The Driving Motivations of Stakeholders in the Delivery of Privacy by Enterprises

Cyndi Nickel, Tomas Sander, Pete Bramhall

HP Laboratories
HPL-2008-153

Keyword(s):
privacy, compliance, privacy enhancing technology

Abstract:

This paper presents a consolidated view of the requirements of stakeholders of an enterprise's privacy implementation. Because there are so many stakeholders in enterprise privacy, the paper also analyzes the tension between the stakeholders as they relate to purchasing behavior of privacy enabling technology. An action this paper motivates is the creation of technology so enterprises might operate in a privacy-respecting manner. The paper is meant to encourage development of products and services that have maximum understanding and therefore appeal across the various stakeholders. Some of the assertions in this paper are supported by interviews of stakeholders within a variety of enterprises in and across geographies and business sectors, who each have been promised anonymity. Enterprise customers reading this document will benefit from understanding concerns of other enterprise privacy stakeholders, filling gaps or oversights for privacy problems that may be pending but not yet surfaced in their own enterprise.

External Posting Date: October 21, 2008 [Fulltext] Approved for External Publication
Internal Posting Date: October 21, 2008 [Fulltext]

The Driving Motivations of Stakeholders in the Delivery of Privacy by Enterprises

Cyndi Nickel, Tomas Sander, Pete Bramhall

Hewlett-Packard Laboratories

Abstract

This paper presents a consolidated view of the requirements of stakeholders of an enterprise's privacy implementation. Because there are so many stakeholders in enterprise privacy, the paper also analyzes the tension between the stakeholders as they relate to purchasing behavior of privacy enabling technology.

An action this paper motivates is the creation of technology so enterprises might operate in a privacy-respecting manner. The paper is meant to encourage development of products and services that have maximum understanding and therefore appeal across the various stakeholders.

Some of the assertions in this paper are supported by interviews of stakeholders within a variety of enterprises in and across geographies and business sectors, who each have been promised anonymity.

Enterprise customers reading this document will benefit from understanding concerns of other enterprise privacy stakeholders, filling gaps or oversights for privacy problems that may be pending but not yet surfaced in their own enterprise.

1.0 Introduction

The purpose of this paper is to provide an executive overview of the differing privacy concerns of the various stakeholders involved in sharing and protecting private information in an enterprise context. The paper is intended to stimulate technology providers to think about privacy enabling technology, and product managers to think about how to create products that have maximum appeal across the stakeholders.

The various stakeholders do not form a coherent system, and their needs, wishes and capabilities/constraints are highly diverse. The set of stakeholders comprises citizens/consumers, Chief Privacy Officers, Chief Information Officers, Marketing Managers, Corporate Legal Departments and Law Enforcement.

This diversity of viewpoints leads to many tensions, which are addressed in this paper. For example, between citizens, who are confronted by powerful data retention technology accompanied by powerful data mining technology, and Marketing Managers who are willing to use data mining technology to its fullest, barraging them with sometimes unwanted advertisements.

Additionally, in reaction to the unscrupulous who take advantage of, for example, weak authentication in current IT systems to steal citizen/consumer identities, money and reputation, many democratic countries have stepped in with laws to balance the power in favor of citizens. The impact of these laws cascades down to other stakeholders involved in regulation compliance: Corporate Lawyers, Chief Privacy Officers (CPOs), and Law Enforcement. Chief Information Officers (CIOs) are the final stakeholders, tasked with implementing many aspects of privacy policies while maintaining strict cost controls in a dynamic and frequently highly distributed IT environment.

This paper is based on original research to gather, identify, understand and contextualize the expressed viewpoints and opinions of a small number of those stakeholders within enterprises of a variety of sizes in a variety of geographies and business sectors. This was done by means of face-to-face interviews. This research was integrated with secondary research, published by industry analysts and others.

Most original sources are not identified, in line with the agreed terms under which the interviews were conducted. They included three manufacturers of motor vehicles (based in North America, Europe and Japan), two pharmaceutical companies (based in Europe and North America), two North America-based financial services companies, an oil company, a consumer products company, a North American telecommunications service company, a rail transportation company and HP itself. The paper is structured according to the viewpoints of the stakeholders in turn.

2.0 Chief Privacy Officer (CPO) View on Privacy

Using the Chief Privacy Officer as the most central stakeholder, let us examine the role first. A CPO often comes from a marketing, legal or IT background. He or she must balance the tensions amongst stakeholders and create corporate policies that support the needs of citizens, corporate marketing, corporate legal, and law enforcement. He or she must develop a strategy for privacy compliance, issue corporate policies, provide for oversight through governance, insure the workforce is trained and respond to privacy violation incidences.

(Figure provided by Ponemon Institute[1])

As the chart indicates, they spend most of their time advising and consulting the organization and responding to incidents.

A CPO is accountable for privacy regulation compliance, often in very complex environments. Today, CPOs focus on policy creation, supported through manual processes, which are verified by self-auditing processes. So after putting into place a governance foundation, CPOs must make it clear that every employee is accountable for maintaining privacy. Therefore, they put in place a

[1] Ponemon Institute granted the authors the rights to use the diagram provided. Diagram created in 2005.

culture of privacy, which is currently often handled through employee education. This includes education of business process users, business process designers,[2] business process managers, and operators of IT infrastructure. Gartner Research's, John Bace states "Failure to adopt an ethical corporate culture during the next two years will jeopardize short-term performance and long-term survival".[3] As the chart above shows, CPOs also spend much of their time acting as consultants for the rest of their organization, and their efficiency goes up as more and more people become aware of privacy policies, ethics, and their own responsibility and accountability for adhering to privacy policies. Regulators are also beginning to focus on accountability..[4]

In general CPOs do not have budgets for privacy-enabling technology, but rather act as advisors to CIOs in these purchasing decisions.[5]

Following are descriptions of how they spend their time.

2.1 Privacy Incidents

Privacy incidents are foremost in a CPO's mind, and many are even measured by the expense associated with privacy incidents.[6]

Although CPOs desire stronger enforcement mechanisms, today in their complex environments, there is not enough privacy-enabling technology to help them in their daunting task. Instead, CPOs may have help desk organizations, specialized in privacy issues that can respond quickly to privacy violation complaints, thereby attempting to limit the cost of civil suits and increase consumers' and regulators' trust.

2.2 Privacy Compliance Strategy

Strategy for privacy compliance necessarily takes into account rapidly changing legislation landscape and policy trade-offs that balance stakeholder tensions, ensuing IT impact assessment, privacy certification, audit strategies, third party monitoring and breach response. More and more, formal risk analysis is being used to make such decisions.[7]

2.3 Privacy Policy Governance

As creators of corporate privacy governance, CPOs not only establish roles and responsibilities, but also auditing and monitoring processes, reporting mechanisms, employee training, and incident management. They may also be

---

[2] The enterprise systems architect of Company A, a North American telecommunications service company, would like privacy policy converted to privacy design guidelines.
[3] Gartner Research, ID Number: G00143283, December 7, 2006. p 4.
[4] washingtonpost.com . Brian Krebs (Staff Writer). Thursday, February 1, 2007; 10:19 AM. http://www.washingtonpost.com/wp-dyn/content/article/2007/02/01/AR2007020100748_pf.html
[5] This is true of all interviewees.
[6] In Japan, privacy data leakage requires a company to compensate a customer. This means that Japanese companies, such as Company B, a motor vehicle manufacturing company, have a strong metric for doing ROI analysis, along with their Risk Management analysis.
[7] Gartner Research, ID Number: G00143283, December 7, 2006.

responsible for change impact assessment, along with a corporation's CIO. Each change to privacy policy has an impact on systems already implemented. Likewise, changes to business processes may create a privacy issue where none existed before. The impact of these changes must be assessed using change impact assessment processes.

Privacy governance spans many enterprise functions, such as legal, marketing, human resources, information technology, lines of business structures and geographical operations. Establishing a mindset of accountability within the organization via governance is a foremost requirement.[8] Once accountability is established, auditing/monitoring processes can enforce accountability, including third party vendor accountability.

Change impact assessment requires an organization to certify new business processes and applications for privacy compliance. Assessment of all existing applications and their associated data flows helps to determine the existing gap between policy and compliance.

Finally, some corporations are concerned about protecting an employee's privacy even during an investigation into his/her conduct.[9]

2.4 Privacy Policy Development and Deployment as a Means to Avoid Incidents

Incidents create high workloads for a Chief Privacy Officer, and in some cases can lead to dismissal.

Policy development is one of the hardest roles for a CPO. The privacy regulation landscape is rapidly changing in all regions of the world as new laws are instituted. Creating a holistic policy statement for global corporations requires broad knowledge of laws around the world. Some corporations are defining global privacy policies, with regional overlays or modifications.[10] When personal data is transferred across jurisdictional boundaries, corporations strive for policies that agglomerate the different laws.[11] When a universal policy can not be created, data must be tagged with country of origin, and data subject "opt in/opt out" preferences must be kept.

Today, most CPOs enforce privacy policies through self-reporting, manual techniques. This governance structure leaves room for large margin of error, and requires in-depth employee training. With corporation growth and attrition, the education task takes constant attention.[12] More automated policy enforcement is desired, but for CPOs working in complex environments, this seems a little more

[8] Both HP and Company B feel that it is important to establish a strong privacy culture among their workforce.
[9] Company C, an oil company, wants to avoid forensic accidental discovery of unrelated crime
[10] Company D, a European manufacturer of motor vehicles
[11] HP
[12] Company E, a North America-based financial services company, and Company A both advocate more automation with the intent to remove discretion from the employees.

than a dream because of limitations found in the initial offerings of privacy policy compliance assessment technologies.[13] But without technology to support, assist, guide, supervise and take action automatically, human error will leave broad gaps in privacy policy enforcement.

2.5 CPO as Internal Auditor

Generally, compliance to privacy regulations is not formally audited by the governmental regulators. This is especially true outside of the financial industry. For these industries, regulators expect companies to self-audit. When an incident occurs, regulators then become involved, and in some cases levy fines. Additionally, in some countries, citizens can file class action lawsuits.[14] For these reasons, CPOs create internal audit procedures.

2.6 Alignment and Tensions between CPO and Other Stakeholders

This section identifies the alignment and tensions between the CPO role and the role of other stakeholders. These tensions must be balanced so that the broadest number of requirements can be satisfied for all concerned.

2.6.1 Alignment between CPO and Citizen

A CPO, among other roles, acts as an advocate for citizens' viewpoints and needs, and therefore there can be high alignment between a CPO and a citizen. After all, a CPO wants to avoid citizen civil suits and meet the individual data subject's expectations. However, because a CPO is balancing the requirements among many different stakeholders, a citizen may not be completely satisfied with privacy policies that a CPO puts into place.

2.6.2 Tension between Marketing and CPO

As legal liability for protecting personal data increases, a CPO is motivated to collect and store as little of this information, as possible. On the other hand, marketing organizations like to collect and store as much as possible, and furthermore, re-purpose the information when new marketing and sales campaigns are considered.

2.6.3 Tension between CIO and CPO

A CPO must make demands on the CIO and his organization, who is responsible for implementing many aspects of privacy policies in the applications, the IT operational infrastructure and their outsourced managed service providers. A CPO, who might not have a technical background, is often confronted with a CIO's legitimate inability to implement privacy policies due to the lack of proper privacy enabling technology, the expense and complexity of implementing

[13] Company F, a consumer products company, feel that some of the some web site scanning tools fall short of their intended purpose in complex environments.
[14] Scalet, Sarah D. (May, 2005). *The Five Most Shocking Things about the ChoicePoint Debacle*. CSO Maginze. http://www.csoonline.com/read/050105/choicepoint.html

privacy policies, and the resulting fragility of current application frameworks. Today, there is room for consultants to help bridge the gap between CPOs and CIOs, and a large opportunity for more robust computing frameworks and policy enforcing engines for CIOs.

It might be noted that a CISO (Chief Information Security Officer)[15] can have a strong alignment with a CPO because when there is a data breach, a CISO's reputation and career is on the line.[16] The CPO might act as an internal auditor for a CISO, and where this might cause tension, Burton admonishes, "Auditors should not be feared or smeared; they should be steered and revered".[17]

2. 7 Privacy Technology for CPOs

In this paragraph we suggest technologies that are helpful for a CPO.

- **Incident tracking system** to aid a CPO's dealing with customer incidents in an end-to-end fashion. The tool might prescribe a workflow leading to incident resolution, and might include and track escalation paths, etc.

- **Capture and Visualization Tools** to aid a CPO in overseeing the organization's privacy compliance. These tools would support the existing manual processes, and might be forms-driven. Technologies that capture and display evidence that proper privacy controls are in place, and that employee privacy training was conducted as planned, etc. are useful here.
- **Automated assessment tools** that can determine the privacy fitness for privacy-critical parts of the organization. Examples include automated website scanning tools that determine the privacy policy compliance of company websites.
- **Real-time compliance tools** to aid a CPO's organization in monitoring or auditing privacy-relevant aspects of the IT infrastructure to enhance his/her confidence that there is ongoing adherence to privacy principles. This could partially replace manual privacy audits of IT. For example, if the privacy objective states "Data should only be used for the purpose for which it was collected", then the technical implementation of this requirement may include a role based access control system that controls access to customers' personal data.
    - Real-time automation of privacy compliance creates a need to have tools that **check and monitor the health** of these systems, for example, tracking the uptime of this access control system to help ensure that it is available more then 99.9% of the time.

---

[15] A CISO is part of the CIO organization, and is different from a CSO (Chief Security Officer). A CSO might be responsible for site safety, and employee investigations, among other responsibilities.

[16] Carmichael, Martin. *Managing Reputation*. CSO Online. http://www.csoonline.com/caveat/022707.html. (March 23, 2007).

17 Burton Group. Author Fred Cohen. Internal IT Audit: Friend, Not Foe, v1.0, 31 March 2006. pp 2.

    - Implementing this concept requires **tools for modeling the privacy- relevant** aspects of IT, as well as agents that are able to collect the relevant information that will be analyzed for a report.

- To help with the CPO's consulting role, any technology that supports a knowledge base of privacy-relevant knowledge, which is easily searchable, with an intuitive search engine that returns relevant information.
    - Making the privacy rule book of an organization easily searchable would be a good first step.
    - Privacy Impact Assessment tools can be used by a CPO to provide support to other developers of products or backend systems which have privacy-relevant components. Through the use of forms and checklists, these tools would flag whether privacy-relevant problems exist in a planned project, and then identify a privacy expert to consult.

Of course a CPO gains benefit from a number of other privacy enhancing technologies used within a company; however we do not mention them in this section, as the CPO's organization is most likely not to be the direct user of these tools.

3.0 Chief Information Officer (CIO) View on Privacy

Another stakeholder is the Chief Information Officer, who is tasked with implementing business systems that conform to a CPO's privacy policies. CIOs are most vocal about needing technology to help enforce privacy regulations. [18] At the same time, they are most aware of the complexity in their computing infrastructure, and the least likely to believe that current privacy enabling technology can solve the breadth of their problems.

Privacy policy implementation is done step-wise, and privacy enhancing technology will also be adopted incrementally. Successful creators of such technology would need to accommodate this.[19] Therefore, new privacy-enhancing middleware is only an acceptable solution if it is transparent to existing application frameworks.[20]

3.1 Process Design and Assessment

With the occurrence of every new regulation, CIOs can be tasked by their CPOs to do an assessment of its impact on their business processes, applications, and IT infrastructure. These assessments can be time-consuming and expensive. CIOs need tools to help with the assessments, looking at business workflows,

[18] Company G, a pharmaceutical company, and Company D both feel that security and privacy can not be effectively implemented using only manual processes.
[19] Company D
[20] Company D

data flows, access control, web site conformance, application designs and information (lifecycle) management. Data flows in an actual operating environment must also be examined to identify transborder data flows, i.e., those that cross jurisdictional boundaries. Auto-scanning tools might be of interest, as assessments can be time consuming.[21]

Additionally, as new applications are designed, architects must design for privacy. This means that designers need awareness of the corporation's privacy policies. Among designers, there are differing opinions as to whether owners (or collectors) of the data should set the policies, or a central/corporate body should set them and then cascade them to the regions for final regional application of policies that conform to local law.[22] If the owners of the data set the policy, then a "sticky" policy approach is likely be taken; if central policy-setting is advocated, then middleware policy enforcement engines will tend to be advocated.[23] (A "sticky" policy is one where the privacy policy is attached to the data, and travels with the data with every data access. Applications using the data are expected to implement the privacy policy.)

Just as application designers must design for privacy, managed service providers, and their customers must also take privacy into account. Many jurisdictions currently include in their privacy regulatory approach the notions of Data Controller and Data Processor, in which the former is ultimately responsible for compliance of his own enterprise and also of third parties who store and/or process personal data on the former's behalf. This separation of responsibility may be eroded or removed as a consequence of a number of upcoming changes in regulatory basis that are under consideration in various forums worldwide, e.g., an enhanced US Federal privacy law, the APEC privacy framework.[24]

3.1.1 Information Technology Privacy Change Management

Once an assessment is made and the gap between privacy policies and the computing environment is identified, a corrective action plan is required. Therefore change management of the computing environment, the educational systems and the governance systems, are required of the CIO and CPO.[25]

3.1.2 Design for Privacy

Education is needed to help a designer implement an application or business process that conforms to privacy regulations, and that is flexible so it can be modified as new regulations come into force. Burton Group states that system

---

[21] Company A's enterprise systems architect
[22] Method used by Company D
[23] Company B and Company D both mentioned this
[24] Richard Thomas, UK Information Commissioner, opinion expressed at the IAPP Summit, Washington DC, March 2007
[25] Caldwell, F., Brittain, K., Heiser, J., Bace, J., Adams, C. (2006). *Predicts 2007: Building Business Value With Risk Management, Ethics, Governance and Compliance.* Gartner Research. (ID Number: G00143283) Gartner states, "The advent of governmental regulations has spawned a more potent set of drivers for greater attention to ITCM and the need to develop a common governance approach to meet compliance audit demands".

architects are expected to implement privacy policies and are held accountable even when privacy policies are created elsewhere.[26]

3.1.3 Special SOA Concerns

Special considerations for Service Oriented Architectures (SOA) applications are suggested, as they may have a high degree of third party involvement, which has a heavy impact on privacy policy compliance. Service Oriented Architectures are architectures that uses loosely coupled services to support the requirements of business processes and users. Resources on a network in an SOA environment are made available as independent services that can be accessed without knowledge of their underlying platform implementation. These concepts can be applied to business, software and other types of producer/consumer systems.[27] SOA designs are becoming popular because they can respond quickly to changing business needs. However, the need for privacy policy compliance functions complicates these designs, and can make them more difficult to implement, as privacy compliance negotiation between services is not yet standardized. [28] Some companies are creating services in-house, so the company can dictate the compliance framework. Some standards bodies have attempted to create compliance frameworks, with limited success so far, and some large application vendors are trying to drive standardization of these frameworks;[29] notably, however, a few important major players are not joining in this endeavor, thus leaving the industry fragmented.

3.2 Third Party Access to Private Information

Since the use of third parties is so widespread, the handling of shared information and the oversight required must be part of third party assessment.

When a company provides managed services, implementing their client's privacy policies is often a contractual requirement or legal obligation; however, this can be difficult to achieve, given today's technology. In the case of process outsourcing, some companies even allow the data subject to choose whether to allow their data to flow across country boundaries.[30]

---

[26] Burton Group. Authors: W. Scott Blackmer, Esq., Mike Neuenschwander, Lori Rowland. "Data Protection and Human Resources: Bridging the Gap Between Privacy Policies and Information Practices". Version: 1. July 14, 2006. ISSN 1048-4620.

[27] Barry, Douglas K. (2003). *Web Services and Service-Oriented Architectures: The Savvy Manager's Guide*. San Francisco: Morgan Kaufmann Publishers. ISBN 1-55860-906-7.

[28] Company B is moving to adopt SOA (Software Oriented Architecture) frameworks and want to be sure that Privacy Enabling Technology supports SOA architecture. However, they store personal data locally.

[29] Massimo Pezzini, Yefim V. Natis, Kimihiko Iijima, Roy W. Schulte, "SOA Group Takes Step Toward Standardization". Gartner Research. Publication Date: 2 August 2006. ID Number: G00142324

[30] Company E allows the borrower to decide whether his/her loan will be processed in India or remain in the US for processing.

3.2.1 Across Company Boundaries

Different companies have different privacy policies, and transferring customer information from one company to another requires an examination by both companies regarding their interpretation of the law.

Sometimes de-identification or anonymization of data before it is sent onward can be useful.[31] Or actual prevention of data flow beyond a corporation might rather be desired. In any case, it is difficult to enforce a right to update or delete personal information, as may required by law, when data crosses company boundaries, and a confirmation mechanism is needed to ensure a third party has updated PII as requested.[32] Some companies write contracts with third parties that give them the right to audit privacy policies on personal data sent onward to them.

3.2.2 Across Country Boundaries

Different countries have different regulations; so again, an enterprise's privacy policy must take these into account. Some country's laws limit the flow of private data across country boundaries, but there is very little technology to help limit such illegal flow of data.[33] When private information crosses jurisdictional boundaries there is yet another complicating legal concern. Nations are beginning to impose their own laws when their citizens' private data flows to other jurisdictions. Europe and Japan are leaders in requiring compliance to their laws wherever their citizens' personal information flows.

3.2.3 Giving People the Ability to Access and Correct their Private Information

In many jurisdictions, every citizen must be given the opportunity to access and correct or update their stored personal information. When their information is spread across many databases, spreadsheets and data stores, this can be problematic. Moreover, when companies use third parties in their business workflows, locating and updating the data, at the request of data subject, this adds complexity.

3.3 Information Technology Outsourcing or Managed Services

Infrastructure Managed Service providers have special concerns when it comes to privacy. In general, an infrastructure managed service provider is responsible for the security of an application environment. The most fundamental element and pre-condition to privacy is security of the IT assets and the data they contain. However the ITO provider typically does not need to access individual data themselves but deals with them in bulk. Clearly, from an infrastructure provider perspective, privacy concerns have to do with the management of these bulk

[31] Company C
[32] Company C
33 Company D indicated that German law restricts migration of their citizens' private data

data. Relevant solutions include storage encryption, secure deletion of data and destruction of media containing them, as well as,technologies that support change management when data move within or between data centers. Privacy is different from security. However, compliance to privacy policies can be delivered only if the means for doing so are built on a foundation of a secure environment.

Business process outsourcing (BPO) has a number of additional privacy concerns, which need to be addressed in technical and non-technical ways. Compared to ITO operations, BPO is often highly people intensive and BPO employees touch privacy-sensitive data directly (e.g. when HR operations are outsourced.) An internationally operating BPO provider must be able to support a variety of applicable regulations and a BPO provider is contractually obligated by the client to put a number of privacy controls in place. Providing reliable privacy and data protection measures is of key importance for BPO providers, as outsourcing customers require strong reassurance that their data are safe in the outsourced environment. Data leakage is the most important risk. Data leakages in outsourcing scenarios can be highly publicized which creates a huge risk to reputation

Thus for BPO providers, technologies that identify and manage the appropriate privacy controls for a specific set of regions from which the data originate are important. In addition technologies that anonymize or deidenitfy data as they flow to a BPO provider help mitigate risks. Auditing and monitoring technologies which are tailored to BPO operating environments are useful to detect suspicious activities early on.

3.3.1 Identity Management

Authentication, authorization, and access control via identity management tools are the foundation of privacy policy implementation for managed service companies. Unfortunately, current identity management technology might not have enough fine-grained control. Managed Service providers might have to support multiple access control systems. CIOs of large, global corporations – especially ones from corporations that have undergone acquisitions – may have an additional complication of using several different vendors' identity management systems.[34] Implementing and operating access controls can require significant effort, so some companies are moving towards consolidating PII into one data set so privacy compliance can be more easily enforced.[35] Others have a highly distributed approach, with each business unit controlling its customer identity management strategy.[36] And these distributed approaches may have a high degree of complexity; one company cited over 32 instances of

---

34 Company D notes the difficulty of implementing privacy policy due to multiple identity management software systems used in their environment. They also have distributed privacy policy implementation.

35 Company C, Company D and HP

36 Company A and Company C have local storage of personal information. Company A cited performance reasons for doing this.

PeopleSoft databases in their company.[37] Others have a hybrid approach, keeping local application data stores as "caches" for performance reasons, but centralizing the data for policy enforcement.[38] All these different aspects of access control can make business process outsourcing difficult.

3.3.2 Data at Rest

The privacy of data at rest is supported by means of access control mechanisms and increasingly encryption technologies. Fine grained access control (e.g., on a field level) are helpful to implement need-to-know based access control policies to data..Storage encryption is a key step to mitigate risks of lost or stolen storage media.

3.3.3 Data in Motion

Data can be at risk when it is in motion. Crossing country or company boundaries should be limited, which might not be possible in today's business environment. Unintended crossing of country or company boundaries should be prevented. [39]

Encrypting, redacting or anonymizing data before it is copied from one location to another, adds a degree of communications security and is also essential if the destination is a physical device which can be removed from a physically controlled secure environment and is thus at risk of theft or loss.

3.3.4 Audit Logs and Privacy

Audit logs can contain immense amount of private information that could be reconstructed with the right data retrieval and mining techniques, thus creating a potential privacy breach situation. Law enforcement agencies make extensive use of audit logs to identify and convict criminals, so their officers would like free access to audit logs. However, in some countries, subpoenas limit law enforcement actions to focused and directed discovery, which complicates protecting the privacy of those not under investigation while exposing information about those who are.

3.3.5 Information Life Cycle and Privacy

Some companies have stipulation for retiring personal information after it is no longer needed, thus reducing their legal risk. Managing these obligations is an important part of information life cycle management of private information.

3.3.6 Privacy Policy Enforcement Engine

The responsibility to enforce an enterprise's compliance to changing regulations (and changing interpretations of existing regulations) makes some CIOs wish for a comprehensive privacy policy enforcement engine. [40] Some companies are

[37] Company C
[38] Company G and HP
[39] Company D
[40] Company E

hanging onto the promise of SOA to provide a mechanism for privacy policy enforcement, which then forces centralization of policy.[41] SOA can help solve privacy issues when the applications are written in-house and policy taxonomies can be agreed. This becomes much more complicated when third parties are involved, as solid standards are not yet in place.

3.5 Privacy Technology for Designers

Designers will benefit from tools that facilitate building their solutions with privacy in mind. Thus educational tools and check lists are an important first step . Technological frameworks are building blocks that make it easy to incorporate privacy enhancing capabilities and policies into systems. Examples are standard libraries that provide privacy-relevant functionalities such as pseudonymization and redaction. (Redaction technologies black out or hid data, in a secure fashion, from documents or structured data. This privacy-enhancing redaction functionality can also be realized in conjunction with integrity mechanisms such as digital signatures on documents or audit trails which makes this a powerful tool, e.g. in compliance scenarios.) Other examples are the availability and widespread support of policy languages that allow privacy policy expression, which can then be enforced by an application.

3.6 Privacy Enabling Technology for CIOs and Managed Service Providers

This section enumerates technology explicitly for CIOs and for managed service providers.

- First there is a need for tools that allow for modeling of business processes and data flows from a privacy perspective. Among these tools might be an assessment tool that automates discovery of data flows.
- At a business level, CIO's need risk-assessment tools, because spending has to be balanced with real risk likely to be encountered.
- Privacy-aware policy enforcement engines can enforce privacy-enhanced access control policies at a database level, or filter out data at a SOA messaging interfaces level. Tools that allow expression and transfer of privacy preferences and policies between organizations are also important, allowing for exchange of data between organizations, so that the receiving organization can more easily determine the appropriate privacy aware data handling.
- To manage sensitive information in audit logs, tools provide for pseudonymization and aggregate reports are needed. Ideally these tools still check for the authenticity of the derived data, as data integrity is often a major concern for audit trails.

[41] Company B and Company C

- An encryption tool for data storage, along with simplified encryption key management is needed. This encryption works best when the platform is a "trusted" device, and makes use of TCP (Trusted Computing Platform) modules to form a root-of-trust.
- Information Lifecycle Obligation Management Technology can ensure the timely deletion of data from the system.
- Email filters for outgoing email are a useful, (in countries where this is not prohibited by citizen privacy laws), for preventing privacy-sensitive information leaving the organization.
- Scanning technologies that allow the detection of privacy-sensitive information on networks or PCs will help an organization to determine if privacy- sensitive information is residing there contrary to policy, and allow the taking of the appropriate action.
- Widespread adoption of encryption technology for storage media would be highly desirable and would mitigate many risks coming from the loss or theft of storage media.

4.0 Citizen View on Privacy

Although sometimes overlooked in the holistic system of privacy stakeholders, citizens are the big stakeholders, and privacy is one thing that the private sector, public sector, and citizen advocacy groups value in common. With the increase in government privacy regulations, they are also becoming more powerful.

Citizens, both consumers and employees, desire privacy because it helps make them safer, and it protects the integrity of their identity. Even though citizens desire their privacy, they are willing to share information about themselves under certain conditions. On the other hand, in many (but not all) jurisdictions, employees can expect little protection of their privacy while at work.[42] However, corporations are legally liable for the protection of the personally identifiable data they hold and process.

4.1 Privacy Makes Citizens Safer

Citizens feel that privacy makes them safer, and governments around the globe tend to support them in this belief, increasingly enacting laws that enhance their citizens' rights to privacy. Governments help balance the power in this system of stakeholders ; without laws, citizens would not have the level of privacy protection they currently have. Citizens rely on privacy regulations to protect themselves, their children and other dependants, e.g., ageing parents.

[42] W. Scott Blackmer, Esq., Mike Neuenschwander, Lori Rowland. (July 14, 2006). *Data Protection and Human Resources: Bridging the Gap Between Privacy Policies and Information Practices, Version: 1*. Burton Group. Document Id: 5878. p 16..

Citizens want to keep their children and their ageing parents from online stalking that might lead to physical stalking[43], and several countries have put laws into effect to protect these innocent and unwitting people from falling prey to this new form of danger that is generated from revealing too much about oneself on the internet. Another form of stalking is online spyware that tracks a citizen's activity as they browse around the internet, or tracks a citizen's purchasing behavior. [44] Worse yet is the threat of crime-motivated spyware that steals citizens' identities.

Citizens feel privacy-enabling technologies help protect their resources[45], both computing and personal time consumed by dealing with spammers and intruding telesales. Ad barrages, some of them explicitly offensive, prevent citizens from enjoying their internet experiences. Much effort has been placed on preventing spying by advertisers collecting internet browsing behavior, consuming computer storage and processing bandwidth, uploading their spy-logs to their central server. Citizens resent the intrusion and theft of their resources.[46]

One of the most serious resources that can be stolen is the integrity of a citizen's name, and his/her creditworthiness or trustworthiness. A lack of authentication mechanisms in this new internet age creates opportunities for the unscrupulous to masquerade as someone else, ruining a citizen's reputation, eroding their wealth, and making them vulnerable to false accusations. As more and more websites, from e-Bay to online dating sites, keep trustworthiness indexes on visitors, citizens' reputations become more and more important to them.

In some cases, loss of control of private information, especially relating to medical conditions and insurance applications, can cause economic hardship and discrimination, In some cases, without privacy safeguards, fresh-starts are not possible. For example, unwise adolescent actions may be re-discovered many years later as they try to build a favorable reputation, e.g., for employment, credit or public office purposes.

Although governments, especially democratic governments, are placing laws into effect to protect a citizen's privacy, many citizens are still worried about governments themselves overstepping their own boundaries in their vigorous pursuit of crime and terrorists.

There is growing public dialogue on whether or not the internet is legally considered public space or private space. Some fear that freedom of speech will be restricted without sufficient privacy to congregate online.

---

[43] Moore, Alexis, Victims Advocacy. (May, 2005). Commentary on: *The Five Most Shocking Things about the ChoicePoint Debacle*. CSO Maginze. http://www.csoonline.com/opinion/comments/10478.html?action=print l

[44] Privacy International. Overview -- Growing interactivity means growth of personal information. September 8, 2004. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65425&als[theme]=Communications%20surveillance

[45] Alessandro Lega, Managing Director, TraiCon a Consultancy&Traininig Company of DAB Group. (May, 2005). Commentary on: The Five Most Shocking Things about the ChoicePoint Debacle. CSO Maginze. http://www.csoonline.com/opinion/comments/5143.html?action=print.

[46] Scalet, Sarah D. (May, 2005). *The Five Most Shocking Things about the ChoicePoint Debacle*. CSO Maginze. http://www.csoonline.com/read/050105/choicepoint.html

4.2 Conditions for Citizens Who Share Private Information

A citizen's sharing of private information is context-specific and depends on their trust of the recipient, how much control they have over the secondary use of the information shared, and the benefit they receive in return. Naturally, the more trust a citizen feels the more they will share. This trust is built on their perception that their data will not be used to cause them harm, and furthermore that there will be a benefit to them for the exchange. In some cases, when anonymity is offered, the benefit can be rather small, e.g., as with grocery store loyalty cards that track product purchases in exchange for coupons. Other times, citizens share in exchange for being known as a particular persona, i.e., a specific partial identity, as in MySpace, YouTube, Linked-In, and other social networking sites. The Ponemon Institute found that consumers felt that anonymity, trust and convenience were important when they considered giving up privacy so they could have a personalized portal.[47]

4.2.1 Information Citizens Need When Deciding to Share Private Information

Citizens are demanding control over sharing with basic "opt in/opt out" capability. As they are deciding, they need some basic information:

- Transparency about how broadly the data will be shared and who has access to the information
- Notice of and restriction on how the data will be used
- Accuracy of the information maintained about them, and the ability to update the information
- Knowledge of information flow across national boundaries into regions with different laws about privacy
- Notifications when control of the private information is lost, as in security breaches

Most of these are impossible for a global enterprise to guarantee, as it is impossible for an enterprise to predict all the future scenarios in which it will operate. There are also many practical difficulties in providing the information and control today, owing to the complexity of many enterprises' systems and processes and business models.

4.3 Privacy Technology Needs for Citizens

The previous Section lists various privacy concerns in which citizens would benefit from technological assistance.

Giving citizens simple ways to manage and control the dissemination of their personal information is crucial. Also the availability of anonymization and pseudonymization technology is an important step towards protecting their privacy. In particular, identification schemes that avoid usage of government-specified identities, such as the Social Security Number, are important steps to

[47] ComputerWorld. Larry Ponemon. "Will privacy concerns thwart personalization efforts?". July 10, 2006.

protect them from identity theft. Citizens typically expect these privacy measures to be easy to use right out of the box and to be embedded in the technology they are using. No steep learning curve should be required.

This applies also to a number of emerging technologies. We just list a few examples, such as those supporting social networking and community sites, location-based services, telematic services in cars (e.g., which collect information about the car, driving behavior and provide directions for the driver), RFID technology, etc. Citizens benefit greatly if such applications, services and products have been designed with privacy in mind from the beginning.

4.3.1 Emerging Technology

There is a variety of technical approaches to providing the individual citizen with the means to manage his/her digital identity information and control its release and subsequent use by others. These range from approaches in which all communication and interaction between citizen and enterprise is done on the basis of anonymous credentials (i.e., no identity information is transferred) to those in which the enterprise's identity management systems are designed to follow all the citizen's requirements regarding his/her identity information (and thus act as his/her proxy) and are verified as actually doing so.

4.3.1.1 PRIME

Some of these technical approaches are being further researched and developed within the PRIME project, a 4-year co-operation between 20 industrial and academic research institutions, that aims to advance the state of the art of privacy-enhancing technologies. It is part-funded by the European Union, and its scope includes technologies and system architectures, reference prototypes and application trials, all within a context provided by legal, social, economic and human factors requirements for these. Hewlett-Packard Laboratories is one of the leaders of the project. Refer to www.prime-project.eu .

4.3.1.2 Microsoft CardSpace™

Microsoft Corporation has developed a system, which is marketed as Microsoft Windows CardSpace™ ,for creating identity relationships with websites and online services. It is not inherently a set of privacy technologies, but provides a consistent way for an individual to manage his/her personal details and the release of these to an enterprise. It is based on the notion of Information Cards, which can replace the user names and passwords that an individual would otherwise use to register with and log on to websites and online services, and includes protocols and mechanisms to aid the individual in deciding which set of information to share with whom.

There are two types of card: Personal cards and Managed cards. The former are created by the citizen and are stored on his/her client device; they contain the usual sort of personal information, e.g., name, address etc. Managed cards are created and managed by a managed card provider, and are stored by it; such

providers are therefore able to act as an identity provider on behalf of the citizen, potentially adding value by providing reliable attestations of the citizen's asserted identity information or credentials.

5.0 Marketing Manager View on Privacy

Many Marketing Managers place high stock in a citizen's trust in their brand. The respect a company shows towards its customers is often reflected in the way it honors a citizen's privacy preferences and protects them from identity theft. Gartner states, "Regulatory compliance is something companies have to do — they are under compulsion to comply. But why are many companies exceeding what is required by law at their own expense? Few are forced to implement good risk management, ethics programs, CSR initiatives and governance best practices. Frankly and unabashedly, they are doing so because it is good for business."[48] Companies we spoke to reinforce this statement.[49]

Yet, Marketing Managers also need to collect information about a citizen's purchasing habits, in order to sell more directly to their needs, using data mining and statistical analysis techniques. High-impact marketing campaigns need correct, up-to-date customer contact information, along with "over contact" management and oversight; thus protecting the company's reputation and dis-association with spam. Many of these campaigns are outsourced to third parties, so protection of customer data as it flows across company boundaries and some cases country boundaries is problematic.

When companies have business models that are driven by advertising revenue, privacy relationships between customers and these corporations are fraught with tension

5.1 Alignment between Marketing Managers and People

Marketing Managers are aligned with people when customers feel desirable purchase opportunities and product information are provided. Amazon.com and Netflix are leaders in using purchasing and browsing behavior to make recommendations-of-worth to the customer. More and more information portals are beginning to auto-configure themselves based on a person's browsing behavior, thus giving the person a better online experience that is customized to their interests. Both Marketing Managers and customers want corporations to have up-to-date contact information when a customer chooses to "opt-in".

When business-to-business services are provided, employers want over-ride "opt-in or opt-out" capability for services provided to their employees. Employers do not want their corporate email servers overwhelmed by spam from one of their own third-party service providers.

---

[48] Caldwell, F., Brittain, K., Heiser, J., Bace, J., Adams, C. (2006). *Predicts 2007: Building Business Value With Risk Management, Ethics, Governance and Compliance.* Gartner Research. (ID Number: G00143283).

[49] Company E

Marketing Managers, using CRM systems, do statistical analysis on data, which often contains citizens' private information. Statistically correct correlations are important to Marketing Managers, and if there was a way to anonymize or de-identify the data and still have statistically correct results, Marketing Managers and people would both benefit from this. The desire to use de-identified data is most important when the outcome might have adverse impact on the person, such as data used in medical research..

5.2 Misalignment between Marketing Managers and People

People are often suspicious of the real or potential flow of information to other companies or countries. Complexity of laws, in different regions and countries, create a difficult situation at best. Third party leakage of a person's private information is as damaging to a corporation's reputation as if they had leaked the information themselves. But sometimes corporations fail to take full oversight responsibility of third party treatment of personal data, despite a legal requirement to do so in many jurisdictions. Corporations often state in their privacy agreements that onward flow of private information will occur in the course of serving the customer, but they do not inform the customer who these third parties are, or how private information is updated by the citizen or, better yet, removed.

There are a number of organizations that offer privacy certification trust marks that can be used to raise citizen confidence, for example, the TRUSTe and BBBOnline certification marks. Making this a requirement of third party vendors may help alleviate some concerns a citizen has about onward data flow.[50]

Yet another problem occurs when Marketing Managers purchase lists from third parties or from their advertising agents. Customers in the marketer's database may have opted-out, yet still be sent unwanted material via the third party on behalf of the originating party. Customers view this as spam and are provoked by their inability to make an "opt out" stick.

5.3 Privacy Technology for Marketing

For marketing teams it will often suffice to data mine anonymized or de-identified data, where statistical correctness is maintained.

Contact management tools (e.g., embedded in CRM systems) will help them to provide company contact management, which allows them to avoid "over-contacting" the customer.

In addition marketers also have an interest in tools that ensure high quality of the data about customers, e.g., by including ways to enhance their correctness, avoiding duplicates etc.

[50] Ari Schwartz,Deputy Director of Center for Democracy and Technology, interview on March 6, 2007.

6.0 Corporate Legal Department View on Privacy

A corporate legal department is concerned about protecting the company from legal action, and should one occur, ensuring that legal damages are limited. Corporate legal departments are tasked with keeping up with a rapidly changing privacy regulation landscape. For global corporations, the problem is even more difficult, as laws between regions and countries can conflict. Many corporations are lobbying law makers to make more uniform laws so that compliance can be achieved. [51] In the meantime, transborder personal data flows receive a lot of their attention.[52] For legal departments, placing all the privacy-sensitive data in a central location and keeping it there, would simplify their legal advisory role.[53]

6.1 Tension between Corporate Legal and Marketing Organizations

Since brand drives business, marketing organizations want protection of their brand, which often means going beyond the minimum legal requirements for privacy protection; legal departments want to protect the corporation from damages and therefore take a defensive approach to privacy compliance, desiring implementation of the minimum required by law.

However, as described in Section 5, Marketing Managers sometimes want to access and use personal data for purposes which go beyond those that were notified to the data subject at the time of collection, and this is illegal in some jurisdictions.

6.2 Privacy Technology for Corporate Legal

For global corporations it is challenge to stay on top of international privacy laws and requirements. Knowledge management tools that give legal teams more systematized access to this knowledge would be useful.

7.0 Law Enforcement View on Privacy

Law enforcement agencies' goals are to prevent crime and to catch criminals, and they need forensic information in this pursuit. Corporate investigations have very similar concerns, when investigating employee misconduct.

Much of the forensic information in this digital age is kept in audit logs. To date, many of these logs contain citizens' private information, either direct information, constant pseudonym information (e.g., nicknames) and transient linking information such as IP addresses. It has been suggested that more and more transparent auditing would better support criminal pursuit.. In their opinion, white

[51] HP and Microsoft, among others, have strong lobbying capabilities in Washington, DC.
[52] Company C says that employee record transborder data flow receives a lot of their legal attention.
[53] Company A and Company B both made the point that personal data is currently widely distributed in their company, and it would be easier to enforce regulations if the data were centrally located. Company C tries to solve the problem by creating binding corporate rules that are distributed to the regions, who translate them for local regulations.

collar crime is more effectively deterred with highly publicized apprehension than attempts to secure private information against theft.[54]

7.1 Tension between Citizens and Law Enforcement

Some private information, e.g., financial and medical information, is protected by regulation that is enforced via regulatory auditing agencies. However, much privacy regulation is enforced mainly by citizens filing civil law suits, not by government or public agency auditors and regulators.

Citizens want law enforcement to protect them from crime and terrorists. But citizens are not happy about just capturing an identity thief only after the damage is done, because they are left with fallout that often takes multiple years to clear up. Citizens are demanding prevention ahead of detection and prosecution.

Additionally, some citizens fear governments overstepping their boundaries. [55] Governments rightly fear terrorists and criminals plotting via the internet, and want to protect citizens from harm. But when it comes to investigations, people want the judicial system to provide checks and balances, requiring law enforcement agencies to provide probable-cause.[56] Citizens want subpoenas to be limited to specific identified targets. This has an impact on the handling of private data in audit logs.

In nations where freedom of speech has been curtailed, or dissent has carried serious reprisals, citizens demand stricter privacy laws[57].

7.2 Privacy Technology for Law Enforcement

Law enforcement agencies will benefit from technologies that maintain fine-grained access control to data and that include pseudonymization capabilities. Auditing technologies with analytical capabilities are important means to detect privacy breaches in the organization.

Technologies for privacy-enhanced information sharing between different agencies are also useful.

Privacy-enhanced technologies such as audit log redaction and pseudonymization may also ultimately benefit law enforcement as they reduce the resistance of corporations to hand over privacy-sensitive data.

---

[54] Hal Abelson, MIT professor, Professor of Computer Science and Engineering.

[55] McCullag, Declan. (September 17, 2001). Geeks Gather to Back Crypto. Wired News. http://www.wired.com/news/politics/0,46900-0.html

[56] Americans for the Preservation of Information Security have formed to help protect US citizens. http://vees.net/freedom/

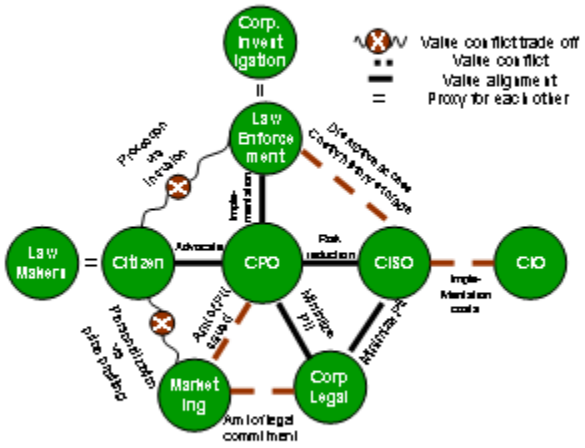
[57] Privacy International, an international privacy advocacy group. http://www.privacyinternational.org/

8.0 Sociogram for the Chief Privacy Officer

Sociograms can be useful to product managers who are devising products that appeal to all decision-makers involved in a product purchase. Privacy-enhancing products have a large and diverse set of stakeholders. At the least, both CPO and CISO must buy into the purchase of privacy enabling technology.[58] For example, in the case of privacy policy modeling tools, Legal, Marketing, and the CPO would have to be in alignment with each other. Admittedly, the decision-making is complicated,[59] and requires a strong integrated governance and decision making.

The sociogram below summarizes the value alignment and value tensions between stakeholders. This sociogram does not try to capture the dynamics of the interaction of the players, which are highly dependent on personalities, but rather the fundamental values the various roles necessarily embody.

Values Based Sociogram (fig 2)



[58] Company E advocates creating marketing messages for privacy enabling technology that appeals to both the CPO and the CISO.
[59] Company C and Company D

In this sociogram, in regards to privacy, law-makers are a proxy for citizens, and furthermore balance the power towards the citizen and away from the corporation. CPOs must become an advocate for privacy regulation enforcement, and therefore, indirectly, an advocate for the citizens.[60] To help motivate this advocacy is a real concern that citizens can become a source of class-action law suits. Citizens want personalized products and online experiences, but they do not want to be price-profiled. Likewise, citizens want to be protected from crime, but they don not want government intrusion into their privacy.

Both CPOs and CISOs are mutually motivated to reduce risk of a breach[61], which is in tension with a CIO's desire to keep costs constrained. A focus on risk analysis based decision-making, when it comes to privacy compliance spending, is highly appreciated by a CIO.

Marketing departments want to win a citizen's trust, in order to have more data on him/her, so they can better produce products for premium prices. Collecting data is key to their success, but CPOs do not want the liability of unnecessary data collection. Corporate legal departments are in agreement with a CPO in regards to limiting the collection of data that puts the corporation at risk. Likewise, legal departments do not want marketing departments to promise, in a privacy statement, more than required by law, but would rather like to keep privacy statements lean, in order to reduce an opening for a law suit. A CIO is in full agreement with the legal department, but only so costs can be contained.

Corporate investigations, as sometimes represented by law enforcement agencies, provide a CPO with strong justification for implementing privacy compliance programs which include internal audits. Audits, internally or externally, increase costs and complexity within an IT organization, and consume personnel, which can be disruptive to the normal flow of the organization. Full-blown investigations can also play havoc in an IT organization, even when the investigation is conducted by an internal investigation team.

This system of values will come into action when privacy enabling technology purchases are being reviewed. Products that appeal to a CPO, CSO, and the corporate legal department, and which support the goals of citizens and law enforcement agencies have the best chances for success.

[60] Scalet, Sarah D. (February, 2005) Five Things Every CSO Needs to Know About the Chief Privacy Officer. CSO Maginzine. http://www.csoonline.com/read/020105/fivethings.html
[61] Company E made this observation

9.0 Conclusions

As the Sociogram shows, the strongest motivational links are between the CPO, CISO, Corporate Legal Department, and Law Enforcement. Privacy enhancing technology that makes use of that strong linkage will most likely lead the market.

This would lead researchers and technology developers to focus on items like:

1) Assessment tools that will automate the mapping of data flows.
2) Fine grained access control technology that allows to implement need-to-know based access to personal data.
3) Audit logs that assist law enforcement and corporate investigations, while securing privacy for those not currently under investigation.[62]
4) Privacy Policy modeling tools that link to Security Policy modeling tools. These policy modeling tools must be understandable by the Corporate Legal department, which has a stake in risk assessment related to privacy policies.
5) Risk assessment tools that allow Corporate Legal, the CPO and the CISO to balance the needs of the other stakeholders.

While there are many other technologies that could be created, these are strongly indicated.

The interviews, that formed the primary research upon which this paper is based, were anecdotal in nature. Although their revelations are supported by secondary market research, more quantitative data is needed from Industry Analysts.

[62] For example, encrypted identifiers that need subpoenas to decrypt but let law enforcement agencies discover patterns, so they can collect enough evidence to justify probable cause.