees to respect personal information.

Firm infrastructure The infrastructure includes many different activities that support the entire organization, including, but not limited to Accounting, Internal Audit, Legal and Risk Management. These activities can become the backbone for good privacy practices. Privacy polices and procedures must be designed into accounting systems because such systems have the potential to contain large amounts of personal information about both employees and customers. Accountants are required to maintain strong audit trails and internal controls over the financial aspects of the accounting systems, but for privacy to be truly protected, additional controls need to be considered to protect granular transaction data. For example, hospital systems must protect patients' data containing medical procedures performed, diagnostic codes, and prescription data. Similarly, in front desk hotel systems revenue data is collected and transmitted to the financial system. However, the details of the bills may contain personal information, such as food, beverages, movies purchased, etc. When such systems are implemented the accounting department should consider Privacy by Design principles for the personal information in addition to the typical accounting internal controls. The internal audit team is responsible for assessing whether the organization's management team is a good steward of the organization's resources. In addition, they are tasked with preventing and detecting fraud. In these roles, internal audit teams will likely find it necessary to monitor the transactional activities in an organization and they may monitor employees and search for conflicts of interest. Various countries have starkly different laws on what is allowed in terms of employee monitoring. Regardless of the legal requirements, good privacy practices should be designed into these internal audit activities, with a close eye on what is required, what is permissible, and what is illegal. Careful thought needs to be given as to how to best conduct these employee-related monitoring activities while at the same time fostering the concept of "good corporate citizenship" with regards to privacy rights of employees.

Legal departments and/or corporate counsel should always be consulted when establishing monitoring activities. A challenge is to balance compliance with best practices, and we argue that that in many cases a positive sum can be achieved by uniquely looking at ways to be in compliance with laws and regulations and also best serve the individual. Risk management teams can also be viewed as having similar challenges. Oftentimes, the goal of risk managers is sharing the risk with an insurance company rather than changing policies and procedures that can actually reduce the risk by implementing better privacy practices. Legal and risk management perspectives often focus on evaluating minimal compliance efforts to meet regulatory statutes, if a focus on developing best practices to improve employee/customer privacy, it is likely that such practices will also meet most international regulations, often at a lower cost.

Human resource management The perspectives of workplace privacy and legal regulations over how employee data may or may not be used vary greatly internationally. Obviously, companies must keep data that is required by law to be collected and kept. At issue is all other data collected about employees. Careful consideration needs to be given to what data should be collected, the retention periods, and practices to insure destruction of data at the end of its life. Organizations, when adopting the Seven Foundational Principles, need to recognize that privacy must be embedded into human resources processes regardless of their regulatory regime. As with customers, privacy policies and practices should be transparent and respectful of the individual. The data should be protected throughout the lifecycle and only used for identified business purposes. These practices need to be embedded into the processes and technologies and not considered as an after thought.

Technology development Technology plays a critical role in almost all organizations, regardless of their industry. Included in this support activity, we also consider Research and Development efforts as they are focused on product improvements, service improvements for customers and internal service provision improvements. A major challenge for organizations in the era of rapidly changing technologies is to understand the benefits and potential risks of changing and new technologies. Prosch (2008) has discussed the tendencies for new technologies that apparently provide value to organizations and individuals to be implemented without clearly and specifically thinking about the privacy implications. Although such adoptions may prove profitable/acceptable in the short run, cultural lag theory predicts that consumer desires and privacy enhancing technologies will eventually catch up. Specifically, cultural lag theory indicates that the initial controls tend to be more reactive than proactive. For example, recently Facebook received much criticism for its renegade 3rd party applications that were allowed to pull and share information in ways not understood nor desired by users. After spending a month with staff members from the Office of the Privacy Commissioner of Canada investigating their practices in their own offices, Facebook agreed to have all such 3rd party applications to be retroactively refitted with better notice, choice and consent features within a 12 month period. If Facebook had required the incorporation of privacy protection into their 3rd party applications at the outset, this costly reworking would have been unnecessary. Additionally, although Facebook certainly has a large customer base, their renegade 3rd party applications may have scared some people away. Or it may have many users that just won't trust any application at all anymore and not use them and only use minimal feature on Facebook, which will cut into its revenue stream.

Procurement Traditionally, procurement activities in manufacturing involved a purchasing agent who determined the best suppliers considering time, quality and price. In today's business environment, procurement must still be authorized to support a business need, but the process of selecting vendors and acquiring goods have evolved into a multitude of purchasing environments. When the goods are raw materials into a production process, little personal information is gathered. In service industries, however, much personal information may be gathered as a result of preparing to deliver a service. For example, to prepare for an upcoming flight, a charter plane service will need to know the passengers' food, beverage, and entertainment preferences and possibly other personal characteristics, including health information. Since the procurement process has personal information, privacy policies and procedures need to be carefully considered and designed into the system. If the catered food is outsourced, special care needs to be made to insure that the customer has been given notice if any personal information is shared, how it is used and also given choices about the collection and use of the data. Many other examples exist in the service sector, and the time has come for tangible privacy guidelines. Table 6 summarizes privacy considerations across the Seven Foundational Principles for the support activities in the value chain.

Inter-organizational privacy challenges - federated PIA

Privacy risk analysis has typically been performed at the individual organizational level. However, "it is important to be aware that organizations are part of a wider system of adding value, involving supply chains, distribution value chains and customer's value chains. By managing the whole value system and cooperating with suppliers and distributors, the entire process—from raw materials to the end product—can be optimized, thus creating greater value and/or lower costs. This way competitive advantage can be achieved (Hergert and Morris 1989)." Although this quote highlights the advantages of inter-organizational coordination, it ignores the risks arising from having data propagated throughout the supply chain. Therefore, articulating and understanding the privacy supply chain is necessary to fully understand the challenges any organization that collects, uses or processes personal information faces.

Table 6 Support activities considerations by foundational principle

Proactive vs. Reactive	For each new technology implemented, consider the potential privacy impact before adopting and simultaneously developing and implementing associated privacy enhancing controls.
Privacy as the Default	Do not collect any support data without giving notice, and use the opt-in method of data collection.
Privacy Embedded into the Design	Develop high quality privacy policies and procedures into all accounting system processes that collect or use personal information.
	Design support activities so that only relevant service employees have access to personal information and only when servicing the employee or customer.
Positive Sum not Zero-Sum	Carefully consider the value of the outsourcing partners used from an employee/customer perspective, and consider more closely aligning these desires with outsourcing choices.
End to End Lifecycle	Consider how long data is really needed before collecting it for all support activities.
	Destroy the data as soon as the business purpose no longer exists.
	Consider thin client-servers where service representatives are not allowed to download any data locally.
Visibility & Transparency	Notify customers/employees of all uses of data collected during the internal audit and human resource processes.
	Clearly convey all uses of third parties, including geographic location, to the customers and employees, where applicable.
Respect for User Privacy	Appropriately train all employees engaged in the support activities to respect personal information.

Traditional supply chain Prior to the widespread use of the internet, organizations largely performed the same primary and support activities, and relationships between entities in the supply chain were relatively simple, as illustrated in Fig. 2. In this supply chain, goods are produced by the manufacturing firm that buys raw materials and components from upstream suppliers. The goods are sold to an intermediary (perhaps a distributor or a retail store) from whom customers buy the finished goods. In this case, some information, such as product specifications or aggregated demand, may be shared between trading partners across the supply chain. However, the consumer only places their orders, including limited personal data, with one organization, and the data is not shared with any other entities in the supply chain. This localizes the privacy risk to the intermediary firm. The basic supply chain is frequently extended by organizations in the transaction. For example, credit card processing entities handle the financial transactions and have access to the information needed to execute these transactions; third party carriers have access to addresses and bills of lading which can reveal the contents of the shipment; and the individuals who make the product deliveries often have information about the specific goods that are being delivered to the consumers. Each of these entities will potentially use personal information, and must implement privacy practices to survive in regulated environments and to gain consumer trust, business value, and competitive advantage. Working with these specialized organizations has become a normal part of business, and evaluating privacy policies and strengthening and implementing them becomes an evolutionary necessity. Additionally, as organiza-

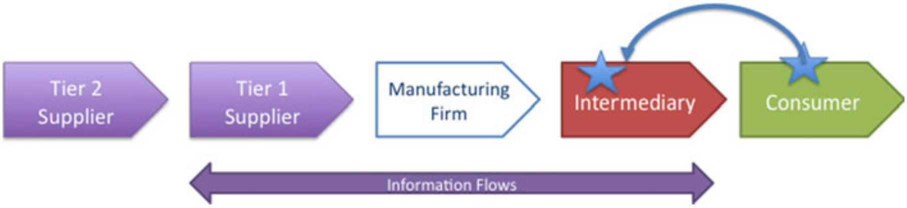

Fig. 2 Minimal propagation of consumer data

tions move toward providing customized goods and services, confidential information can move further up the supply chain (such as passing consumer information to a contract manufacturer who can provide mass customization of goods and services.) As a result, the "traditional" supply chain actually has additional propagation of personal information, as shown in Fig. 3.

Outsourcing primary/support activities In the mid-1980's outsourcing deals became increasingly popular and gained attention in the press (such as Kodak's 1989 outsourcing of their IT initiatives). Since that time, outsourcing has become very common, and organizations have gained experience in outsourcing both their primary and support activities. Thus, the concept of virtual organizations has taken hold. Enabled by inter-organizational computer systems, these business arrangements are performed with the goals of achieving a combination of cost savings from economies of scale and/or best practices in process execution. Research (although mixed) has shown some evidence of satisfaction in the outcomes from outsourcing projects (Kakabadse and Kakabadse 2002). Although efficiencies may be gained, these arrangements introduce more complexity into the privacy supply chain. Figure 4 depicts a supply chain for an intermediary organization that has chosen to outsource its call center activities. The outsourced call center employees will need access to customer data that is already being stored in the intermediary's enterprise

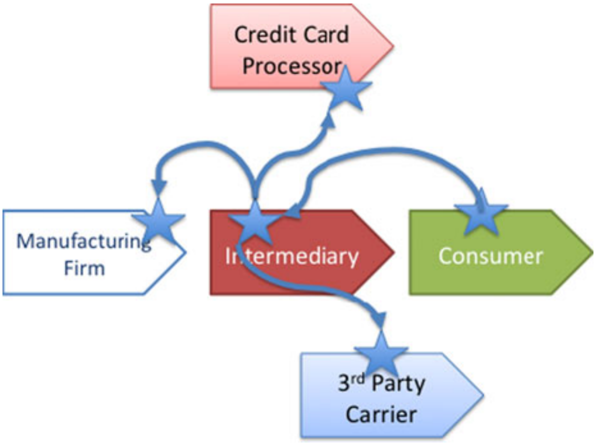

Fig. 3 Additional propagation of confidential consumer information in traditional supply chain environments

system. For example, to respond to customer's post-sales service questions, the call center team will require access to data regarding the goods the consumer has purchased as well as their billing and/or shipping address. Additionally, the call center employees will collect further information about the customer and their purchases during the service activities. In this process, two privacy challenges arise. First, the call center may use its own information systems to support its call center activities, requiring data from the intermediary to be transformed and loaded into the call center's system. Their system may improve customer service because of its unique optimization and the economies of scale enjoyed because the costs of development will be shared across all client organizations. However, by creating multiple copies of customer data, the privacy issues also multiply (Nehmer and Prosch 2009). Questions of who has the responsibility for privacy practices should be addressed prior to any outsourcing negotiations by the organization representing the entity ultimately responsible for collecting the data (called the data controller in the EU).

Second, even if the call center provider does not use its own information technology, and all data remains under the direct control of the intermediary, opportunities exist for the employees providing the outsourced service to misuse data to which they have access. For example, if consumers must provide credit card numbers for services or add on products, the call center staff will have access to critical information, and solid data protection policies and procedures must be embedded into associated systems in order to minimize the risk that these employees can misuse the data.

Because of these privacy concerns, organizations must evaluate the risks of outsourcing arrangements before finalizing their cost/benefit analysis. A common concern is with outsourcing centers in foreign countries with different privacy standards. For example, privacy definitions are embedded in cultural understanding - and understanding the differences between cultures can be very difficult. For example, Capurro (2005) provides an overview of how Japanese and Western cultures differ at fundamental levels, and how getting individuals from these cultures to arrive at a similar understanding of "privacy" is very difficult. Organizations also need to be mindful when contracting with "non-traditional" service providers, such as using prisoners in U.S. jails for order processing

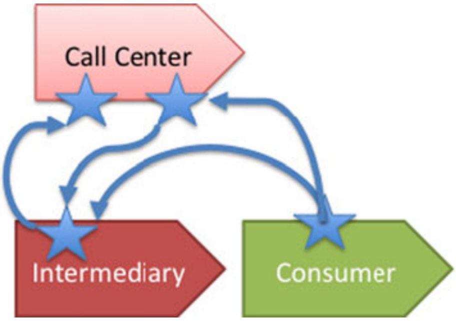

Fig. 4 Introducing an outsourcing provider of call center/customer service activities

outsourcing services (Sullivan 2005). In these cases, the public impressions of privacy[1] concerns can be as important as the likelihood of a problem occurring.

Outsourcing IT: software as a service

A growing percentage of organizations are electing to source their IT applications from Software as a Service vendors, and the trend is predicted to continue to grow (Carr 2008). Currently, one of the most well-known SaaS vendors, Salesforce.com, is recognized as providing customer relationship management software, and they currently report having over 63,000 customers and 1.5 million subscribers. For these customers, Salesforce hosts the data used in their applications - and much of that data relates to consumers. At the same time, although Workday is much less well-known, they have clients which are very large organizations: Chiquita and Flextronics for example. These clients are adopting Workday for their human resources management application, and, therefore, all of their employee data will be hosted by Workday. Given the types of data stored "in the cloud," organizations adopting SaaS solutions must understand the privacy risks, and providers of these services must implement practices to insure the privacy of this data.

The Privacy by Design Value Chain becomes even more complex if organizations adopt "platform as a service" (PaaS) solutions to integrate functionality from several SaaS sources into one business process. For example, Salesforce.com has made their application platform, Force.com, available to developers worldwide. These developers can elect to create "native" applications that are hosted by Salesforce, or they can create applications that reside on their own infrastructure, but integrate with the Salesforce.com platform as "composite" applications. In the case of composite application situations, potential risks exist for users of these services given the information asymmetry surrounding the developer and application architecture (David and Mann 2007). Therefore, organizations adopting PaaS solutions must understand the risks of having consumer data residing in several different systems with service providers with which they have not worked directly (see Fig. 5) and determine ways to gain additional assurances that these applications will meet their privacy requirements. As mentioned earlier, Facebook—a free service provider that has become a platform for development came under investigation in Canada for a lack of privacy standards in their third party applications that were pulling personal information and displaying it to other users. As previously mentioned, Facebook is now faced with ensuring that the third party applicators retroactively reprogram to meet the new privacy requirements.

An integrated example

As organizations and their strategies evolve, new business relationships will emerge that will further challenge privacy practices. For example, many organizations are currently incorporating "social media" into their technology capabilities to

[1] We view security as a necessary, but not sufficient condition of privacy. So when we discuss privacy, we are also referring to the necessary security to ensure privacy.

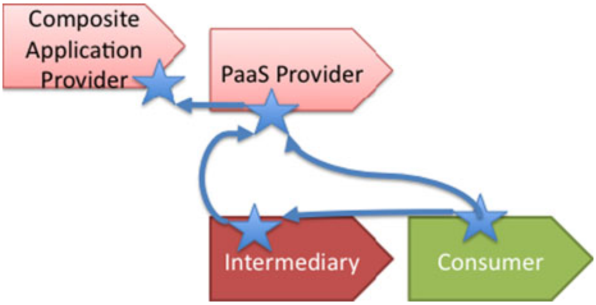

Fig. 5 Outsourcing IT to Platforms a Service (PaaS) providers

strengthen their relationships with their customers. These platforms are being used to gather customer input into product design. Customers are using them to exchange purchase recommendations, and in many cases, consumers are providing post-sales support for their product communities. In these cases, the company is building strong bonds with their customers and collecting a significant amount of data—with significant privacy implications. Consider the example of a Consumer Packaged Goods (CPG) organization that creates a branded social network space to better engage its consumers (see Fig. 6).

This organization has an in-house ERP system that collects customer and sales data for those who have purchased directly from them in the past. To develop the "social" component of their IT infrastructure, they have decided to outsource their community capabilities to a SaaS provider that specializes in supporting online communities. As such, all of the issues discussed above relating to SaaS outsourcing apply to this organization. Next, to initiate the new community, the

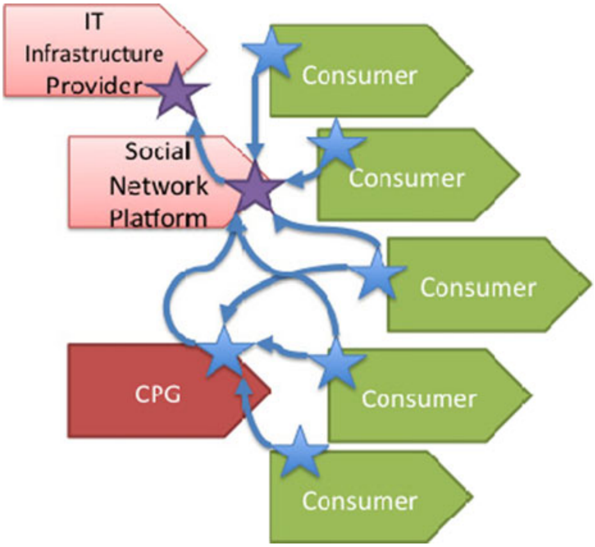

Fig. 6 Personally Identifiable Information shared through social media communities

CPG needs to create profiles for their existing consumers, resulting in personal data being copied from the ERP system to the social network. When considering Privacy by Design, this is a new business use of the data, so new notice and choice options should be developed and made available. Additionally, the CPG's on-line community attracts not only existing customers, but other "fans" of the brand who want to participate in the product design/evaluation discussions. As such, the social network platform is collecting personal data from a wider range of individuals, and their privacy must be taken into consideration as well.

An additional complication arises if the social networking platform has chosen to outsource the actual operation and maintenance of its IT infrastructure; now, as Fig. 6 highlights, a third organization has access to the customer data: the IT Infrastructure Provider. Additionally, the consumer is likely unaware that the Network Platform Provider and the IT Infrastructure Provider handle their personal information. We propose that practical privacy guidelines must be developed to insure that consumer rights are protected in these federated situations (as well as in the other business models). Third party handlers of personal information become a major pillar in trusted federated societies, and if they do not engage in privacy best practices that are definable, measurable, objective, flexible, and well respected, then the rest of the players in the federation cannot really provide assurance to the customers and employees that their personal information is adequately protected.

Summary and conclusions

Designing privacy into the value chain model is a practical, business view of organizational and privacy issues. Too frequently privacy is viewed from a legalistic viewpoint and potential synergies that can result from an organizational-individual positive sum relationship never gets discussed, much less developed and implemented. This puts privacy where it belongs in an organization—everywhere personal information exists. Further, good privacy practices can add value (even if by reducing negative consequences) to an organization and sometimes create a competitive advantage. Further research is needed to consider the internal stakeholders' communications among the various departments within an organization with the goal of better communications and shared values, and we believe the value chain approach helps to further this research agenda. One goal for future researchers is to take the Seven Foundational Principles and develop specific guidance that can be used by organizations to assess privacy practices in a definable, measurable and objective methodology that is also flexible. Also, federated environments necessitate that organizations can "trust" their third parties/intermediaries/cloud computing providers. Research and case studies are needed regarding how these organizations can create value and competitive advantages by voluntarily providing their customers with privacy practice compliance reports. For the most part, the future is bright for the protection of personal information because solutions, not problems are being proposed, researched, developed and implemented.

Acknowledgements We would like to thank Dr. Ann Cavoukian for motivating this research and Michelle Chibba and Estella Cohen for many helpful suggestions. We would like to thank The Privacy Projects for providing the initial funding to establish the Privacy by Design Research Lab at ASU.

References

Aiken KD, Bousch KM. Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. J Acad Market Sci. 2006;34(3):308–23.

Aiken KD, Osland G, Liu B, Mackoy R. Developing internet consumer trust: exploring trustmarks as third-party signals. In: Henderson GR, Chapman Moore M, editors. Marketing theory and applications, Vol. 14. Chicago: American Marketing Association; 2003. p. 145–6.

Capurro R. Privacy. An intercultural perspective. Ethics and Information Technology. 2005;7:37– 47.

Carr N. The big switch: rewiring the world, from edison to google. New York: W. W. Norton & Company, Inc.; 2008.

Cavoukian A. Ontario issues guidance on RFID use. Network Security. Kidlington: Feb 2008. Vol. 2008, Iss. 2;2008, pp 2,20.

Cavoukian A. *Privacy by design: take the challenge*. Office of the Information and Privacy Commissioner of Ontario, 2009.

Cavoukian A, Hamilton T. Privacy payoff: how successful businesses build customer trust. McGraw-Hill, 2002.

Da Silveira G, Borenstein D, Fogliatto FS. Mass customization: literature review and research directions. Int J Product Econ. 2001;72(1):1–13.

David JS, Mann A. The emergence of on-demand software aggregators: implications for developers, customers, and software companies. Proc. Americas Conference on Information Systems (AMCIS), Keystone, CO, 2007.

Dekker HC. Value chain analysis in interfirm relationships: a field study. Manage Account Res. 2003;14 (2003):1–23.

Fiore MA, Lee S-E, Kunz G. Individual differences, motivations, and willingness to use a mass customization option for fashion products. Eur J Market. 2004;38(7):835–49.

Morgan G, Ryu K, Mirvis P. Leading corporate citizenship: governance, structure, systems. Corp Gov. 2009;9(1):39–49.

Hergert M, Morris D. Accounting data for value chain analysis. Strat Manage J. 1989;10(2):175. Retrieved October 22, 2009, from ABI/INFORM Global. (Document ID: 810231).

Hildner L. Defusing the threat of RFID: protecting consumer privacy through technology-specific legislation at the state level. Harv Civ Rights-Civ Lib Law Rev. 2006;1:133–76.

Hosford A. More with less. B2B. 2009;94(8):18.

Kakabadse A, Kakabadse N. Trends in outsourcing: contrasting USA and Europe. Eur Manage J. 2002;20 (2):189–98.

Lee H, Padmanabhan V, Whang S. Information Distortion in a Supply Chain: The Bullwhip Effect. Management Science, Vol. 43, No. 4, Frontier Research in Manufacturing and Logistics (Apr., 1997), 1997, pp 546–558.

Luo X. Trust production and privacy concerns on the Internet A framework based on relationship marketing and social exchange theory. Ind Market Manage. 2002;31(2002):111–8.

McKnight DH, Choudhury V, Kacmar C. Developing and validating trust measures for e-commerce: an integrative typology. Inf Syst Res. 2002;13(3):334–59.

Nehmer R, Prosch M. Privacy, data pollution, organizational responsibility, and the sustainability of information ecologies. Arizona State Unveristy, Working Paper, 2009.

Patnayakuni R, Rai A, Seth N. Relational antecedents of information flow integration for supply chain coordination. J Manage Inf Syst 23(1);Summer 2006.

Porter M. Competitive advantage: creating and sustaining superior performance. New York: The Free Press; 1985.

Porter M. Strategy and the internet. Harv Bus Rev 79(3);March 2001.

Prosch M. Protecting personal information using generally accepted accounting principles and continuous control monitoring. Int J Discl Govern. 2008;5(2):153–66.

Prosch M. Preventing Identity theft throughout the data life cycle. J Account. 2009;207(1):58–62.

Shih D, Lin C, Lin B. RFID devices: privacy and security aspects. Int J Mobile Commun, 2005.

Spreng RA, Harrell GD, Mackoy RD. Service recovery: impact on satisfaction and intentions. J Serv Market 9(1);1995.

Sullivan L. Prison call centers put squeeze on service sector. NPR. http://www.npr.org/templates/story/story.php?storyId=4505278. Downloaded October 25, 2009, 2005.

Supply-Chain Council. Supply-Chain Operations Reference Model. http://supply-chain.org/, 2008