Use of Employee Information Framework
White Paper

October, 2008

Acknowledgements

We greatly appreciate the valuable contributions from the RIM Council Use of Employee Information Working Group under the leadership of Gail Magnuson, Global Data Privacy Director, Manpower Inc. This whitepaper is the summation of a number of significant reference documents created and validated by the working group that lays the foundation for the Use of Employee Information Framework.

Table of Contents

Introduction

This paper addresses the issues that employers, providers and regulators face in working together to build trusted relationships with employees around the world in order to engage the total workforce. Maintaining the privacy of employee information not only is the right thing to do but provides significant business benefits in hiring and retaining people. Ponemon Institute's "Most Trusted Companies" studies have shown that building customer trust in a brand is an important product differentiator. Building trusted employee relationships through maintaining the privacy of employee information can also provide benefit to brand, image and the work environment.

Maintaining the privacy of employee information is not easy. There are legal, technical, logistical, monetary and global business considerations that impact management decisions. So how does an enterprise determine their path through these business considerations to arrive at a decision on how to manage employee information that meets the business and employee needs? This whitepaper provides a framework to assist an enterprise in understanding all of these business considerations.

To begin the discussion it is important to define PI/SPI (Personal Information/Sensitive Personal Information) as used in this and supporting documents. The definition of "Personal Information" in this paper shall mean any and all information relating to an identified or identifiable individual (an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity).

The definition of "sensitive personal information" in the US that triggers the security breach notification laws varies by state, but generally includes: (Name or "any information identifiable to a natural person") in combination with (SSN, medical information, fingerprint, other biometric data, Date of Birth, Mother's maiden name, digital signature private key, PIN code, Driver's License #, State ID card #, Employee ID #, Employer taxpayer #, Passport #, credit card #, debit card #, any other financial account # in combination with any required security code, access code or password that would permit access to the account.

Within the EU, sensitive information is defined as "special categories" of "personal data" collected or processed in EU countries - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Additional information elements and categories were designated as sensitive based on views expressed in two supporting employee surveys. The differences in the legal definition of "sensitive" employee information versus information elements identified in employee surveys can be considered as a trend for future consideration.

The Use of Employee Information framework has been developed as a tool through which companies can make decisions in their privacy and security programs relative to the use of employee information. The framework recognizes the complex interactions of information elements, business needs, employee needs and global economic and regulatory considerations and most importantly the business value or context in which a company makes those decisions. Here are some of the demonstrable benefits that have been identified to date.

- ✓ Improve information efficiency - Only PI/SPI information minimally required is collected and stored.
- ✓ Attainable level of legal compliance - Sharing of PI/SPI information is consistently and legally defined across internal and external business units.
- ✓ Improve employee trust – Employee perceptions of SPI information is acknowledged and honored whenever feasible.
- ✓ Reduce risk – Privacy related employee information breaches could be minimized.
- ✓ Gain workforce flexibility -- Position the enterprise to accommodate the emerging workforce.
- ✓ Gain significant innovation without the need of growing a workforce.
- ✓ Streamline, automate or eliminate business processes – Elimination of FTE and equipment
- ✓ Lower unit costs – Outsourcing and/or off-shoring
- ✓ Vendor Information Checklist – Facilitate the management and auditing of vendors

1. Use of Employee Information Framework Overview – Sample Case

This framework presents a methodology for making important decisions about employee information. The type of relevant decisions can range from the policy (strategic) level to the program (implementation) level. To aid in the understanding of how to use the various elements of the framework (illustrated below in Figure 1), we have posed a sample case to show how the framework can be used to arrive at a decision. The sample case along with five possible solutions is outlined in the box at the end of this section. There is a dialogue box within each of the subsequent sections to illustrate how that section can be used to further the decision making process.

Figure 1

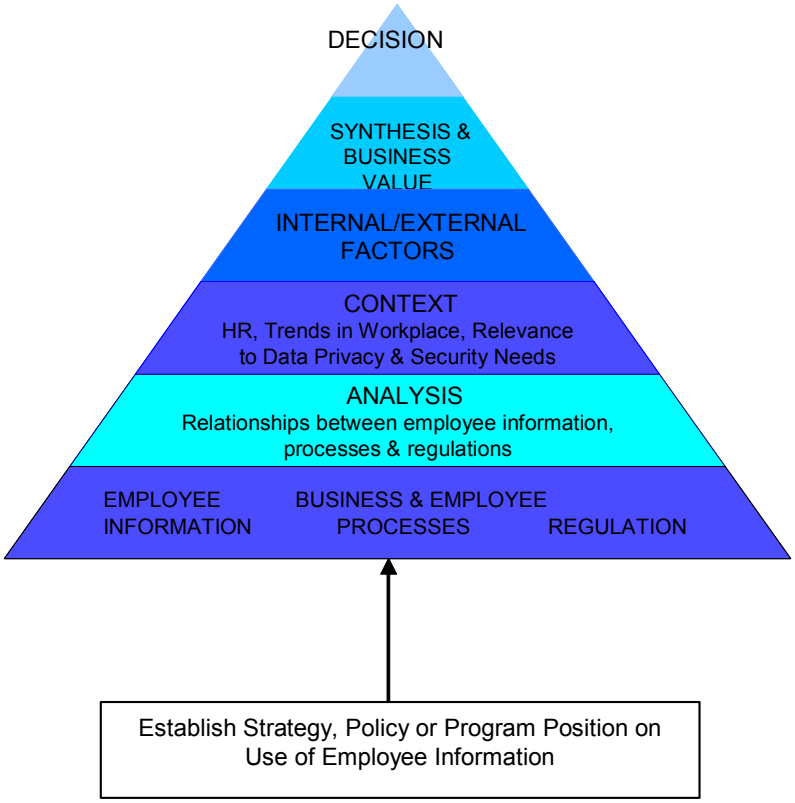


Figure 1 places into context the process that companies may consider as they analyze the myriad of categories and elements of employee personal information (PI), sensitive personal information (SPI) and processes in order to make policy and program decisions. The framework summarizes the information gathering and analysis conducted by the Use of Employee Information working group. All of the information detail that follows can be used as reference material, a sample process, and as a baseline as companies document and analyze their enterprise. The framework follows a bottom-up information gathering and analysis process. All of the sample tables represent a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decisions for their organization.

The first step undertaken was to develop a composite inventory of PI/SPI information, business and employee processes and an overview of the current regulatory environment as a necessary foundation for the steps to follow. This first step can be viewed as a gathering of factual information that will form the basis for the analysis to follow. A discussion of this process is in **Section 2.**

The second level of the framework looked at a number of relationships relative to PI/SPI, the business and employee processes that may generate and/or use the information, and the regulations that govern the use of that information. Current[i] observations on these key relationships are found in **Section 3**. Current regulatory drivers are discussed in **Section 4.** Table 1 below charts the various relationships analyzed in **Sections 3 and 4**.

Table 1 identifies the various correlations that were examined combining regulatory information, employee information, business processes, employee processes and employee needs research. The left column represents foundation information – law (regulations), employee information that may be acquired, created or processed, and the business and employee processes that may interact with employee information. Once this foundation information is determined, there are many different ways of assessing the interactions of employee information, the law and business and employee processes. The categories along the top were selected as logical ways of looking at the connections of law, employee information and processes.

Note that 'Workplace Activities' are defined as privacy related actions that impact an employee in the workplace such as employee monitoring. Business processes are those actions undertaken by the business that utilizes the employee information. Payroll and benefits administration are examples of business processes that utilize employee information.

Each completed cell represents a supporting table that documents these relationships. For example, there is a supporting table that takes 19 categories of regulations (law) and correlates to employee information elements. That supporting correlation table identifies when an employee information element may be relevant to a particular category of regulation (law).

Table 1
Framework Matrices

	Employee Information	Business Processes	Employee Processes	Business Observations	Employee Needs Research
Regulations (Law)	Relates Employee Information To Law	Relates Business Processes To Law	Relates Employee Processes To Law		
Employee Information		Relates Business Processes to Employee Information		Makes Business Observations of Employee Information	Relates Employee Needs to Employee Information
Business Processes	Relates Employee Information to Business Processes			Makes Business Observations of Business Processes	
Employee Workplace Activities	Relates Employee Information to Employee Workplace Activities	Relates Business Processes to Employee Workplace Activities			

The third level of the framework involved analysis and evaluation of information and processes, putting into context the needs of the total workforce. It includes such subjects as engagement drivers, future trends in the workplace and the relevance of these issues to information privacy and security needs of the workforce. Discussion of these important contextual issues is in **Section 5**.

The fourth level of the framework involved identifying and understanding the impacts of internal factors and external factors that may play a role in the use of employee information. These internal and external factors are discussed in **Section 6**.

Finally, there are a series of additional observations that filter through all of the previous levels of information generated and analyzed. The intent was to synthesize common elements and trends that can provide useful insight in the decision making process. A discussion of observations gained from the working group's analysis is included in **Section 7**. A key element of that synthesis process is a discussion of the business value to the organization. This is also included in **Section 7**. Concluding remarks on utilizing this framework for decision-making are included in **Section 8**.

During the course of the discussions within the Use of Employee Information Working Group, a number of important suggestions and issues were raised that were documented for future upgrades to the framework. They are described in **Section 9**. There were also suggestions made that are appropriate for future topics of discussion and possible project activities that would be appropriate in an ongoing RIM Council Workplace Program. These are documented in **Section 10**.

The Sample Case

Company XYZ, headquartered in the U.S., is a multi-national company operating in all major global economies (North America, South America, EU and Asia). They have permanent and contingent employees in all of these economies. Up until now, Company XYZ has operated its country subsidiaries as independent units with little sharing of personal information. Only financial information has been consolidated. With the globalization of the world economy, Company XYZ has decided to consider consolidating some or all of its personnel information and its contingent workforce management relationships to more discretely manage the business. It has also considered outsourcing some components of its business operations in countries that are more economically able to deliver the functionality. Since RFID and GPS technologies may be able to improve the production environments, the Company is considering enabling such technologies for tracking equipment, product and personnel in select production sites.

Company XYZ needs to make a decision on how they should structure an employee privacy policy given its decision to consolidate personnel information, contingent workforce management relationships and enter into outplacement agreements. They also want to be careful about the promises they make to their employees and certainly want to continue their practice of being compliant with local laws.

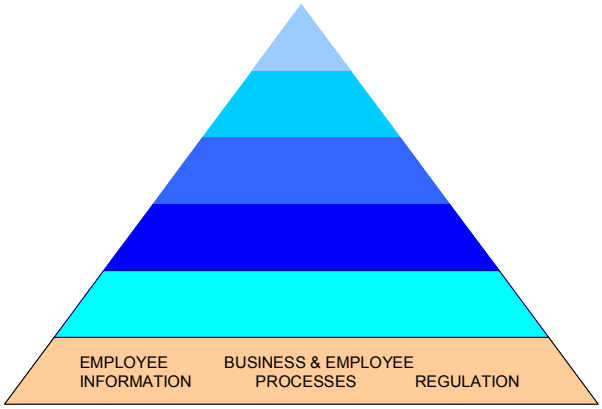
There are five possible solutions they are considering (samples can be found in Appendix 2):

1. A policy for U.S., a policy for EU and EU like countries and a policy for all others (with country specific supplements) - This approach allows the XYZ Company to minimize its commitment to employees, while being compliant with the laws. It may require the Company to continue to maintain the majority of its sensitive personnel information in the original country because it is difficult to obtain a permit to transport sensitive personal information. This might minimize the opportunity for outsourcing.
2. One global policy with separate notice requirements for each country - This approach definitely would allow the XYZ Company to make a mostly consistent commitment to employees, while being compliant with the laws. It would definitely allow the Company to consolidate most all of its personnel information into a global database including sensitive personal information from countries that would permit it. This would also allow the opportunity for outsourcing.
3. Individual country policy - This approach definitely would allow the XYZ Company to minimize its commitment to employees, while being compliant with the laws. It would definitely require the Company to continue to maintain the majority of its personnel information in the original country. This would eliminate the opportunity for outsourcing.
4. An EU based (minimum standard) policy for all countries - This approach definitely would allow the XYZ Company to make a very consistent commitment to employees, while being compliant with the laws. It would definitely allow the Company to consolidate most all of its personnel information into a global database, exclusive of a significant amount of sensitive personal information. This would definitely allow the opportunity for some outsourcing.
5. No separate employee privacy policy – may have privacy built into confidentiality agreements - This approach may allow the XYZ Company to make a somewhat consistent commitment to employees, while being compliant with the laws. It would allow the Company to consolidate a little of its personnel information into a global database. This would only allow the opportunity for outsourcing of functions that did not involve personal information across countries.

How can the UEI framework facilitate their decision process?

The first step required in the analysis process is to take inventory of its personal information (sample reference material can be found in Appendix 2) for each country entity and the regulatory requirements (by jurisdiction) for the acquisition, use, movement, protection and retirement of employee information.

2. Laying the Foundation – Information Inventory and Legal/Regulatory Considerations



Through a series of work sessions, the RIM Council Use of Information working group developed two important documents that lay the foundation for the analysis that followed. A company that wishes to use this framework should to develop their own employee information inventory and a list of important regulatory requirements to aid in strategic decision making.

Developing the employee information inventory, the categories, the elements and the levels of sensitivity, is the objective of the first step. The other lists are presented to help flesh out the inventory and to subsequently help to identify the source and point of collection, the opportunity for notice and consent, the sharing within the business and its purpose, and the sharing externally with other entities within the company and third parties as well as to identify trans-border flows and access. In addition, the inventory will also serve as the opportunity to identify security, retention and deletion business rules that will apply to each category and/or element. These lists will not be complete during the first pass, even with the starter information provided by the RIM Council Use of Information working group, nor is there one right answer for the categorization process. It is expected that the teams would apply their knowledge to the processes.

The initial employee information inventory should include:

- List of employee information subjects for who employee information is collected, stored, used, shared and retired. For example, the classification of 'employee' may include former employee, retired employee, temporary employee, etc.
- List of business entities that govern, collect, use, share and/or transfer employee information. For example an insurance provider is a business entity that collects uses and potentially transfers employee information.
- List of media that may be used to collect, store or share employee information. These may include e-mail, fax, ID badges, voice mail, etc.
- **List of employee information categories, information elements, definitions and sensitivity (PI and SPI). For example, the information category of personal may include information elements of citizenship, country of residence, place of birth, etc.**
- List of summary business processes that access and/or use employee information. For example, the business process of health plan management provides, where there employees are not covered by government health plans, health plans for employees and their families or partners.
- List of employee processes that access and/or use employee information. For example, career planning is a process initiated by an employee that may use and/or generate employee information.

A compilation of legal and regulatory considerations is the second important foundation document for the analysis to follow. Regardless of the strategy or policy chosen, it is always important to understand the overall privacy regulatory requirements so that decisions can be made in the context of the law. Without a

full understanding of the total effect of regulation on the business and employee objectives in the use of employee information, it will not be possible to make strong and effective policy that will stand the test of time. While a company may choose many different strategies, the legal and operational impacts of privacy are rather large to retrofit it to the strategy, policy or program when only partially thought through.

There are three pieces of information to consider:

- The compliance practice
- The employee data affected
- The regulations that drive the compliance (state, U.S and international)

The Use of Employee Information working group organized this regulatory information in line with six privacy principles, which are more or less consistent with the AICPA/CICA Privacy Framework column 5 (U.S. Safe Harbor).

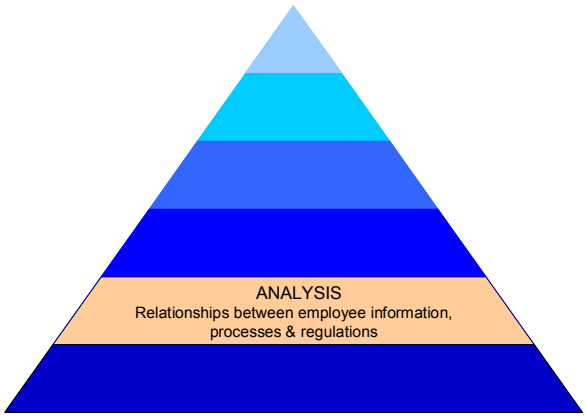
- Notices, consents, & rights to object, access or counsel
- Limits on processing, data scope, quality and accuracy
- Security and confidentiality of processing
- Restrictions on cross-border transfers
- Restrictions on sharing data with third parties
- Other accountability and administrative requirements

The working group looked to be as comprehensive globally as possible, time permitting. The team also looked for additional regulatory impacts in the labor, export and other regulatory areas where available. It is important to consider the impacts of laws beyond privacy when conducting this research, because often what is acceptable in the world of privacy may not be acceptable under another regulatory regime.

The Sample Case (Continued)
Employee Information and Legal/Regulatory Considerations

Company XYZ has conducted an inventory of employee information for each country entity, identifying the information elements, the categories of information (sensitive or not sensitive), business processes that use the information and employee processes that generate or use the information. Company XYZ has also documented the movement of employee information within each country and the potential for movement across borders. The next step is to identify the relationships that are relevant to the decision of how to construct an employee information, business process and system architecture as well as the employee privacy policy that would support these relationships and the architecture. For example, if the business processes and the personal information are similar with no major differences, country to country, then the personal information and business processes can easily be consolidated, or distributed, or outsourced depending upon regulatory requirements and business objectives. There may be other factors later that will prevent consolidation or reduce its probability or prevent outsourcing, however this would the first test of just how consistent the personal information and business process could be. The more consistent, the more options the XYZ Company has to choose from.

3. Key Considerations: Creating a Uniform Process - Identifying Relationships to PI/SPI



a. Relating Business Processes to Employee Information

This set of employer related questions revolves around the use (or not) of employee information in business processes. This analysis serves to confirm the completeness of the business processes and employee information and to provide thoughtful consideration over what information is truly needed (minimum necessary) for conducting business.

Table 2 below is a sample of the information used to correlate the business processes to employee information categories. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 2
Framework for Correlating Employee Information Categories to Business Processes

Business Process Category	Personal	Public Information	Recruiting	Security	Sensitive - Background	Sensitive - Benefits	Sensitive - Business	Sensitive - Discrimination	Sensitive – E.U.	Sensitive - Financial	Sensitive - Government	Sensitive - Health	Sensitive - ID	Sensitive - Monitoring	Sensitive - Performance	Sensitive - Personal	Sensitive - Potential	Work Equipment	Work History	Work Information
Benefits: EAP	✓				✓	✓		✓		✓		✓	✓			✓	✓			
Benefits: Health Plan Mgmt	✓				✓	✓		✓				✓	✓			✓	✓			
Benefits: Workers Compensation	✓				✓	✓		✓				✓	✓			✓	✓	✓	✓	✓

For Employers – Key Considerations on Handling Employee Information within Business Processes

What employee PI/SPI is used (or not used) in your business processes?
What are the restrictions that need to be honored in the use of employee PI/SPI?
Are controls in place for the use of employee PI/SPI within your business processes?

For an enterprise to arrive at an answer to these questions, an assessment should be developed of the relationships between the required business processes and business employee information needs. Such an assessment can shed some light on the minimum information requirements and the restrictions to be honored in some or all situations. The observations that follow reflect the composite analysis of the processes and business information needs generated by the UEI Working Group. They are categorized as process related.

- ✓ There are categories of employee PI/SPI information (Personal, Sensitive-Personal and Sensitive-Potential) that are used by nearly all business processes and can be identified and controlled consistently across the organization.
- ✓ There are categories of employee PI/SPI information (Recruiting, Security, Sensitive-Monitoring, Sensitive-Performance) that are used by very few business processes or in a very specialized manner suggesting that the information can be minimized in terms of storage and control.
- ✓ Business processes such as Privacy Management, Compliance and Audit and Employee Information Management are but a few processes that use nearly all categories of employee information.

A detailed matrix that contains a list of summary business purposes/processes and observations regarding those processes are available in Appendix 1 (Business Processes to Employee Information Matrix).

The Sample Case (Continued)
Relating Business Processes to Employee Information

In observing the business processes that Company XYZ engages in relative to employee information we find that it collects the minimum information. Its business is such that it does not require background checks, drug testing or health checks, so the amount of Sensitive Personal Information (SPI) is limited. This increases the flexibility of the Company in the options it will be able to choose relative to an overall employee privacy policy strategy. In addition it also increases the Company's flexibility in trans-border flows of personal information to gain efficiencies of processing and may allow the Company to outsource certain business processes to areas of the world know for their ability to provide high quality service at significantly low price points.

b. Relating Business Processes to Business Observations

The second set of questions is also from an employer's perspective on their business processes. Table 3 below is a sample of the correlation information used to frame the observations of employers and business processes. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 3
Key Business Observations – Privacy/Scope Related to Implementation of Business Processes

Business Process Category	Summary Business Purpose/Processes	Key	Business Observations re Processes Delivered Consistently and/or Privacy Issues
Benefits: EAP	Employee Assistance Process	✓	This is a business service not commonly offered globally. In some countries, it may not be perceived as a benefit. It does require the management of SPI.
Benefits: Health Plan Management	Health Plan Management	✓	Healthcare is also not a service that is offered globally, especially in countries with government provided healthcare. It does require the management of SPI.
Benefits: Supplemental Benefits Admin	Supplemental Benefits Administration	✓	Supplemental benefits are not provided consistently around the world, due to the economic situation of the work force and the expectations of the work force. It does require the management of SPI.
Benefits: Workers Compensation	Workers Compensation and On the Job Accident Management	✓	This information straddles the business and the employee "spaces". Often this is an area of conflict between what really occurred and whether the employee has a real claim. This is an issue that is applicable in countries where there are labor laws that protect the workers.

Note: The key column refers to importance of the Business Process Category/Purpose

For Employers – Key Considerations for Enhancing Employee Business Processes

What is the minimum amount of employee information that can sustain business processes?
What employee information do you need to prove that the process was completed?
Do you provide notice & consent, as required, to your prospective, current & former employees?
Do you provide notice & consent to contingent workers in your privacy notice & contracts?
How is your business protecting the employee information it holds?
What controls do you have in place as they relate to employee related business processes?

For an enterprise to arrive at an answer to these questions, an assessment should be developed of the key issues and relationships between required business processes and business information security needs. Such an assessment can shed some light on the gaps between processes that generate and use employee information and security and privacy needs. The observations that follow reflect the composite analysis of the processes and business needs generated by the UEI Working Group. They are grouped by information, process and policy.

Information:

- ✓ The more sensitive the personal information is to the business process, the likelihood the best place for managing such information would be as close to the source as possible with the least amount of replication. Perhaps such management would be performed by local systems.

Process:

- ✓ The business processes that many businesses are aware of and are working globally to close the gaps regarding privacy and security include:
    - Third Party, Client and Vendor Management of Personal and Sensitive Personal Information re Contracts and Security[ii]
    - Trans-Border Flow and Onward Transfer Management via Country Adequacy, Contracts, Safe Harbor or BCRs
    - Employee Fraud Management & Investigation
    - Processing Purposes (Primary), Legitimacy Conditions and Legal Basis Management[iii]

- Ongoing permissions for additional Secondary Uses as required
- Sensitive Personal Information processing of EU SPI, Health Information, Financial Information, Some Ids (SSNs, SINs)[iv]

- ✓ The business processes that businesses are also actively addressing include the whole suite of security issues surrounding PI/SPI[v].

Policy:

- ✓ Businesses in leadership positions are also championing solid corporate social responsibility programs that protect the rights of all workers[vi].
- ✓ The full privacy impacts of new PI/SPI & technology, such as GPS, RFID, Biometrics, especially in monitoring, are yet to unfold.
- ✓ Permissions management and relevant products, services and content is the way to build relationships for life.
- ✓ Hiring practices, in certain countries however, continue to utilize certain PI/SPI that is protected from use by law in other countries[vii].
- ✓ The collision of national laws over email and internet monitoring, e-Discovery of EU private e-mails that are to remain private or of the release of information in the name of anti-terrorism and Whistle-Blowing regarding ethics hotlines are a few of the examples that may cause temporary or permanent interruptions to the purposeful flows of personal information.
- ✓ Managing Works Councils to meet a common business objectives or goals in a timely manner is often next to impossible. Depending on strategic interests, a business may decide to locate facilities inside or outside the EU.

A detailed matrix that contains a list of summary business purposes/processes and observations regarding those processes are available in Appendix 1 (Business Processes to Business Observations Matrix).

The Sample Case (Continued)
Relating Business Processes to Business Observations

In observing Company XYZ relative to its business process categories, the business processes are predominantly the same across countries and units, with the exception of the strong labor union and works council activity in Europe and the fact that they have a number of production environments that require varying safety rules and regulations and accidents, while few, do happen and result in ongoing HR workmen's compensation settlements in many of Company XYZ's countries. These two areas would perhaps not be good considerations for the Company in its consolidation of business processes and systems to support the business processes.

The Company has a great relationship with their contingent worker supplier that could easily be expanded globally with the exception of the workmen's compensation function as this would transport sensitive personal information outside of the EU.

c. Relating Employee Information to Business Observations

For each of the analysis steps, a set of key questions is raised to help frame the assessment process. This set of questions is from an employer's perspective on employee personal information. Table 4 below is a sample of the correlation information used to frame the observations of employers and employee personal information. Note that this sample table represents a composite view developed by RIM Council member

companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 4
Employee Information Relative to Business Observations

Information Category	Information Elements	Key	Business Observations
Personal	Employee Place of Birth	✓	Ultimately will be SPI and part of an identity theft piece of information
Sensitive- Benefits	Benefits Usage	✓	This information would include SPI
Sensitive- Background	Criminal arrests or convictions	✓	SPI; Part of the hiring process; Perhaps should not be kept by the hiring entity
Security	Digital Certificate or "Site Key"	✓	SPI; Part of security information

Note: The key column refers to importance of the information category/element

For Employers – Key Considerations for Employee Information Privacy:

What employee information do you really need?
Have you defined the business purpose for it?
Do you provide notice & consent, where required, to your prospective, current & former employees?
Do you extend notice and consent if needed, to contingent workers?
Can employee information be anonymized to reduce risk?
What employee information do you really need to transport across borders for storing or viewing?
Can employee information fields be separated for transport?
Do you have the proper controls in place for transport?
Can the transport be done securely and with appropriate contractual arrangements?

For an enterprise to arrive at answers to these questions an assessment is needed of the key issues and relationships between required business processes and the categories of employee information. Such an assessment can shed some light on processes and information that are important to the enterprise and that which is less important. The observations that follow reflect the composite analysis of the processes and information generated by the UEI Working Group. They are grouped by information, process and policy.

Information:

- ✓ Consider or anticipate what information will become SPI so that one does not depend on it so heavily that major processes must be re-architected[viii].
- ✓ Do not keep SPI that one does not have to keep; offload the risk to another entity, but put in place security breach notification, incident management protocols and vendor audits as part of the contract and initial/ongoing implementation.

Process:

- ✓ Address the management of PI/SPI consistently, integrating the health care implementations in the U.S. with the information privacy implementations, if separate[ix].
- ✓ Consider both paper and electronic information in scope for your information management security program.
- ✓ Safeguard PI/SPI of family members as well as employees.
- ✓ Collect, store, use, share, distribute, and/or trans-border flow for access only the minimum PI/SPI needed to fulfill the task or activity.
- ✓ Safeguard PI/SPI commensurate with its sensitivity or ability if lost to cause harm. The higher the sensitivity the higher the safeguards.

Policy:

- ✓ Consider a consistent hiring process globally that is as free from discrimination as possible and perhaps takes a "labor law high road approach," thus achieving common processes globally that are not only more efficient, but also is supportive of a company's commitment to corporate social responsibility.
- ✓ Address the differences between what employees see as sensitive and employers see as sensitive, especially individual location, family, performance and salary information, which are viewed as SPI by employees.
- ✓ Consider the impact and use of certain PI/SPI pieces of information now readily available due to technology such as photos, GPS, RFID and emerging information, such as biometric information and other information from blogs, Facebook, etc., and from searches.

A detailed matrix that contains a list of key information categories, information elements and observations relative to business processes is available in Appendix 1 (Employee Information to Business Observations Matrix).

The Sample Case (Continued)
Relating Employee Information to Business Observations

In observing Company XYZ relative to employee personal information and the business decisions that the Company might make, it is always critical when building information architecture that will be privacy enhanced, that the key decision need not be altered for some period of time into the future. For example, if birth date is to become sensitive personal information, then perhaps it is important to minimize its use or not capture it in total at all. In the production areas for example, if GPS and RFID technology can be bypassed for an even more innovative privacy neutral technology, this would be a better choice for the Company, The concept of building with privacy in mind is critical in the more privacy sensitive EU countries.

d. Relating Employee Information to Employee Needs

The fourth set of questions is from an employee's perspective on how an employer uses their personal information. To provide some guidance, we looked at the 2006 Ponemon Institute study, *Americans' Perceptions about Workplace Privacy*. It was the first study to provide insight into information privacy and security needs of employees in the workplace. We also included 2007 Ponemon Institute/Littler study, *Workplace Survey on the Privacy Age Gap*, which provided additional support on issues first surveyed in the 2006 study. It should be noted that both of these research studies were U.S. based. It is also important to note that the surveys addressed *secondary* uses of PI/SPI.

An understanding of the commonality and gaps in the perceptions of employees on how their employer handles employee information is helpful in determining overall policy considerations beyond regulatory considerations. Again, this is guidance for employers on the *secondary* use of PI/SPI.

For this analysis, the responses from the two surveys were matched to information categories/elements used in previous tables. Employees identified information categories/elements where they believed it important for the employer to obtain consent prior to a secondary use or sharing. Table 5 below is a sample of the survey results contained in the two studies. The 2007 Ponemon/Littler study is also illustrated by total respondents, workers between the age of 18 and 30, and workers older than 50 years of age.

Table 5
Employee Needs Relative to Employee Information

		2006 Ponemon Tacit Study	2007 Ponemon Littler Study	2007 Ponemon Littler Study	2007 Ponemon Littler Study
Information Category	**Information Elements**	**Obtain consent before secondary use or sharing PI**	**Obtain consent Before secondary use of PI (Total of both age groups)**	**Obtain consent Before secondary use of PI (YA: worker between ages of 18 and 30 years)**	**Obtain consent Before secondary use of PI (OA: worker more than 50 years of age**
Sensitive- Health	Dependent Health Claims	86%	95%	93%	96%
Sensitive- Health	Disability history or current status	86%	95%	93%	96%
Sensitive- Health	Disability Requirements	86%	95%	93%	96%
Sensitive- Health	Employee Health Claims	86%	95%	93%	96%

*Secondary Use

From Employee Perspective - Key Considerations on How an Employer Handles Employee Information

What PI do employees consider sensitive enough to obtain their consent before a secondary use?
Are employers and employees views of PI and SPI secondary use consistent?
Do employees understand the definition of secondary uses of PI/SPI?

The survey results contained in the two studies were used to frame the observations below and are grouped by information and policy. The information observations are further categorized from the employee perspective and employer perspective.

Information: Highlights of Employee Perspectives of Sensitive Personal Information

- ✓ Sexual orientation is the most significant information element. While it is defined as sensitive EU, it is important to note that older U.S. employees (for which the study is based) find the information element extremely sensitive. Younger U.S. employees, while still finding sexual orientation sensitive, are less likely to rank it as sensitive as the older U.S. employees.
- ✓ Sensitive-financial information is the most significant information category primarily the credit report information element.
- ✓ Performance history is the next most significant employee information category. This category of PI is not always part of an employer's highly sensitive information.
- ✓ Social Security number is a significant information element and may reflect the successful process of public education to the risk it plays in identity theft.
- ✓ Health conditions and associated information have a high score in importance based on awareness in recent years to HIPPA privacy requirements.
- ✓ Time records as reflected in project and time records or possibly records billed to clients is of significant importance.

- ✓ Religious and philosophical beliefs while defined as sensitive EU, U.S. employees indicate importance.
- ✓ Information about dependents and family members are important information elements.
- ✓ Information elements that reveal political activity of the employee are sensitive.
- ✓ Salary history and other information elements that use salary information such as tax documents are considered as sensitive.
- ✓ Travel itineraries and associated travel information are considered as sensitive.
- ✓ Education information along with racial and ethnic information appears to be less sensitive but still important to employees.
- ✓ E-mails, home related information such as phone numbers and address, and benefit information all fall in the middle level of sensitivity.
- ✓ The remaining information categories and information elements were below 50% in response rates and can be viewed as having lower levels of sensitivity.
- ✓ Employees did not appear concerned over gender, name or even photographs.
- ✓ Sensitive background information having to do with criminal arrests or court cases is of significant importance.
- ✓ Employees consider performance, benefits, and certain personal and business contact information as sensitive.

Information – Highlights of Employer Perspectives of Sensitive Personal Information:

- ✓ Business perceptions of sensitive personal information do not correlate to the employees' perceptions of sensitive personal information[x].
- ✓ Employers are more focused on the legal definition of sensitive, while employees are focused in on a more personal definition of sensitive.
- ✓ Employees are growing more aware of sensitive personal information[xi].
- ✓ In other studies, there is some evidence that not all SPI related to identity theft is known by employees and thus is often not protected[xii] .
- ✓ The concept of 'consent' is important to employees, however opt-in or opt-out are equal in preference.
- ✓ The use of the term 'consent' in this study is different than the use of consent in the EU relative to consenting to the privacy notice, the collection of SPI and the trans-border flow of PI/SPI. Consider using 'consent' in the narrower EU context and 'permissions' for additional choices an applicant or employee or alumnus is provided regarding what can be done with their PI/SPI.
- ✓ Employers need to define primary use versus secondary use and communicate that definition to employees in the privacy notice and in employee communication.

A detailed matrix that contains a list of information categories, information elements and research on employee needs is available in Appendix 1 (Employee Information to Employee Needs Research).

The Sample Case (Continued)
Relating Employee Information to Employee Needs

In analyzing Company XYZ relative to the employees' perspective on employee information, it is important to factor into the decision criteria items such as what is the minimum set of PI necessary to collect and/or store and what SPI is really needed. Is there a difference between the employees' perspective and the Company's perspective?

In today's world, where there is all sorts of fears relative to terrorists, identity thieves, stalkers, scammers, phishers, organized crime, etc. there is little information left that one does not consider "sensitive" from the perspective of the employee and the Company. Protection is critical.

Company XYX has already minimized the PI/SPI collected. If protection is important to employees, the Company would be extremely wise to reinforce via stronger procedures, better protection tools, revised controlled access further limiting the "need to know" practices, revised retention criteria and other demonstrable actions that demonstrate the care for employee personal information. This also applies to other corporate intellectual property and client and customer personal information. These reinforced protection implementations would take the highest regulatory requirements into consideration without necessarily requiring a policy commitment. By doing this the Company gains the support of employees in helping to protect their own PI as well as the other corporate PI/SPI. The Company also does not necessarily need to raise its policy commitments to its employees beyond the minimum regulatory requirements in each country thus minimizing its liabilities as well. This also allows the Company to meet the needs of its employees and also be flexible in it policy decisions at the end of this analysis.

e. Relating Employee Workplace Activities to Business Processes

The final set of questions is from an employee's perspective on business processes. The 2006 Ponemon Institute study, *Americans' Perceptions about Workplace Privacy*, provided insight into the views of employees with respect to employee related workplace activities and business processes. Table 6 identifies and correlates employee activities and business processes from that study. Table 7 is a similar comparison utilizing information from the 2007 Ponemon Institute/Littler study, *Workplace Survey on the Privacy Age Gap.* The last four columns are the employees' response to the business action resulting from an employee workplace activity. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 6
Employees' Perspective on Privacy Relative to Business Processes

Business Process Category	Summary Business Purpose/Process	Acceptable secondary uses of PI	Resign employment	File complaint with HR	Complain to Supervisor	File union grievance	Contact an attorney	View PI in company files
Communications	Employee Communications	42%						

Business Process Category	Summary Business Purpose/Process	Acceptable secondary uses of PI	Resign employment	File complaint with HR	Complain to Supervisor	File union grievance	Contact an attorney	View PI in company files
	Management							
Business Marketing Product Development	Product Marketing Program Management	10%						
Privacy Management	Access & Recourse Process		10%	24%	21%	15%	16%	74%
Payroll & Contract Administration	Payroll	63%						

Table 7
Employees' Activities Affected by Business Processes

Business Process Category	Summary Business Purpose/Process	Employee disciplined for company critical blog post	Employee disciplined for non-company personal blog	Employee disciplined- blog posting unlawful personal conduct	iPod allowed in workplace with unannounced searches	Employer monitors company social network web site	Employer monitors e-mail and internet use on company network	Employer require access to all e-mail accounts used for company business
Security & Risk Management	Employee Monitoring and Network Traffic Analysis	77%	80%	70%		82%		38%
Privacy Management	Notice & Awareness				68%		59%	

Key Considerations - How an Employer Uses Employee Information in Business Processes

Do you have a process for determining employees' top level concerns regarding use of PI and SPI?
Is there a policy in place to address secondary uses?
If permissions are required for certain secondary uses, is there a process in place to acquire?
Are employee PI/SPI privacy and protection policies known?
Are policies on business processes such as use of equipment, monitoring, etc. known to employees?
Do you have a business process for addressing employee PI/SPI related questions or concerns?
Is this process known and readily accessible by employees?

As in the section above, we looked at the 2006 Ponemon Institute study, *Americans' Perceptions about Workplace Privacy* and the 2007 Ponemon Institute/Littler study, *Workplace Survey on the Privacy Age Gap* for guidance. In this section there is some guidance with respect to their employer's handling of personal information (PI). For this analysis, business processes were correlated to employee PI related activities. The observations from this analysis are below and are grouped by process and policy.

Information:

- ✓ If an employee learned that their employer is not properly protecting PI, 10% would quit, 31% would go to an attorney or the union and 45% would complain to a supervisor or to HR. Only 9% would do nothing.
- ✓ Employees find secondary uses of PI for purposes of facility safety or anti-terrorism reporting requirements acceptable.
- ✓ Employees find secondary uses of PI for purposes of payroll processing and education and training somewhat less acceptable.

Process:

- ✓ Many companies define these secondary use business processes as primary use.
- ✓ Employees rely primarily on their colleagues for job related support rather than official documents, unofficial documents or internet searches.
- ✓ Employees believe the best time to learn about privacy commitment is during new employee orientation and in the normal course of communication with Human Resources.

Policy:

- ✓ Employers might consider defining both primary use and secondary use policy statements and clearly communicating the definition and the policy to employees
- ✓ U.S. employees care about the ability to view PI in the company files.
- ✓ U.S. employees accept workplace surveillance and e-mail monitoring but are less accepting of drug testing.

A detailed matrix listing the summary business purpose/process and employee workplace activities is available in Appendix 1 (Employee Workplace Activities to Business Process).

The Sample Case (Continued)
Relating Employee Workplace Activities to Business Processes

In analyzing Company XYZ relative to the employees' perspective on business processes, it is important to factor into the decision criteria items such as defining a comprehensive set of primary uses of PI and a very limited set of primary uses of SPI; identifying uses of SPI that would be problematic and/or unnecessary; identifying as well secondary uses of PI/SPI that would qualify for subsequent consent; as well as the extent to which employees may access/use company computer for personal use for purchasing; participation in blogs or social networks; or general personal email. The key is to build in policies to address these and other overlaps between employees and their personal use of company computer resources. The concept of 'consent' is important to employees and should be an important factor when determining the structure of an overall privacy policy. Naturally 'consent' is mandatory in some jurisdictions while not in others.

The same is true with the right of access. In some of Company XYZ's jurisdictions it is fundamental while not in others. Creating a policy that is somewhat equal can be a challenge. This is also true with employee monitoring. In the EU it is more difficult to conduct employee email and internet monitoring exercises than it is in other regions of the world. Again a consistent policy is difficult in this area.

The Company has taken a position that a small amount of personal use of company computer resources is acceptable and can be carried out according the guidance provided in its Code of Conduct. There is no conceptual difference in Company XYZ's perspective of internet use and phone use. This has been researched and is acceptable globally.

Employee monitoring is a bit of different matter as the limitations are different country by country. Company XYZ has more research to do before making a global policy statement that could be effective in all countries.

4. Key Considerations: The Legal/Regulatory Perspective – Identifying Relationships to PI/SPI

The regulatory environment relative to employee information is a complex mix of federal, state and international legislated law, supporting rules and judicial decisions that have an impact on an enterprise in terms of collection, access, storage, usage, sharing, trans-border flow and retirement of PI and SPI. The UEI Working Group developed a summary document of regulatory drivers and compliance practices in the U.S., EU and other global jurisdictions. This addendum document is titled UEI Compliance Practices Regulatory Drivers dated November 10th 2006 and is intended to present a high level summary. Each company should determine in more detail appropriate regulatory considerations.

From this summary of regulatory drivers and compliance practices, correlations were developed that looked at business processes to law, employee processes to law and employee information to law. The intent was to provide guidance and trends in key connections. Nineteen categories of law were analyzed and are described below, along with the some observations from each of these correlations.

a. The Regulatory Drivers (all categories from reference charts):

Key Considerations – What other regulatory factors complement, contradicts or conflict with privacy regulations or privacy strategic approaches?

> *What are the regulations that affect employee information or business processes?*
> *Do these regulations affect the collection, access, storage, usage, sharing, trans-border flow and retirement of the employee information? Do they change the company's purposeful and permitted flow of personal information?*

For an enterprise to arrive at an answer to these questions, a review of the key regulations and pending regulations in the various jurisdictions the business entity does or plans to do business in is needed. These key regulations can then be evaluated against the required business processes and business information security needs. Such a review can shed some light on processing requirements, restrictions regarding use of employee information, security and privacy needs.

The categories of law considered for analysis and some sample general observations include:

Labor Laws - Laws governing the full spectrum of the HR processes including those that address the rights of works councils and those of labor unions.

- ✓ Currently these laws are very tailored by country.
- ✓ Labor law approaches to discrimination vary by region.
- ✓ As many companies adopt Corporate Social Responsibility programs and strong Code of Ethics Policies it becomes easier to develop common global HR processes as many companies have done with privacy and security.
- ✓ Unfortunately many country specific laws require the support of the unions and works councils. This brings the added complexity of not only country specifications, but individual process and information negotiations that are specific within a country.
- ✓ National labor laws implementing the European Works Council Directive require "consultation" with the works council representing the employees affected by company activities, including collection of personal information. The resulting criteria for business process and information often result in some very unique local requirements.

Export Laws - Laws governing the restrictions over the export of intellectual property or government secrets from one jurisdiction to another.

- ✓ In Korea, it is illegal to export SSN.

- ✓ In many countries it is illegal to export information solutions that service military or government employees.
- ✓ In some countries the assignment of a foreign national to work on a certain government employee information solution database is considered the same as exporting the information out of the country and is therefore not allowed.
- ✓ In some countries it may be illegal to export employee personal information out of the country, no matter what individual consents have been collected or contracts signed.

Security Breach and ID Theft Laws - Laws that relate to information that identifies a security breach or forensic information that relates to information that helps discover the root cause of the security breach or the subsequent identity theft.

- ✓ U.S. laws in the majority of states have data protection laws that pertain to the loss of certain sensitive personal information such as the combination of an employee name and SSN (or bank account number or credit card number or driver's license number) that employers must obey. If such information is lost or stolen the employee must be notified and provided certain protections.
- ✓ States differ on the data definition and triggers for notification. Many states have tort laws to support employee claims against an employer in the event of negligence and harm.
- ✓ The EU data directive formulates any infraction of the directive as a 'breach.'
- ✓ Japan has more stringent data 'breach' laws.
- ✓ Many countries are developing such laws in reaction to the massive losses of data in the U.S.

Anti-Terrorism - Laws that allow access to personal information as a part of an anti-terrorism initiative.

- ✓ U.S. Patriot Act expanded law enforcement access to personal information for example on voice mail and e-mail held by third parties.
- ✓ The collection of information under U.S. Patriot Act has caused reaction in the British Columbia, Belgium and the EU. There have been concerns over the examination of government data by British Columbia, the monitoring of Swift transactions without authorization from the Belgians and the transfer of airline passenger information to the U.S. by the EU
- ✓ The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA) is a tool used by the U.S. government to fight drug trafficking, money laundering and other crimes. Since 9-11, the act is an important anti-terrorism tool to stop the flow of funds to terrorist organizations.

Notice and Consent – Laws that require notices to data subjects and obtaining consent from data subject.

- ✓ Providing notices to Data Subjects and obtaining consent are implemented in EEA, Canada, and about 40 other countries with privacy laws.
- ✓ Notices to certain EEA and EU country Works Councils are required before engaging in any new collection of personal information.
- ✓ Notices are required to employees under FCRA for any credit reporting information.
- ✓ Notices are required to certain employees under Health Information Portability and Accountability Act (HIPAA) for personal health information.

Access and Complaints – Laws that relate to the information that would be available under the access rights or complaint processes.

- ✓ A right to access, correct or delete certain personal information is very commonly found in countries that have personal data protection laws, which includes at least 65 countries, including the 28 in the EEA
- ✓ Such access and correction requirements in the U.S. are not as comprehensive.
- ✓ The "habeas data" laws commonly found in Central and South America has access and correction requirements, although they are in some countries limited to data held by government agencies.

- ✓ Companies that offer access, correction, and objection rights to employees in some countries will have difficulty justifying to employees and unions why they do not do so for employees in other countries, so some companies use practices like these globally, within reason.

Marketing Permissions – Laws that provide the ability of the individual to state a preference or permission for marketing activities or purposes.

- ✓ Marketing "opt-in" requirements are common in the EU and EEA for electronic communication by email, SMS, MMS, fax where employees are also clients or customers as well.
- ✓ Marketing "opt-out" requirement under Fair Credit Reporting Act (FCRA) for affiliate marketing provide employees with an opportunity to opt out of "marketing" communications by the employer and its affiliates.
- ✓ Marketing "opt-out" requirement under CAN-SPAM provides employees an opportunity to opt out of commercial e-mail messages (CEMM's).
- ✓ Certain technologies have adopted "opt-in" or some form of double "opt-in" to ensure that the individual has definitely said yes to receiving information that they will have to pay to receive, such as SMS messages.

Ethics and Sarbanes Oxley Act (SOX) Hotlines – Laws that govern the locations of these hotlines and the functions available at these locations.

- ✓ Rule 10A-3, adopted by the SEC to comply with § 301(4) of the Sarbanes Oxley Act (SOX), requires companies with securities listed on the U.S. exchanges to establish procedures that permit employees of those companies and their subsidiaries (wherever located) to make anonymous reports of "questionable accounting and auditing matters."
- ✓ Article 29 Working Party (the "Working Party"), an advisory and independent group composed of a representative from each of the 25 EU Member State Data Protection Authorities, released an opinion regarding compatibility of whistle blowing systems and EU data protection law. The eight concepts were intended to alleviate concerns related to SOX hotlines. The Commission nationale de l'informatique et des libertés (CNIL) also issued an advisory about the same matters issuing recommendations for keeping the reporting within France, unless the violation is truly a SOX violation.

Employee Monitoring - Laws that govern the employee's right to privacy and the employers' right to monitor.

- ✓ In the U.S. monitoring is limited to what is reasonably necessary to prevent legitimate harms. Employees have "no reasonable expectation of privacy" on company computer and communications systems in the workplace.
- ✓ The European Union Data Protection Directive (EUDPD) does not expressly address employee monitoring. While it is the general view of DPA's that employee monitoring involves the collection of personal data and is therefore covered under the EUDPD and national implementing legislation, not very much guidance has been issued by the DPA's on employee monitoring, except in the U.K. and France where certain personal processing within the business community is permitted and privacy guaranteed.
- ✓ Companies that have global or regional web site monitoring programs will have a difficult time adhering to the guidelines that have been developed.
- ✓ EUDPD general consensus is that employees must be provided with detailed disclosures of monitoring practices and that the monitoring practices themselves must be "proportionate" to the harm that the employer seeks to prevent.
- ✓ In Canada, the Privacy Commissioner and arbitrators consider a four-part test when deciding on the organization's right to collect information using surveillance.
- ✓ The eDiscovery processes in the U.S. are causing issues between the EU and the U.S. relative to discovery on both sides. Judges in the U.S. have no sympathy for the EU privacy laws when it comes to discovery on either side of the pond and the EU is outraged at the privacy violations that occur daily in the U.S. judicial system with EU citizens' information.

Limits on Processing – Laws that limit certain processing without permission, such as secondary use of personal information, the use of SSN/SIN for new purposes, the restrictions under certain law governing health information, automatic decisions in the hiring process and fair credit decisions.

- ✓ EU Data Protection Directive (95/46/EC) Art 6(a) provides that personal information must be processed "fairly and lawfully."
- ✓ EU Data Protection Directive (95/46/EC) Art 6(b) states that personal information must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."
- ✓ Processing non-sensitive personal information based on establishing one or more of the grounds in EUDPD Art. 7. Sensitive personal information from EUDPD Art. 8 (or use one of the grounds in the national law of the country in which the information was collected).
- ✓ EEA and Canada maintain only information that is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
- ✓ EEA and Canada keep personal information accurate, complete and up to date.

Security Protections – Laws requiring a higher standard of protection over certain information that is more sensitive than other personal information.

- ✓ In EEA and Canada implement appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of information over a network, and against all other unlawful forms of processing.
- ✓ Specific security guidelines have been promulgated in Spain, Italy, Poland, Japan, and under HIPAA Security Rule only if a company is a covered entity.
- ✓ In Canada personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- ✓ At least six U.S. states (AR, CA, NV, NC, RI, TX) require "reasonable safeguards" to prevent "unauthorized access, destruction, use, modification or disclosure" of "personal information" (generally including types of information that can be abused for identity theft) and at least three U.S. states (CA, NV, RI) also require written agreements requiring security safeguards with third parties who will receive the information.
- ✓ In most U.S. states, encrypting will entitle one to safe harbor under Security Breach Notification statutes.

Restrictions on Cross-Border Transfers – Laws governing restrictions over trans-border flows of information.

- ✓ There are restrictions on cross-border transfers from EU, EEA and Hong Kong, Argentina, Australia and New Zealand to name a few countries to "inadequate" third countries.
- ✓ Model contact clauses, safe harbor certification, binding corporate rules, legal bases (derogations) in EUDPD Art (26)1 are options for overcoming an "inadequate" designation.
- ✓ To process data in an EU jurisdiction and if transferring data out of an EU jurisdiction, it is often required to file a notification with the DPA.
- ✓ In Spain if transferring SPI, need the consent of the data subject.

3rd Party Information Sharing Restrictions – Laws governing the sharing of personal information with 3rd parties.

- ✓ Procedures for review and control of data processing vendors required in order to get Binding Corporate Rules approved in the EU, and to comply with Model Contracts and Safe Harbor.
- ✓ In Japan, consent may be required before sharing can occur with another party. Note that subsidiaries are viewed as third parties.
- ✓ Under FCRA, when obtaining background check information, sharing can only occur for use for the same purposes

Privacy Training – Laws governing required privacy training.

- ✓ Privacy training is required in order to get Binding Corporate Rules approved in the EEA and to comply with Model Contracts and Safe Harbor.
- ✓ HIPAA (U.S.) requires conducting privacy training for protection of "protected health information" (PHI) if the company is operating a HIPAA covered self-funded group health benefit plan, or collects health care information through company clinics that conduct certain HIPAA-covered financial and administrative transactions electronically.

Accountability and Audit Requirements – Laws requiring accountability for complaint tracking, audit, incident response, DPA registrations and permit processing and works council notification and review.

- ✓ In Germany, DPO's are required for any location with more than five employees that is processing personal information.
- ✓ In France, DPO's are optional but appointing one will get you more timely responses from the CNIL (DPA), and will relieve you of some of the CNIL's filing requirements.
- ✓ In Italy DPO's are required.
- ✓ HIPAA (U.S.) requires appointing a privacy officer to be responsible for protection of "protected health information" (PHI) covered by HIPAA.
- ✓ Audits required in order to get Binding Corporate Rules approved in the EEA and to comply with Model Contracts and Safe Harbor.

Retention Requirements – Laws governing the minimum and maximum retention requirements for retaining employee information.

- ✓ On February 21, 2006, the European Council adopted a Directive on retention of communication information. It requires "all providers of publicly available communication services" to store and retain communication information.
- ✓ Personal information processed by an EU Whistleblower System should be kept for the period of time necessary for the purpose for which the information have been collected or for which they are further processed.
- ✓ Document retention policy that provides for retaining these records for a period during which they will be legally required or legitimately needed, but that also ensures that all records containing personal information are kept in identifiable form for no longer than legitimately needed.
- ✓ Document retention policy required in order to get Binding Corporate Rules approved in the EEA and to comply with Model Contracts and Safe Harbor.

Occupational Safety – Laws governing safety in the workplace.

- ✓ Federal disability discrimination laws do not prevent employers from obtaining and appropriately using information necessary for a comprehensive emergency evacuation plan.
- ✓ OSHA requires record keeping for workplace accidents.
- ✓ Some states have laws related to bringing weapons in the workplace.

Secondary Usage – Laws governing new uses of personal information beyond what was contained in the notification to the individual.

- ✓ Prospecting for new employees – use of referrals (CAN-SPAM).
- ✓ FTC enforcement of web site deceptive trade practices.
- ✓ FCC requirements for text messaging and cell phone usage the FCC adopted rules to prohibit marketers from sending unsolicited messages to wireless phones and other devices without "opt-in" consent from a consumer.
- ✓ Within the EU, any new or secondary usage requires a new notification and consent from the data subject.

- ✓ EU Data Protection Directive (95/46/EC) Art 6(b) states that personal information must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

Works Councils (EU) - Laws governing the rights of works councils and their effect on cross border flows of information.

- ✓ "Works Councils" are rare outside the EEA and EU, but consultation with or approval by unions or similar groups may be required by collective bargaining agreements in other countries.

The Sample Case (Continued)
The Regulatory Drivers

Company XYZ has documented the locations of employee information at rest as well as the various in-country and minimal cross-border transfers of employee information. Company XYZ with, the assistance of General Counsel, has identified the broad categories of regulatory impact. It has always been the practice of XYZ Company to create a simple process and information model that can be consistent around the world, allowing the company to adhere to most laws, with the exception of the specific labor union and works council laws in the EU. Company XYZ has established a global strategy for each category of law as it relates the employee information summarized below. This strategy will drive a bit of the policy.

Labor Laws: Strive for HR common processes where possible.

Export Laws: Follow local law.

Breach & ID Theft Laws: Global notification to the highest standard globally

Anti-Terrorism Laws: Cooperate as required with local law

Notice & Consent Laws: Provide Notice and offer implicit consent globally

Access & Complaint Laws: Provide reasonable access and a transparent complaint process.

Marketing Permission Laws: Common set of marketing permissions based on opt-in

Ethics & SOX Hotlines: Common set of hotlines

Employee Monitoring: Minimal employee monitoring

Limits on Processing: Common collection, storage, use sharing and trans-border flow

Security Protections: Common global security program.

Restrictions on Cross Border Transfer:

Third Party Information Sharing: No unaffiliated third party sharing.

Privacy Training: All employees will be trained.

Accountability & Audit Requirements: Do it

Occupational Safety: Adhere to local "OSHA" like regulations and monitor locally.

Secondary Usage: Minimize and/or eliminate the need for secondary usage consent.

Works Councils: Adhere to the local practice as required by law.

b. Business Processes and Connections to the Law

This is the first of three correlations that examines what relationships there may be between common business processes relative to the use of employee information and categories of law described in the previous section. The supporting matrix identifies those business processes that may be impacted by one or more elements of a particular category of law. For example, a company that is considering using employee information for a marketing campaign may be subject to laws governing marketing permissions that require the employee's consent. A correlation may also mean that a particular business purpose/process triggers some element of the law. For example, an employee safety incident may result in a U.S. OSHA report filing and subsequent investigation.

Table 8 below is a sample of the correlation information used to frame the observations obtained from businesses processes and the impacted category of law. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 8
Business Processes to Laws

Business Process Category	Summary Business Purpose/Processes	1. Labor Laws	2. Export Laws	3. Security Breach & ID Theft	4. Anti Terrorism Laws	5. Notice & Consent	6. Access & Complaints	7. Marketing permissions	8. Ethics & SOX Hotlines	9. Employee Monitoring	10. Limits on Processing	11. Security Protections	12. X-Border Transfers	13. 3rd Party Data Sharing	14. Privacy Training	15. Accountability & Audit	16. Retention Requirements	17. Occupational Safety	18. Secondary Usage	19. Works Councils (E.U.)
Benefits: EAP	Employee Assistance Process					✓				✓			✓	✓		✓	✓	✓		
Benefits: Health Plan management	Health Plan Management	✓				✓	✓			✓	✓		✓	✓	✓	✓	✓	✓		
Benefits: Supplemental Benefits Admin	Supplemental Benefits Administration	✓				✓						✓	✓	✓	✓	✓	✓			

The findings below are based on observable trends and patterns from the completed matrix and are grouped by process and policy. Naturally, these findings would be revised if those that precede these were to be revised.

Process:

- ✓ Information management, Workforce and Risk Management, Works Council and Compliance related business processes (including auditing and statutory compliance management) are impacted by nearly every category of law.
- ✓ Nearly every business process is impacted by the following categories of law and regulations and therefore would benefit from a common approach:
    - Security Protections
    - Restrictions on trans-border transfers
    - 3rd Party Data Sharing Restrictions
    - Privacy Training
    - Accountability & Audit Requirements
    - Retention Requirements

- ✓ The following business processes would benefit from adopting a common approach to labor management (given the possibility of developing a common definition to labor laws):
    - Benefits
    - Compliance
    - Employee Management
    - Government Reporting
    - Health
    - Safety & Labor Relations Management
    - Legal
    - Payroll & Contract Administration
    - Privacy Management
    - Procurement
    - Recruiting
    - Training & Career Development
    - Travel & Expense Management
    - Workforce Management

Policy:

- ✓ Adopting a Permissions approach to communications related to use of employee information with future, current and former employees for life will benefit employers in a significantly tight workforce over the coming years.
- ✓ Providing an open and transparent notice, information privacy and security program, access and opportunity to dialog and ask questions will build and sustain trust at a time when trust is essential to attracting and retaining employees.
- ✓ Employees want to work for an ethical company. Those companies with strong corporate social responsibility programs, responsible hiring and labor management programs and innovative work environments will be the employers of choice.
- ✓ Employee monitoring that erodes trust may not be worth it.
- ✓ Being a strong advocate on behalf of employees with vendors and third parties is essential to retaining trust as well. Vendor and third party management is critical.

These findings are core findings. They represent the first juncture where a set of business decisions might be drafted as to the use of employee information. Given the footprint of the company, what personal information and sensitive personal information shall be collected for which business processes; to be stored in which location(s); to be used by which individuals in which locations for which purposes performing which roles; to be shared with which entities within the company and outside the company, again for which purposes performing which roles; to be transferred across which borders for which purposes; to be retained for what duration and to be securely destroyed after what period. This composite set of use of employee information will be tested for its completeness and adjusted after the subsequent steps.

The byproducts of this phase are also important to note. While the process was not conducted to identify opportunities for efficiency gains in reengineering processes, it is evident that some reengineering of process would benefit the company if it were to be under taken.

c. Employee Processes and Connections to the Law

This is the second of three correlations that examines what relationships there may be between common employee processes relative to the use of employee information and categories of law described in the previous section. The supporting matrix identifies those categories of law that affect or impact an employee process. For example, the employee process of determining the length of family leave and the business obligation for granting such a leave may be subject to federal labor law (FMLA). For example, an employee process may trigger or invoke a law because of the theft of a laptop. If the theft occurred during work related travel or work from home, this could trigger security breach notification laws.

Table 9 below is a sample of the correlation information used to frame the observations obtained from employee processes and the impacted category of law. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 9
Employee Processes to Laws

Employee Process Category	Detail Employee Processes	1. Labor Laws	2. Export Laws	3. Security Breach & ID Theft	4. Anti Terrorism Laws	5. Notice & Consent	6. Access & Complaints	7. Marketing permissions	8. Ethics & SOX Hotlines	9. Employee Monitoring	10. Limits on Processing	11. Security Protections	12. X-Border Transfers	13. 3rd Party Data Sharing	14. Privacy Training	15. Accountability & Audit	16. Retention Requirements	17. Occupational Safety	18. Secondary Usage	19. Works Councils (E.U.)
Career	Career Planning																			
Career	Educate Oneself														✓					
Career	Establish Work Experience					✓						✓								
Financial	Manage Finances																			
Financial	Monitor Credit & Background									✓		✓	✓	✓		✓	✓			

The observations below are process related and based on observable trends and patterns from the completed matrix.

- ✓ Some of the employee initiated processes identified may not result in PI that is retained by the employer.
- ✓ PI that is generated and subsequently retained by the employer is subject to full access under anti-terrorism laws, access and complaints laws, cross-border transfer laws and retention requirements laws.
- ✓ Most employee initiated processes are governed by one or more categories of law.
- ✓ There is a corresponding business process for nearly all categories employee-initiated processes.
- ✓ Employees will need to understand the impact of the laws before they will be able to fully protect their PI/SPI or perhaps there will be a set of tools that they will depend upon to be their Privacy Editor, Privacy Sheriff, Privacy Agent and Security Guard.

At this juncture the company would then review and adjust its business decisions, adding or removing PI and adding or removing business processes to accommodate the employee sensitivities and their need for education.

d. Employee Information and Connections to the Law

This is the third of three correlations that examines what relationships there may be between employee information elements and categories of law described in the previous section.

A correlation may mean that the law affects or impacts the use of the information, such as a labor law may prevent the use of race during hiring. A privacy law may affect the use of an e-mail address for marketing if the individual has not given permission to receive marketing material. It may also mean that the information triggers some element of the law, for example, a foreign national (aka their nationality) may not be able to have access, under the export laws to certain government information.

Table 10 below is a sample of the correlation information used to frame the observations obtained from employee processes and the impacted category of law. Note that this sample table represents a composite view developed by RIM Council member companies for reference only. Companies looking to use this framework should go through their own exercise and analysis to arrive at the appropriate decision for their organization.

Table 10
Employee Information to Laws

Information Category	Information Elements	1. Labor Laws	2. Export Laws	3. Security Breach & ID Theft Laws	4. Anti Terrorism Laws	5. Notice & Consent	6. Access & Complaints	7. Marketing permissions	8. Ethics & SOX Hotlines	9. Employee Monitoring	10. Limits on Processing	11. Security Protections	12. X-Border Transfers	13. 3rd Party Data Sharing	14. Privacy Training	15. Accountability & Audit	16. Retention Requirements	17. Occupational Safety	18. Secondary Usage	19. Works Councils (E.U.)
Personal	Charitable Contributions				✓		✓						✓				✓		✓	
Personal	Citizenship		✓		✓		✓						✓				✓		✓	
Personal	Country of Residence				✓		✓						✓				✓		✓	
Sensitive Benefits- Financial	Salary & Compensation				✓		✓						✓				✓		✓	✓
Sensitive Benefits- Financial	Salary Plan				✓		✓						✓				✓		✓	✓

The observations below are based on trends and patterns from the completed matrix and are grouped by information, process and policy.

Information:

- ✓ All information categories and associated information elements are subject to laws governing access through anti-terrorism laws, access rights and complaint process laws, restrictions on cross-border transfer laws, minimum and maximum retention requirement and schedule laws, and restrictions on secondary usage laws.
- ✓ Labor laws touch many information categories including performance, personal, sensitive background and discrimination related information, sensitive health information, work history and current work information.
- ✓ It is the labor laws that often differ by jurisdiction. These differences have often been accommodated by local procedures and implementation rather than common global procedures and implementations. This allows some employment practices to be rather rigorous where there are laws and other employment practices to favor businesses where there are fewer labor laws.
- ✓ Security protection laws address not only system based PI and SPI, but also sensitive background, discrimination, financial and health information on paper as well as electronic.

- ✓ Privacy training laws are primarily applicable to several information elements in sensitive-discrimination information category and sensitive-health information category.
- ✓ Export laws apply to protecting the export of military personnel by protecting the export of their military history and classification.

Process:

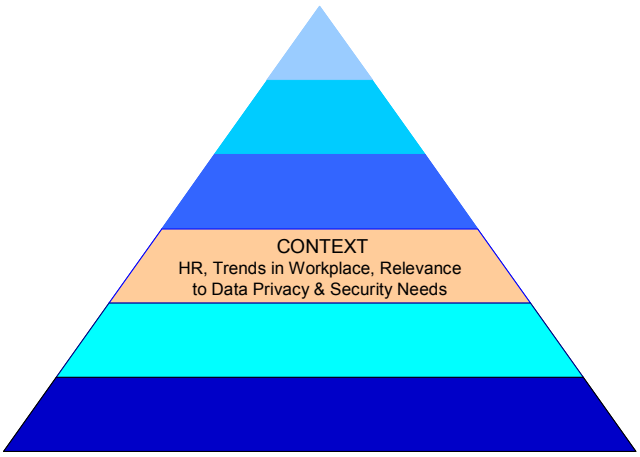
- ✓ It would benefit business to review its operational and information practices across its jurisdictions to discover just how different the processes are or are not.
- ✓ Laws that limit certain processing (especially secondary processing) without permission are primarily applicable to information categories such as sensitive-EU sensitive information, sensitive-financial and sensitive-health information. This correlates closely to employee needs to provide permission before information elements such as sensitive-financial and sensitive-health to are used for a new purpose.

Policy:

- ✓ Due to the increase in losses of PI and SPI in the U.S., Canada and Japan in 2005/2006 and to the rise in identity theft many countries will develop and implement security protection and breach notification laws that help protect individuals from the loss of PI/SPI that contributes to information that leads to identity theft.
- ✓ Over time the definition of SPI as it relates to identity theft will expand from what it is today, which includes SSN, bank number, credit card number, genetic information, biometric identifiers or driver's license information in conjunction with name to include birth date, other government issued ids, address plus maiden name to name a few options.
- ✓ As the definitions of SPI expand, so will the limitations on use of certain PI/SPI without permission. Also, the requirement for additional security will expand as well.
- ✓ The definition of secondary use as it relates to the privacy notice is critical. It is important to note that most companies state explicitly in their privacy notification the full primary purpose, making the need for permissions for additional secondary use(s) less important.
- ✓ The e-Discovery process in the U.S. creates a dilemma regarding adhering to regulations outside of the U.S. For example, in the EU citizens are allowed private use of company email under certain circumstances. This part of the email is to be free from employee monitoring and discovery for litigation purposes. The current processes that extract, load and then search documents in the e-Discovery process do not provide the capability refrain from extracting the personal emails of EU citizens. The U.S. law requires that it is all discoverable, thus creating a dilemma. The same is true relative to employee monitoring.
- ✓ Employee monitoring will expand from potentially phone usage, to email and internet usage to perhaps vehicle tracking, file transport tracking, video monitoring to tying it all together in some integrated monitoring form.
- ✓ Works councils in the EU can delay implementation of new policy for many, many months. They can also demand changes to policy that would be difficult to adhere and can create regulatory requirements that are unreasonable.

At this juncture the company would then review and adjust its business decisions again, adding or removing PI and adding or removing business processes to accommodate the these findings.

5. The Context: Meeting the Information Privacy and Security Needs of the Total Workforce



We now have proceeded up the pyramid of information gathering and analysis on the information privacy, security needs and regulatory requirements of the business and to some extent the information privacy and security needs of the employee. To further the decision-making process, what will a given decision mean in the overall context of workforce management? The observation and research suggest the bottom line today is that information privacy and security needs of the employee are not currently a driving factor when an individual is considering employment.

The Sample Case (Continued)
The Context: Meeting the Information Privacy and Security Needs
Of the Total Workforce

Company XYZ has now developed a visual representation of the implications of the five possible solutions for an employee privacy policy strategy. This representation takes into account where and how employee information is accessed, stored and moved as well as the regulatory requirements for notice and consent within each country of operation. A preliminary decision has been reached as to the 'best' strategy. The next set of analyses can provide 'adjustments' or further quantification to this solution based on projections of workforce attributes and composition.

a. Relevance to the new age and upcoming/future employees

Do the engagement drivers change with the new worker?
Do the engagement drivers change for the existing workforce and the workforce that is moving towards retirement?

The Manpower Inc. whitepaper, *Engaging the Total Workforce*, refers to the combination of permanent and contingent workforces as the "Total Workforce" of human resources that employers now rely on to conduct business. The paper defines the contingent workforce groups as temporary employees, contractors, outsourced employees and consultants. Although there is no official data on the total size of the contingent workforce, Manpower estimates that it represents approximately 20 percent of the average company's total workforce. For this paper we will use the research embodied in the Manpower Inc. to consider the factors that drive individuals when they are considering employment.

Currently the twelve engagement drivers identified which most affect motivation and performance of both permanent and contingent employees alike are the following:

- ✓ Being treated with respect
- ✓ Having a clear understanding of what is expected
- ✓ Having a sense of belonging
- ✓ Being treated equally
- ✓ Access to tools, resources and information to perform
- ✓ Receiving the training that is needed to perform in the role
- ✓ Open and honest two-way feedback
- ✓ Strong teamwork
- ✓ Receiving recognition
- ✓ Opportunities to learn, develop and progress
- ✓ Understanding how the role contributes to the success of the business
- ✓ Security (Job)

However, the needs of the workforce may be changing in much the same way as consumers have become more aware of privacy and information security. The biggest driver of the need for information security and privacy, as with the consumer, is the loss of sensitive personal information due to security breaches. The number of employees that have received security breach notifications has already become a significant portion of the country's population. This in turn may increase the level of fear and concern over all the employee information that the employee views as sensitive, which may be far more than just the current narrow definition of financial account numbers, driver's license numbers, name, health information and the EU SPI information.

Naturally, security breaches may also drive additional legislation and regulation that will require employers to respond with further protection of the employee's sensitive personal information. Currently draft legislation is also expanding the definition of SPI. The decision companies may be faced with is a decision to broaden the definition of what to protect.

So perhaps a company may consider anticipating a change in the employee driver where and the employee may choose to work for a company or to leave a company based upon the company's ability to protect the privacy and security of their information. This may be especially relevant in the company that holds information about a large number of employees, across a number of global locations and also chooses to centralize its employee information. Naturally, this company's breach would more likely to be a media event, especially if the PI contained a sizeable amount of SPI.

b. Trends in the Workplace

The future workers will also have unique needs and come to the work place with a different set of values.

In the Gartner report dated May 15, 2006 entitled, *Campus Trends Portend Challenges in Next-Generation Workforce*, several key observations are made about the soon-to-enter the workforce student population. They will come to the work with "high computing efficiency and greater collaborative behavior than their predecessors." This suggests that the engagement drive stressing strong teamwork will be even more important for the upcoming employees.

This report also suggests that this generation will have an, "expectation that their organization's computing environment is a work-life toolkit that will allow them to blend personal and professional activities." This will present a challenge for employers as they consider internal guidelines in the monitoring of employee use of the Internet and e-mails.

In the Gartner report dated March 27, 2006 entitled, *Future Worker 2015: Extreme Individualization*, baby boomers (today's 45-55 year olds) will lead another wave of entrepreneurship and innovation." For these

workers, the engagement driver of security may be less important, but they will be required to expand their skills to operate in the digital environment as defined by the younger part of the workforce.

From the Employee's perspective:

What changes are we expecting in the ways we work?

The Gartner report states that the worker of the future (2015) "will be more independent and take control over defining their workplace and work models." There will then be more personalization of the workplace presenting a new set of challenges for employers as they determine ways to secure PI/SPI in a more decentralized environment.

A second key issue projected for the future workplace environment involves the manner in which businesses determine the technology (software and hardware) that is used by employees. In today's work environment these decisions are made based on the enterprise's need designed for use by the broadest number of employees as possible. Gartner describes this method as 'pushing' the technology to the employee. They project that this method will not meet the needs of the future worker as stated in the previous paragraph, will want far more control and independence in selecting and personalizing their workplace technologies.

From the Employer's perspective:

What changes are we expecting in the ways we work?

The Gartner report further summarizes three key underlying truths that will share the workplace in the future:

- ✓ The extremely individualized worker will have tremendous influence over how the future work environment takes shape.
- ✓ Human beings will gravitate toward other human beings, not only face to face but increasingly virtually.
- ✓ Smart companies will capitalize on people's natural affinity to work with other people – not as units of production but rather as engines of innovation.

c. The Relevance of it all to the Information Privacy and Security Needs of the Workforce

What will be the challenges of Information Privacy and Security in this new world of work?

There will be old challenges offered up not only in new ways, but perhaps with different outcomes. A recent case study in the *Harvard Business Review* of June 2007 entitled, "We Googled You," presents a not-so-far-fetched scenario in which a prospective employee's past associations easily found on the Internet presented a real dilemma for the hiring company and the job they wanted to the applicant to perform. The issues presented in this case study suggest:

- ✓ Younger employees (under 30) have grown-up with the Internet and are comfortable posting sensitive personal information.
- ✓ It cannot be assumed that a younger employee will have that same comfortable view of an employer sharing their personal information.
- ✓ It cannot be assumed that employee information obtained from broadly available sources on the Internet is accurate.
- ✓ Accepting applicants with questionable Internet posted personal information may be an appropriate price to pay for employees with digital savvy and experience.

In a future world where people will function and move freely in far-reaching virtual communities, companies will need to look at how to leverage that fluid environment with their employees. The Gartner report dated

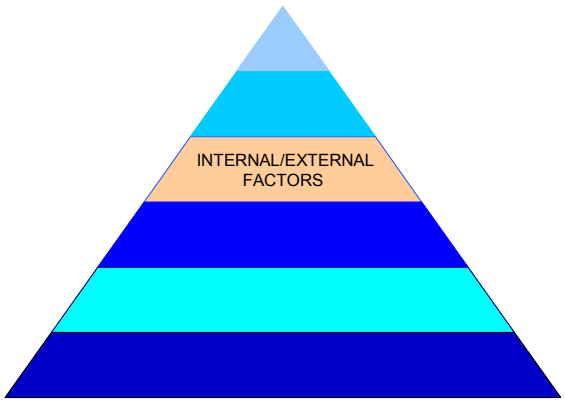
March 27, 2006 entitled, *Future Worker 2015: Extreme Individualization* describes three challenges companies will face:

- ✓ Can they translate those large and fluid networks of trusted friends into professional contacts and value?
- ✓ Can they set effective guidelines for interaction across cultures and regions and for privacy and confidentiality in these virtual communities?
- ✓ Do they have applications and infrastructure in place for secure collaboration, management and distribution of information?

If a company can overcome the challenges described in these three bullets the Gartner report suggests that benefits can be realized.

At this juncture the company would then review again its business decisions again, adding or removing PI and adding or removing business processes to accommodate the these findings. The intersection of the significant impact of technology and social networking that the future worker has grown accustom to with the fact that to date privacy and security have not been primary decision making factors in the hiring process needs to be seriously factored into our key business decisions to ensure that we strike a balance in our overall use of employee information. Certainly we all want to protect PI, however we also want to meet the challenges we face in continuing to deliver the rich functionality that the future worker has grown accustom to.

6. Internal and External Factors



The Sample Case (Continued)
Internal and External Factors

Company XYZ needs to conduct one last examination to provide 'adjustments' or further quantification to the preliminary decision based on global economic projections and their possible impact on countries of operation. Also important are projections of government stability in the countries of operation. Each of these projections should be further quantified in terms of the probability of occurring and the resulting risk to the company.

a. The Global Economy

What are the connections in the overall global economy?
As Asia emerges and re-emerges as a driving economic force what are the ramifications for Europe, North America and the other regions of the world?
What are the impacts of a U.S. economic slow down to the overall global economy?

This section is the section that is the most specific to a given company, because the business observations are tied to so many different factors that effect the company's directions. Different companies are affected more or less deeply by these factors, due to their industry and their current geographical footprint and are able to profit more or less by these factors.

- ✓ The speed at which change is occurring in the global economy is increasing.
- ✓ From year to year economic growth and earning power has shifted from one country to another and one region to another.
- ✓ One year the U.S. for example has a banner year and many countries in the EU are suffering with a very sluggish economy, while China and India and other countries in Asia are enjoying resurgence.
- ✓ The next year it reverses itself and the EU strengthens and the U.S. lags behind.
- ✓ War and peace follow a similar cycle with a fragile stability and a constant threat of problems in certain countries.
- ✓ The era of the terrorist further complicates matters from a number of perspectives. Certainly our overall safety and the lives of those lost during the various attacks around the world.
- ✓ The overall shortage of skilled workers has many companies and countries searching for the best and the brightest globally, willing to import them from where ever it takes.
- ✓ The pockets of shortages in certain countries and companies to import skills that are in high demand are driving mass flows of persons from one country to another in another part of the world. Extreme poverty in one nation is also contributing to that flow of individuals leaving their country to look for work to support their families back home.
- ✓ The company that is flexible and dynamic that can move business processes and information to react in response to such a requirement, while still balancing the needs of their total workforce, will be the company that will be able to win in the changing world of work. It will not be simple.

b. The Workforce: Will the staff be available to do the work that you need done?

Where will you find the skilled workforce you need?
What does it take to attract and retain these skilled workers? How long will we need these skills?
What about the unskilled workforce? What responsibility do we have to these workers?

The Manpower Inc. report, *Confronting the Talent Crunch: 2007,* clearly describes the challenges and the opportunities many governments and businesses have and will have in acquiring and keeping the skilled workers they will need to sustain the business and the economies over the next ten years. The paper explores a number of ways that might be used to reduce the demand and/or increase the supply of these resources. Businesses will need to be prepared for significant changes in the skills that are required. Rather than wholesale replacement, businesses are encouraged to consider helping employees stay fit for the race; facilitate re-skilling and up-skilling programs; entertain job redesign; consider more flexible use of available talent; encourage prolonged working life.

The Manpower Inc. report, *The New Agenda for an Older Workforce*, looks at several global trends of the workforce. "According to the Organization for Economic Co-operation and Development (OECD), between 2025 and 2030, 12 million people a year will be exiting the global workforce." In countries with older populations such as Japan, Italy and Germany, this will represent a significant management challenge to replace these job vacancies with qualified people. Increases in retirement levels will be acerbated by talent shortages already becoming pervasive in many countries.

This increase in retirement and the available pool of talent may be mitigated to the extent that older workers take steps to minimize the impact of reductions in company-paid retirement programs. The Manpower Inc. report states, "Although the percentage of older adults who are working longer is growing in some countries, most would still prefer to leave the workforce as early as their financial situation will allow."

Given the increased interdependence on the global workforce, internal factors (those within an enterprise's control) and external factors (those beyond an enterprise's control) matter in the decision process. Which of the external and internal factors in the decision about using personal information are critical? What is needed in a company's privacy and security program in order to support the information decision?

c. Internal Factors that Matter: The Corporate "Radio Dials"

What is your corporate culture? What are your values?
How do we know, behave, relate, recognize and pursue?

Using the "radio dial" questions below, each company would place themselves on the continuum based upon their collective understanding of these questions. While the questions themselves could be refined the idea is to create a picture on a page of the corporation and its culture. This is both an enabler and a limiting factor in making decisions about the use of employee information because these are factors that do not change over night, especially the more culturally oriented ones. It is very important to get this exercise right because decisions must be made in the context of the corporate culture.

Corporate Global Presence Today and Tomorrow
- ✓ *Are you global or local?*

Business and Client Strategy Today and Tomorrow
- ✓ *Are you multi-brand and integrated or are your lines of business siloed and independent?*

Privacy and Security Strategy Today and Tomorrow
- ✓ *Have you taken a global high road to Privacy and Security or a minimalist approach?*

Employee Status on the Engagement Model Today and Tomorrow
- ✓ *Are you employee centric or focused on business at all cost?*

Workforce Composition Today and Tomorrow
- ✓ *How dependent are you on skilled labor vs. unskilled labor & does it matter where your labor is?*

Unions and Works Council Status Today and Tomorrow
- ✓ *Are you relatively free of unions and works council oversight heavily involved with such oversight?*

Workforce Outsourcing Today and Tomorrow
- ✓ *Are you outsourcing in some way 15-20% of your non-critical work product or significantly less?*

Complexity Factor[xiii]
- ✓ *Are you a complex company or a non-complex company?*

Operation Factor[xiv]
- ✓ *Have you knitted your company together operationally with strong "threads" or not?*

Company Approach to Location of Employee Information
- ✓ *Have you established a centralized approach to Employee information or a decentralized approach?*

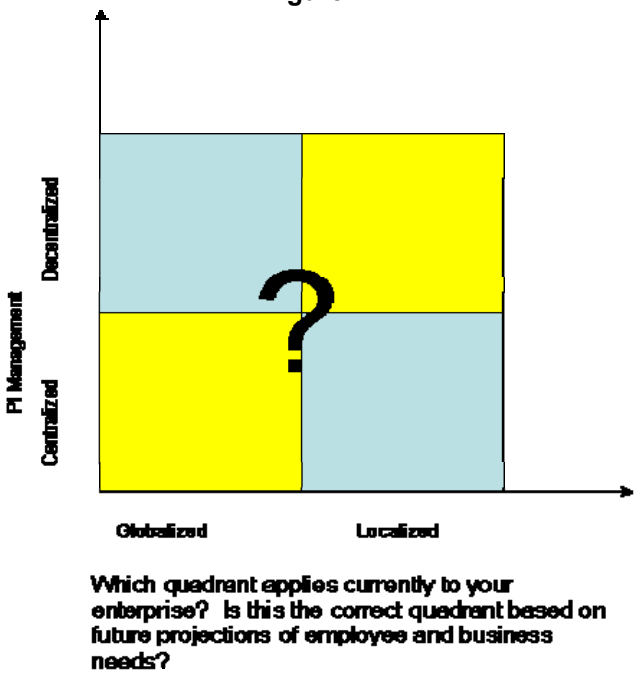
d. External Factors that Matter: Quadrant Analysis

Finally this level on our framework pyramid, recommends taking a look at external and internal strategic factors that could influence the decisions on use of employee information and processes. While the extremes of these factors are quantified below, it can be useful to consider these factors on a continuum.

They can be instructive in placing your organization in an environment on the continuum today and/or also projecting your organization's position in that environment in the future. Figure 2 below is an example of a quadrant analysis that considers the external business environment of globalized versus localized as compared to the decision to manage PII in a centralized or decentralized manner.

Our goal is to consolidate this quadrant approach with the above radio dial approach to come up with one exercise or a consolidation exercise that brings the two together.

Figure 2



- ✓ *Globalized vs. Localized – Centralized vs. Decentralized PII Management*
  Does your enterprise have a presence in more than the U.S.? Is your enterprise currently in many countries but projects no expansion for the future? Is your enterprise forecasting a contraction in the number of countries?

- ✓ *Global Pandemic or Healthy Population – Highly Automated and Connected vs. Manual and Localized*
  Does your enterprise have a presence in countries that are more susceptible to pandemic? If strategic analysis suggests that a pandemic is likely, what steps would you take to protect the health information of your employees?

- ✓ *Global Peace or War - Highly Automated and Connected vs. Manual and Localized*
  Does your enterprise operate in one or more volatile regions of the world? Does your enterprise have contingency plans to move PI/SPI processing to manual in the event of service disruption?

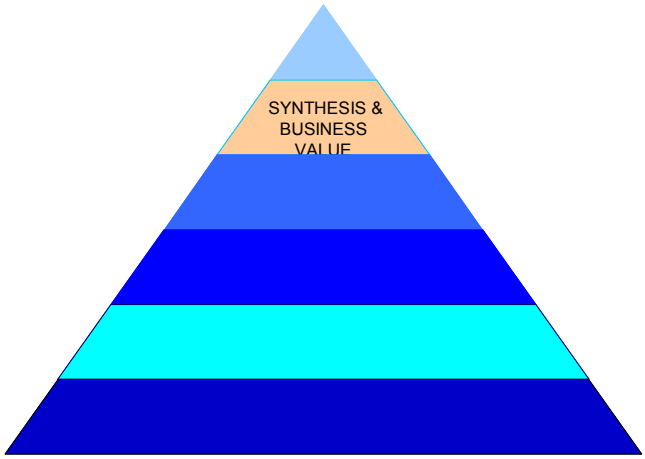
- ✓ *Reemerging and Emerging Economies vs. Slow Growth Economies – Highly Mobile Workforce vs. Stationary Workforce*
  Does your enterprise operate in mostly emerging or reemerging economies? How does that impact workforce mobility and opportunities?

- ✓ *The Hope or Fear Factor – Highly Mobile Workforce vs. Stationary Workforce*
  What are the attitudes of the population in the countries of operation? Are people upbeat or pessimistic about the future? How does that impact the workforce? Are people willing to move to different regions when they have a pessimistic view of the future?

- ✓ *Legislative Activity or No Regulation - Highly Mobile Workforce vs. Stationary Workforce*
  Does your enterprise operate in a country or countries where there is significant legislative activity? Conversely, do you operate in a country or countries where there is little or no regulation? Does the highly legislated environment have an impact on the mobility of the workforce?

If there is a time in this process to thoroughly review the core findings, it is at this point. The business decisions; the footprint of the company; the PI/SPI collected, stored, used, shared, transported, retained and securely destroyed; by which entities within the company, outside of the company, in which locations, by which roles are all open for renegotiation. Those companies that have focused on their core competencies might chose to come together with their key business partners at this time, to use this opportunity, not only to perform the use of employee information, but also to solidify opportunities for efficiency gains in reengineering processes. Together or as a company alone this is the time that some reengineering of process would benefit the company if it were to be under taken.

7. Synthesis and Business Value



Synthesis suggests taking all of the information and correlations that we have discussed and putting them together to create a complete picture of the use of employee information. In this case the 'complete picture' is one or more decisions related to how and what a company will do relative to their processing of employee information. Figure 3 below suggests that it is a step-by-step process where questions are raised, relevant information defined and a series of analysis conducted, resulting in an ongoing refinement of preliminary decisions. Those preliminary decisions are then filtered through factors that may not be easily quantified but rather are based on probability risks.

Finally there is the question of what is the value to the business of proceeding with a decision or decisions reached.

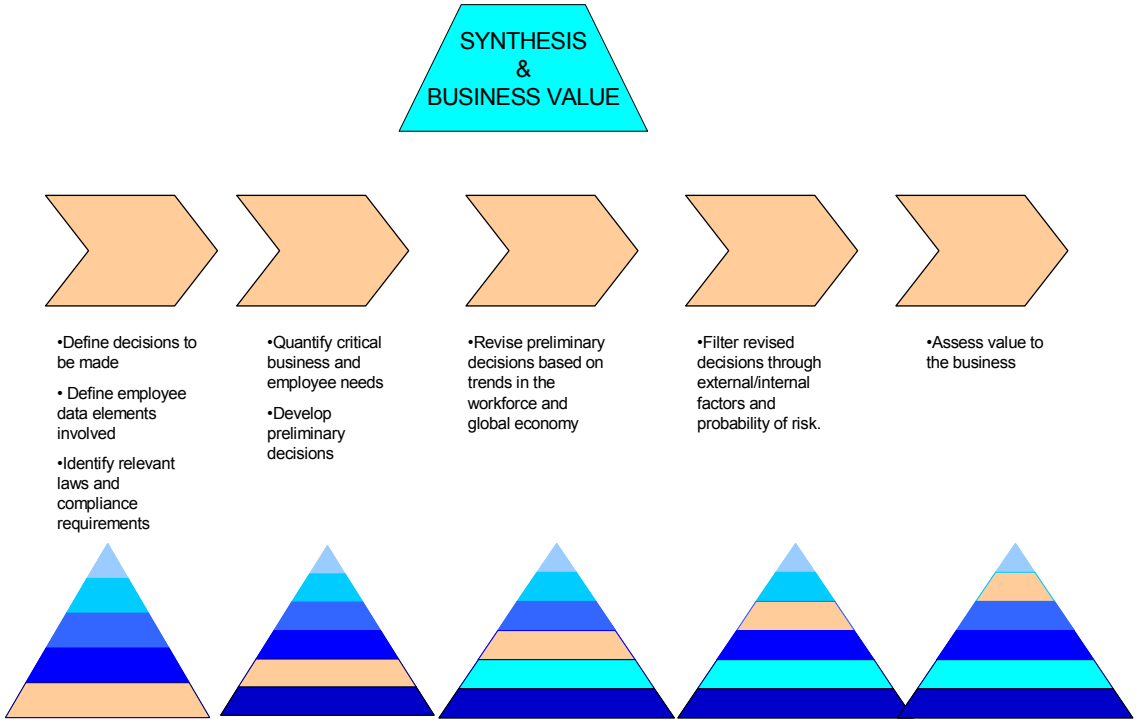
- ✓ *What are the expected returns to the company as it relates to the employee?*
- ✓ *What are the expected financial returns to the company?*
  - *Reduced FTE?*
  - *Reduced Hardware?*
  - *Other Capital Returns?*
- ✓ *What are the expected Non-financial returns?*

The value to the business can be quantified as:

- ✓ Improve information efficiency - Only PI/SPI information minimally required is collected and stored.
- ✓ Attainable level of legal compliance - Sharing of PI/SPI information is consistently and legally defined across internal and external business units.
- ✓ Improve employee trust – Employee perceptions of SPI information is acknowledged and honored whenever feasible.
- ✓ Reduce risk – Privacy related employee data breaches could be minimized.
- ✓ Gain workforce flexibility -- Position the enterprise to accommodate the emerging workforce.
- ✓ Gain significant innovation without the need of growing a workforce.
- ✓ Eliminate business processes – Elimination of FTE and equipment
- ✓ Streamline business processes – Elimination of FTE and equipment
- ✓ Lower unit costs – Outsourcing and/or off-shoring
- ✓ Automate business processes – Elimination of FTE
- ✓ Vendor Information Checklist – Facilitate the management and auditing of vendors

Taken in context, a decision made in this step-by-step manner reflects a process that is similar in nature to typical product, marketing, even financial decisions that companies make. It takes more time, but ultimately it is understood what risks a business may be incurring by one set of decisions versus another set of decisions. For example, if it is determined that the future trends in the workplace necessitate focusing employee resources in an APEC country versus an EU country, a different set of decisions would result.

Figure 3



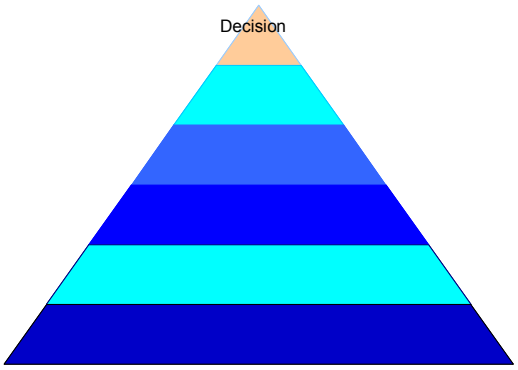
The Sample Case (Continued)
Synthesis and Business Value

The final task is to assess the financial implications of the decision in terms of cost of implementation and the possible value to the company. To summarize the cost implications of each of our possible solutions:

1. A policy for U.S., a policy for EU and EU like countries and a policy for all others (with country specific supplements) with no global commitment for protection, allowing only free flow of employee information where countries permit it - It may require the Company to continue to maintain the majority of its sensitive personnel information in the original country because it is difficult to obtain a permit to transport sensitive personal information. This might minimize the opportunity for outsourcing. This would result in higher implementation and maintenance costs for PI/SPI in each individual country. The higher the number of countries, the more expensive and more difficult it will be to maintain consistency of data and applications across multiple and independent databases.
2. One global policy with a global protection commitment for all with separate notice requirements for each country – This strategy might allow the Company to consolidate most all of its personnel information into a global database including sensitive personal information from countries (most of them) that would permit it. This would also allow the opportunity for outsourcing. This would result in lower implementation and maintenance costs for PI/SPI in a global database. Additionally it would be easier to maintain consistency of data and applications. While outsourcing would be a viable option, it does raise the risk of breaches if strong controls are not put in place.
3. Individual country policy without a requirement for a global commitment for protection - would definitely require the Company to continue to maintain the personnel information of its employees in certain countries in the original country. This would eliminate the opportunity for outsourcing. This would result in higher implementation and maintenance costs for PI/SPI when maintained in each country. Additionally it would be more difficult to maintain consistency of data and applications across multiple countries.
4. An EU based (minimum standard) policy for all countries - might allow the Company to consolidate most all of its personnel information into a global database, including some of its sensitive personal information. This standard however may not be the highest over time. This would definitely allow the opportunity for some outsourcing. This would result in lower implementation and maintenance costs for PI/SPI in a global database. Additionally it would be easier to maintain consistency of data and applications. While outsourcing would be a viable option, it does raise the risk of breaches if strong controls are not put in place.
5. No separate employee privacy policy – may have privacy built into confidentiality agreements - It would allow the Company to consolidate a little of its personnel information into a global database. This would only allow the opportunity for outsourcing of functions that did not involve personal information across countries. Because of the possible hybrid nature of some PI consolidated into a global database and some company specific, this would be the most costly to implement and maintain data and applications. The same increases in costs would be seen in trying to outsource this hybrid environment to a third party.

Note that there are many other pros and cons one would want to weigh. This example is a rather simple one for illustration purposes only.

8. Concluding Remarks – The Final Decision



The Use of Information Management Framework can be used at a number of different levels, from summary to detail, to facilitate the decisions regarding the use of employee information and to gain efficiencies of and flexibility in business operations as the world of work changes dynamically from day to day. Since the process is repeatable at all levels it can be used regularly to facilitate a retooling process when needed, ensuring that the use of employee information continues to be used as planned. The key to repeatability is good documentation especially in the first phase of fact finding of the four key categories of information that form the foundation for the analysis and decisions to follow.

The Sample Case (continued)
The Final Decision can be selected from the table below

Use of Employee Information Framework
Sample Draft Case Decision Matrix

The following table documents those employee privacy policy choices as they relate to the elements of the UEI Framework analysis.

Objective	Policy Options with the Sample Analysis of Each Framework Step				
Framework Step by Step Process	A policy for U.S., a policy for EU and EU like countries and a policy for all others (with country specific supplements)	One global policy with separate notice requirements for each country	Individual country policy	An EU based (minimum standard) policy for all countries	No separate employee privacy policy
1. Sample Case - Company XYZ Objectives: Consolidate PI/SPI; Outsource select processing; Retain the one contingent worker provider company; Use tracking technologies					
2. Laying the Foundation – Information Inventory & Regulatory Considerations					

Objective	Policy Options with the Sample Analysis of Each Framework Step				
Framework Step by Step Process	**A policy for U.S., a policy for EU and EU like countries and a policy for all others (with country specific supplements)**	**One global policy with separate notice requirements for each country**	**Individual country policy**	**An EU based (minimum standard) policy for all countries**	**No separate employee privacy policy**
Information Inventory	Info easily consolidated, distributed/outplaced	Info easily consolidated, distributed/outplaced	Info NOT easily consolidated, distributed/outplaced	Info easily consolidated, distributed/outplaced	Info NOT easily consolidated, distributed/outplaced
Business Processes	Same	Same	Same	Same	Same
Regulatory Considerations	Outsourcing Difficult But might be addressed	Outsourcing Difficult But can be addressed	Outsourcing Difficult and harder to addressed	Outsourcing Difficult But can be address	Outsourcing Difficult and harder to address
3. Key Considerations – Creating a Uniform Process:					
Relating Business Processes to Employee Information	SPI limited – a plus for outsourcing	SPI limited – a plus for outsourcing	SPI NOT limited –No offshore outsourcing	SPI limited – a plus for outsourcing	SPI NOT limited – No offshore outsourcing
Relating Business Processes to Business Observations	Keep workman's compensation local	Keep workman's compensation local	Keep workman's compensation local	Keep workman's compensation local	Keep workman's compensation local
Relating Employee Information to Business Observations	Minimize birth date use, use GPS in U.S. not EU	Minimize birth date use, use GPS all but EU	Minimize birth date use, use GPS all but EU	Minimize birth date use, use no GPS	Minimize birth date use, use no GPS
Relating Employee Information to Employee Needs	Satisfied Employee Needs – Kept Policy Option Open	Satisfied Employee Needs – Kept Policy Option Open	Satisfied Employee Needs – Kept Policy Option Open	Satisfied Employee Needs – Kept Policy Option Open	Satisfied Employee Needs – Kept Policy Option Open
Relating Employee Workplace Activities to Business Processes	Personal Email & Internet Use Policy Acceptable Global Monitoring Policy not Possible	Personal Email & Internet Use Policy Acceptable Global Monitoring Policy not Possible	Personal Email & Internet Use Policy Acceptable Local Monitoring Policy Possible	Personal Email & Internet Use Policy Acceptable Global Monitoring Policy too Limited	Personal Email & Internet Use Policy Acceptable Global Monitoring Policy too Limited
4. Key Considerations - Regulatory Perspective:					
Regulatory Drivers					
Business Processes and Connections to the Law	Regulatory Flexibility with Operational Consistency	Regulatory Consistency & Operational Consistency	Maximum Regulatory Flexibility & Limited Operational Consistency	Regulatory Consistency & Operational Consistency	Maximum Regulatory Flexibility & Little Operational Consistency
Employee Processes and Connections to the Law	Some Global Equality	More Global Equality	Little Global Equality	Some Global Equality	Little/No Global Equality

Objective	Policy Options with the Sample Analysis of Each Framework Step				
Framework Step by Step Process	**A policy for U.S., a policy for EU and EU like countries and a policy for all others (with country specific supplements)**	**One global policy with separate notice requirements for each country**	**Individual country policy**	**An EU based (minimum standard) policy for all countries**	**No separate employee privacy policy**
Employee Information and Connections to the Law	Some Global Protection	More Global Protection	Little Global Protection	Some Global Protection	Little/No Global Protection
5. Context:					
Relevance to the new age and upcoming/future employees	Proactive	More Proactive	Not Proactive	Kind of Proactive	Not Proactive
Trends in the Workplace	Proactive	More Proactive	Not Proactive	Kind of Proactive	Not Proactive
Relevance to Information Privacy and Security Need of the Workforce	Proactive	More Proactive	Not Proactive	Kind of Proactive	Not Proactive
6. Internal & External Factors:					
The Global Economy	Proactive	More Proactive	Not Proactive	Kind of Proactive	Not Proactive
The Workforce	Proactive	More Proactive	Not Proactive	Kind of Proactive	Not Proactive
Internal Factors that Matter	Cost Effective	More Cost Effective	Not Cost Effective	Kind of Cost Effective	Not Cost Effective
External Factors that Matter	Cost Effective	More Cost Effective	Not Cost Effective	Kind of Cost Effective	Not Cost Effective

9. Potential Framework Upgrades

- ✓ Add a privacy and/or security or other compliance policy column to the law matrices so that companies could correlate the information and processes to their policy or policies
- ✓ Also order the columns and rows by priorities (varying) to see what would present itself (this may be a tool to verify the business process and information categories)
- ✓ Add labor laws and export laws to the regulatory descriptions and matrices

10. Potential Ongoing Workplace Program Activities

- ✓ Bring together in a series of discussions the Labor lawyers and the Privacy lawyers. These groups often do not speak and at times contradict each other.
- ✓ Establish a series of discussions around Works Council management.

- ✓ Establish a series of discussions or research around privacy sensitive labor issues that differ globally, such as 1. Diversity and the collection and tracking thereof or not; 2. Sexual Harassment and Pregnancy Discrimination in the workplace around the world; 3. Union Management 4. Data Retention; 5. Data elements that are high controlled from employee law; 6. Others to suggest.
- ✓ Discuss emerging legal issues such as 1. Investigation and Law Enforcement practices; 2. e-Discovery issues across borders; 3. Employee Monitoring.
- ✓ Discuss emerging management and workforce issues such as 1. Virtual Team Management; 2. Cultural Differences; 3. Flexible Working; 4. Language Differences; 5. Performance Management & Succession Management; 5. Vision of the future - Technology will be expanding what is known about an individual (Facebook) - what will companies do - How much will you be required to know; 6. Corporate controls versus employee privacy - How far do you go? Guidance on items such as drug testing and employee monitoring (for example) would be helpful.
- ✓ Discuss contractual issues such as 1. Use of vendors for various employee tasks - training vendors to complete reports that don't send everything (PI related) when it is not needed; 2. Acquisitions - merging different criteria and requirements across companies; 3. How companies control sub-contractor employees in a common environment; 4. Vendors authenticating employees through their call centers.
- ✓ Ensure that the customer privacy program addresses employees as customers.
- ✓ Develop a definition of SENSITIVE personal information – what IT and Security needs to understand and what criteria should be established for handling – what is appropriate for education and training.
- ✓ Develop a definition of primary and secondary use definition for employee information – how should employee 'choice' be defined?

Appendix 1 Correlations – Attached Files

- Business Processes to Employee Information Categories – Table 2
- Business Processes to Business Observations – Table 3
- Employee Information to Business Observations - Table 4
- Employee Information to Employee Needs Research – Table 5
- Employee Workplace Activities to Business Process – Table 6 & 7
- Business Processes to Law Matrix Summary Findings and Observations – Table 8
- Employee Processes to Law Matrix Summary Findings and Observations – Table 9
- Employee Information to Law Summary Findings and Observations – Table 10

Appendix 2 Additional Reference Materials – Attached Files

- Sample Employee Privacy Policy Documents:
  - Solution #2 – one global privacy policy with separate notice requirements for each country: Global Internal Privacy Policy for Employees, Clients & Business Partners – Sample.pdf and Employee Privacy Notice Template.pdf
  - Solution #4 – EU based policy for all countries: EU Based Candidate Data Protection Policy – Sample.pdf

Appendix 3 Additional Reference Material – Available through RIM Council website

- UEI Compliance Practices and Regulatory Drivers 11-10-06.pdf
- UEI Employee Information Use v17.pdf
- Manpower Inc., 2006, *Engaging the Total Workforce*.
- Manpower Inc., 2007, *The New Agenda for an Older Workforce*.
- Ponemon Institute, May 1, 2006, *Americans' Perceptions about Workplace Privacy.*
- Ponemon Institute, Littler Mendelson, April 5, 2007, *Workplace Survey on the Privacy Age Gap.*

Appendix 4 Additional Reference Material

- Gartner, March 27, 2006, *Future Worker 2015: Extreme Individualization.*
- Gartner, May 15, 2006, *Campus Trends Portend Challenges in Next-Generation Workforce.*
- Palmisano, Samuel J., "The Globally Integrated Enterprise," *Foreign Affairs* May/June, 2006.
- "Staying on Top of Your Game: Five Trends that will shape your career in the coming decade," *Fast Company's March Playbook,*
- IAPP, "The German Data Protection Implications of International Group-Wide HR Databases,*" The Privacy Advisor*, September 2006.
- Brettle, Oliver, "Employee Monitoring in the UK and Generally: Concerns Beyond the UE Data Protection Directive," White & Case, 6th Annual Privacy Law Symposium, April 27, 2006.
- Innes-Stuff, Suzanne, "Whistle-Blowing Hotlines under EU Data Protection Law*,"* White & Case, 6th Annual Privacy Law Symposium, April 27, 2006.
- Patané, Marianna, "The Thorny issue of Employee Consent: A European Perspective," White & Case, 6th Annual Privacy Law Symposium, April 27, 2006.
- EU Keynote, "How Multi-National Organizations Can Best Achieve Compliance for Cross-Border Data Transfers."
- Wugmeister, Miriam H. and Karin Retzer, "Cross Border Development: Data Retention – Implications for Business,*"* IAPP *The Privacy Advisor,* March 2006,

- Hengesbaugh, Brian L. and Michael Mensik, "Global Privacy Regulations and HR Outsourcing Arrangements: How to Manage the Regulatory Risks," IAPP *The Privacy Advisor*, June 2006,
- IAPP, "Re-Thinking Privacy: 10 Reasons Why Your Business Should Be More Concerned About Workplace Privacy," *The Privacy Advisor,* April 2006.
- Moisi, Dominique, "The Clash of Emotions," *Foreign Affairs,* January/February 2007.
- Coutu, Diane, "We Googled You," *Harvard Business Review*, June, 2007.

[i] As of 2007
[ii] Through out the entire life cycle of assessment, RFI, RFP, contract negotiation, including model contract and security breach requirements, audits and quality controls, incident preparation, incident management and exit processing
[iii] Processing Purpose as defined in the Privacy Notice includes all of the processing to be done for the individual, rather than depend upon asking for a secondary purpose later on
[iv] This includes information from Employee Assistance Programs, Health Care claims, special disability statuses and programs, time reporting of sick and medical related leaves, to some extent workers compensation and on the job accident, insider trading monitoring and administration and even travel and expense management. This also includes the wider range of IDs, such as driver's licenses, passport #s, national IDs, etc. It also includes the growing list of what is to be defined as Sensitive Personal Information, which is going to increase over time as indicated by the current definition in the Leahy Security and Privacy Act of 2007 bill as of January 2007.
[v] This includes the classification and security of PI/SPI at rest, in transit and in use. It includes comprehensive security programs with policies, standards and procedures for most all industries on-line and off-line, stronger authentication, authorization, administration, monitoring, encryption, surveillance, testing, risk based assessments and generally participation by both employers, vendors, clients and employees. The issues of employee monitoring have yet to unfold.
[vi] These programs support a multi-faceted approach to the workforce. They address everything from a commitment to stopping human trafficking to programs to stop the spread of disease, to the protection of personal information and the commitment to privacy and the support of a diverse workforce.
[vii] In certain countries, it is acceptable to hire based upon age, marital status, child bearing age and potential, race, gender, height, weight, skin color, certain background check information, automated decisioning, certain assessment scores, or certain health related information, etc. While most businesses strive to maintain a fair and equitable hiring process, it is also still a common practice to utilize certain information gathered from the internet from sites like Facebook, or sites that point to political activist activity that would perhaps discourage a company from hiring an individual or pictures to select individuals. As companies make the transition to a consistent company wide program of Candidate Attraction and Selection and Diversity Management Program the full suite of data elements that are the collective object of Labor laws around the world and the laws themselves are candidates for consideration in this program.
[viii] For example, the healthcare system in the U.S. has moved away from SSN as an authentication tool to birth date. Birth date will soon become SPI, forcing those that have implemented such processes to re-architect their systems and processes again.
[ix] Ensure that a comprehensive data flow of PI/SPI is performed for employee information that includes all external entities and all internal processes. Consider all of the various departments within your company as part of your cross-functional team. Consider how to integrate all of the regional and global units to provide a global flow, not just a corporate flow or a single country flow of employee PI/SPI. Include the exception processes such as fraud management, investigations, SOX controls, project management in IT and the Business communities and all of the major lines of business areas plus the support units of IT, Legal, Marketing, Sales, Product Development, Compliance, Audit, HR, Communications, Training, Security, Procurement, Corporate Affairs, PR, Government Affairs, Operations Management from various areas.
[x] Employees rate performance, time reporting, work history and home address & family information as highly sensitive or sensitive, where these are not on the major list of protection from identity theft and harm from the business's perspective
[xi] The Leahy Security and Privacy Act of 2007 includes a combination of address and mother's maiden name; address and online id/password; birth date in the definition of SPI (verify)
[xii] Reference the EDS Ponemon Institute study of 2004, where individuals would not release their SSNs, but would release most of the other information that would contribute to identity theft, such as driver's license.
[xiii] (Create a complexity factor by identifying the following for a Company: # of unique departments or divisions; # of unique product or service lines; # of employees; # of unique groups of employees by skill type; # of unique jurisdictions the company operates in for productions, sales, operation and service; # of systems and data centers; # and type of employee benefits by jurisdiction; # and type of employee related systems including the core product systems if employee data is present; # and location of works councils).

[xiv] (Create an operations factor with some of the following: privacy strategy (such as global consistency, local implementations only, least cost, ensure local and regional requirements are addressable), business strategy (add samples here), employee strategy (add), company values and vision, pending litigation, sector, centralizations or decentralization; location of employees; geographic reach; disbursement; pending legislation, proactive/reactive; risk tolerance; budget factors; FTE factors; Consistency with other compliance programs; Time; Availability of resources internally; presence or absence of existing compliance structure; maturity level; governmental attitudes; degree of regulation; cultural implications and expectations; etc.