Journal of Information, Law and Technology

The Value of Privacy Engineering

Steve Kenny and John Borking
PISA Consortium
Dutch Data Protection Agency

This is a **refereed** article published on: 22 March 2002

Citation: Kenny S and Borking J, 'The Value of Privacy Engineering', Refereed Article, *The Journal of Information, Law and Technology (JILT)*. 2002 (1)
<http://elj.warwick.ac.uk/jilt/02-1/kenny.html>

Abstract

The title of this article The Value of Privacy Engineering we take to consider two currently topical areas of the privacy arena. First, we identify the constituent value drivers o f privacy. Leveraging such drivers will propagate any business model aiming to instantiate privacy. Second, we give an example of how one may implement a privacy strategy through privacy engineering. This article does not therefore address EU policy matters regarding privacy in any explicit sense.

Privacy is an evolving legal, philosophical, technological, compliance and also competitive advantage arena. From a company's perspective, the current absence of standards, competing assurance service lines and the policy divergence between the US and EU make privacy a complex area to address, in terms of both organizational and system architectural design. Augmenting these matters is the resistance to measurement revenue streams exhibit when they are appended to a privacy enlightened business case.

We define privacy engineering as a systematic effort to embed privacy relevant legal primitives into technical and governance design. Because privacy related problems can have so many interrelated, responsible causalities, isolating the roots of risk may be akin to finding a needle in a haystack. In order to unify privacy engineering with *ex-ante* risk management we introduce Design Embedded Privacy Risk Management (DEPRM), a framework developed for the Privacy Incorporated Software Agent (PISA) Consortium <<http://www.cbpweb.nl/bis/top-1-1-9.html>>. DEPRM builds in compliance with data protection legislation, from the very outset of system development. It also encapsulates the theoretical basis of Privacy Enhancing Technologies (PET). PET has been defined as a coherent system of ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing (and storage) of personal data, all without losing the functionality of the system.

Keywords: Reputation, DEPRM, Instantiation, Privacy, Engineering, Data Protection.

1. Introduction

Privacy is an evolving legal, philosophical, technological, compliance and also competitive advantage arena. From a company's perspective, the current absence of standards, competing assurance service lines and the policy divergence between the US and EU make privacy a complex area to address, in terms of both organizational and system architectural design. Augmenting these matters is the resistance to measurement revenue streams exhibit when they are appended to privacy enlightened business cases.

We define privacy engineering as a systematic effort to embed privacy relevant legal primitives into technical and governance design. Because privacy related problems can have so many interrelated, responsible causalities, isolating the roots of risk may be akin to finding a needle in a haystack. In order to unify privacy engineering with *ex-ante* risk management we introduce Design Embedded Privacy Risk Management (DEPRM), a

framework developed for the Privacy Incorporated Software Agent (PISA) Consortium <<http://www.cbpweb.nl/bis/top-1-1-9.html>>. DEPRM builds in compliance with data protection legislation, from the very outset of system development. It also encapsulates the theoretical basis of Privacy Enhancing Technologies (PET) (Hes and Borking, 1998). PET has been defined as a coherent system of ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing (and storage) of personal data, all without losing the functionality of the system (Borking and Raab, 2001, parenthesis added).

2. The Privacy Products and Services Market

At this time there remains a paucity of privacy consulting services [1] and business models aligning privacy initiatives with strategy and competitive advantage enablers. Below we note some potential reasons why the market has yet to fully recognize the potential value inherent in privacy.

- Implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter referred to as The Directive) into national laws is relatively recent - 1st September 2001 in the Dutch case. France and Luxembourg, at time of writing, have yet to ratify their data protection legislation;

- Controllers are dealing with data protection internally without recourse to external assistance and firms are undervaluing both the potential contribution of privacy to their business, and the risks to their business from a strategy dismissive of privacy;

- Data Protection authorities across the European Union still pursue dissimilar operating strategies. The Spanish Data Protection authority has invested heavily in privacy auditing and holds a reputation as being particularly litigious. France on the other hand does not execute audits, while in The Netherlands, Privacy Enhancing Technologies (PET) are promoted as a structural solution for privacy invasion. Exposure to data protection financial punishment within the EU, generally, is of a much smaller explicit first order magnitude than for instance anti-competitive penalties which may be as high as 10% of global group turnover [2];

- Because national data protection authorities have limited educational resources, controllers may not appreciate fully how extensive data protection implications may be. Further, controllers lack of sharing of experiences and knowledge is itself indicative the fledgling stages of a community of practice;

- American and Eastern multi-nationals, at governance level, may be unaware or unconcerned with European data protection legislation.

3. The Demand Structure of Privacy

At time of writing no empirical research exists on current or temporal value customers place in privacy, relative to other variables such as quality of service, salient to product pricing and consumer decision-making. However, from a social anthropological perspective, Perri (2001) identifies three variables intuitively representing a significant composite of a PET demand function.

- Risk perception - as some type of distribution, the shape of which one would imagine can be manipulated;
- Price sensitivity - privacy risk is traded off against price increments;
- Transaction costs - given information asymmetries endemic to monopolistic competition market structures, costs accrue to consumers differentiating amongst the privacy characteristics of service offerings.

The supply side of the privacy market is projected to be influenced by a polarity of perception between *fear* of regulatory developments leading to compliance with available standards, producing *de facto* privacy offerings, and *hope* of a demand cluster of at least sustainable niche market size demanding privacy offerings. Strategic aspirations then present different challenges [3] and possibilities for organizations to manage their available demand structures.

4. The Value of Trusted Brand

The execution of contracts in electronic commerce juxtaposes a delay between payment and delivery over that found in conventional delivery channels for much tangible procurement. Standifird (2001, 279-295) notes that such a delay increases risk for potential buyers due to the new real and perceived possibilities of fraudulent seller behavior presented for instance. Therefore, mechanisms capable of assuring trustworthy behavior, such as i-escrow.com developed. Such mechanisms are founded on the basis of forcing the cost of opportunistic vendor behavior to be greater than its benefit. According to Barney and Hansen (1994, 175-190), reputation serves as a governance mechanism capable of assuring trustworthy behavior. If the marginal cost of reputation in a transaction were less than the marginal gain attributable, reputation would be a source of competitive advantage to which improved margins can be associated[4].

Reputation is itself not a homogeneous entity. Standifird (2001, 279-295) examined 102 successfully concluded eBay auctions of Palm Pilot Vs between January 3 and January 16, 2000. Reputation of sellers was measured by positive, neutral or negative feedback ratings presented to potential buyers, by the eBay site. Limited support was found for sellers with positive reputations being able to sell products at higher prices. Strong support was found for firms with negative reputations being forced to sell products at lower prices however. Therefore, it can be inferred that an increase in negative reputation

will have a greater impact in determining prices than an increase in positive reputation. Two caveats are noteworthy. First, the type of reputation, emerging as significant, could vary in relation to the market position of the incumbent or entrepreneur. Second, reputation may be prioritized temporally in relation to a functional application. Reputation for a particular function, such as fulfillment, may be more important for a given company's current market position than reputation for a function such as sourcing.

5. Achieving Trusted Brand

The case above regarding eBay reputation rating indeed does not decompose the internal variables of reputation. Scientific research on the characteristics of such constituent elements does not yet exist, so limiting greater analytical consideration (indeed one questions if a generic topology would ever be possible to define given the diversity of business models and the function of time). However, given the characteristics of perceived reputation - Standifird, Weinstein and Mayer (1999) define reputation as the current assessment of an organisations desirability, as established by some external person or group of persons - then one may consider the management of employee, partner and customers data as a custodian exercise where demonstrated integrity is paramount[5].

Generally, a corporate ethics initiative will seek to develop integrity, both from organizational and technological perspectives. Integrity is clearly a key construct protecting against negative reputation, indeed the Audit profession has operated viably largely on the basis of its perceived integrity since its inception. In such sensitive cases we may see the *transference* of one (damaged) reputation onto the (good) reputation of any associated entity - a principle leading to a discounted acquisition valuation for instance. Data protection is explicitly concerned with legitimate and transparent processing of data. Such processing is highly akin to a legally derived notion of integrity, the minimum level compliance with which is mandatory, but not limiting.

Demonstrating such beliefs and systems to relying parties may thus become a key component of the firm's reputation strategy. This could be also be achievable through certification from a governmental[6] perspective and good corporate governance, social responsibility and stewardship from a commercial viewpoint. In an operational sense, maintaining good reputation seems to require a fusion of traditional asset contingency planning processes with public relations, marketing and legal strategy, collectively simulating a press disaster scenario for instance.

Considering privacy risk to be a component of compliance risk dovetails neatly with ethical risk. Deck (1999) develops the Friedman [7] argument that as free markets provide a business with adequate incentive to maximize wealth, a residue of duties and obligations accrue in pursuing such ends. Business ethics (and, to a degree, personal ethics) has a part to play in this space, assuming corporate culture can distinguish between 'ought' and 'must'. It follows that both implementation environment and perceived reputation will benefit from ethical initiatives undertaken to accompany privacy engineering. Von Solms (2001) notes resistance of senior management to substantially accept responsibility and accountability in the case of information security. In European data protection, such arguments are superfluous as The Directive defines the data

controller of an organization as its Chief Executive Officer. Data protection therefore fits neatly into senior management's fiduciary responsibility for good corporate governance.

6.The Tangible Value of Privacy

It is relatively easy to measure some subset of total benefits attributable to privacy engineering from categories of revenue, risk, costs and compliance. Revenue may be considered through cross or up selling opportunities with established customers, increased number of transactions per customer and higher repeat business directly attributable to privacy engineering. Clearly achieving credibility in such augmentation with respect to funding decisions depends upon both the experience and skill of the proponent, and to a lesser extent the sophistication of the analysis.

Risk can either be ignored, assigned to someone else or mitigated. In the latter case the costs of mitigation strategy must be less than the perceived loss of potential sales, cost of negative publicity, loss of goodwill and legal exposure[8]. Endangering citizens privacy may in the future trigger on a system developer product liability claims for software (...deliberately) written to jeopardize the privacy of the citizen[9]. It is intuitive to first begin considering risk as it relates to the privacy-engineered integrity of high value information. That is information that generates revenue, information that is essential to the smooth running of the business and information pertaining to future revenue streams - research, new product plans, marketing plans, business intelligence and so on. However, justifying privacy engineering solely on the basis of Fear, Uncertainty and Doubt (FUD) could marginalize privacy as an operating expense, with the result of a lack of consistency in its internal funding profile.

Engineering privacy into systems at the outset clearly will cost less than reacting to possible regulatory developments of the future requiring privacy engineering to be retrofitted. It is the experience of the Dutch Data Protection Authority advising the use of Privacy Enhancing Technologies (PET) for information systems that when developers take as point of departure PET design principles, total cost of ownership increases with no more than 1% (see Borking, 2001). Business cases may easily become less attractive if resultant systems infringe data subject rights and are thus necessarily re-engineered at a cost one suspects greater than 1%, even assuming sufficient documentation.

Proactive privacy engineering may therefore represent cost avoidance for the business process to be developed. Such value can be defined as an opportunity gain, rewarding implementation. Consider also the viability of the business process without privacy engineering. Financial services are one sector where electronic document processing offers substantial paper, processing, postage and printing cost savings[10]. The processing restrictions of data protection legislation applied to such a business process can, however, mitigate against business case value if the implemented system infringes data subject rights and hence is necessarily re-engineered or scrapped.

Compliance relates to cost avoidance and protection of existing revenue streams, indeed, privacy engineering may in the future become a base technology or pre-condition of doing business in the first place. It is useful to split compliance arguments into three subsets.

- *Regulatory* - controller failure to manage data protection may generate negative consequences from national data protection authorities;

- *Competitive* - loss of competitive advantage resulting from competitor opportunity gain from leveraging the value of privacy equating to your opportunity cost;

- *Partner* - failure to implement effective privacy engineering could mean losing the ability to participate with a key partner or club of information sharing partners that use privacy engineering as a integral part of their collective market identity. Corporate customer relationships thus suffer, because partners are not convinced data protection friendly systems are in place, affecting account renewal for instance.

7. Measuring Tangible Value

The most straightforward way to attach numbers to business cases augmented by privacy engineering is by focusing attention first on identifying privacy enabled and enhanced business processes and second on quantifying the incremental value they accrue[11]. Below (adapted from Nash et al, 2001) we generalize three categories of electronic commerce application, Business to Consumer (B2C), internal systems and Business-to-Business (B2B)[12].

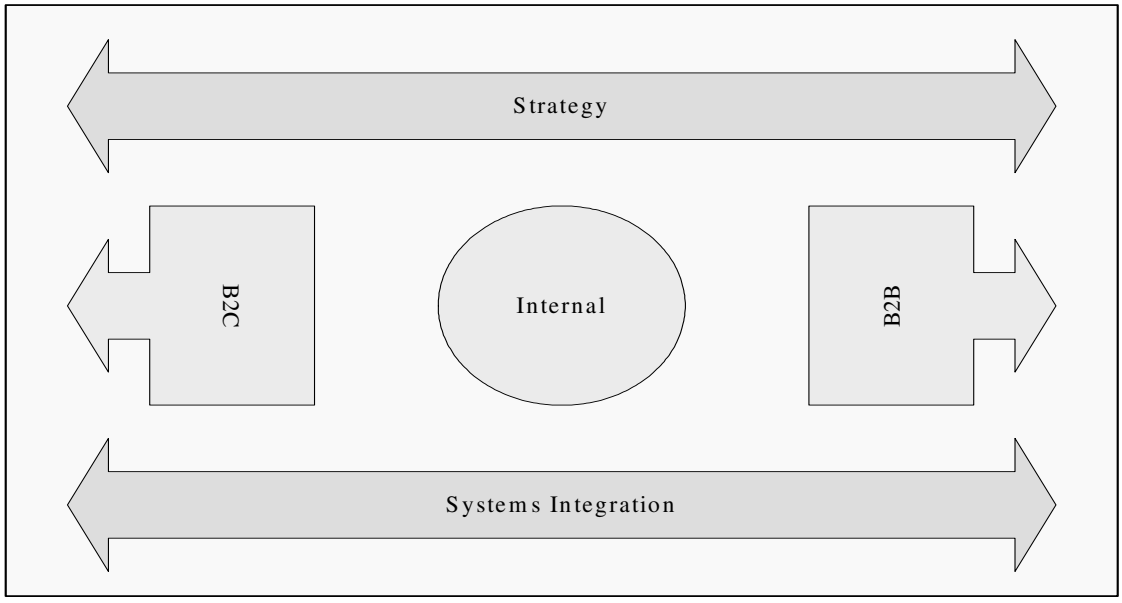

Figure 1: Three Categories of E-Commerce Application

Strategy refers to the alignment of partner business processes and the readiness of customers to adopt e-business applications. Systems integration integrates B2C, internal and B2B processes with each other. Clearly, well documented, integrated and flexible information architectures and database systems are at a base level important (Gartner,

n.d). Several categories of e-business application can be considered in terms of their potential for privacy engineering[13].

- Relationship applications. There is an inherent conflict between users needs for personalized services based on unique preferences, and the traditional PET tenant of minimising the amount of personal data one collects. However, privacy engineering in the health informatics field has resulted in system designs that can guarantee highly conditional linkabilities of identity in terms of access control (see Van Blarkom, 1998);

- Transactional applications. B2C systems provide the functionality to open accounts, submit, modify and track orders. B2B functionality will transmit orders, process invoices and track order status. Clearly, processes should be considered in light of achieving functionality while minimizing the least amount of personal data - as a birth date field, is a range an adequate substitute for the precise data of birth?[14]. System integration considerations could apply to the revision of personal data across all instances of that data;

- Payment / Funds Transfer applications. Electronic payments yield significant information about customers in terms of preferences and buying patterns, which both merchants and card-issuing banks appreciate mining. In the US, the Gramm-Leach Bailey Act[15] regulates financial services companies, yet fears remain that billing data continues to be leveraged as an asset without sufficient regard to citizen rights. What value then the goodwill generated for consumers in response to perceived certainty that their data is processed in accordance with their wishes?

Once targets for privacy engineering have been identified, the simplest way to measure value is by establishing metrics appropriate to the business process under consideration, in concert with high-level business objectives. One may then compare a baseline against the privacy engineered future state through facilitation, defining questions which finally elicit intrinsic value. Because such questions are innately quantifiable, it should then be possible to assess the Euro value of the privacy investment by considering our revenue, risk, cost and compliance constructs[16]. A B2C example is given below.

Figure 2: A Business to Consumer Example

8. Practical Implementation Using a Balanced Scorecard Framework

A key repercussion of the dot com bubble is that companies around the world are transforming themselves for competition based on information. A firm's ability to exploit intangible assets has thus become far greater than their ability to invest and manage physical assets. The Balanced Scorecard (Kaplan and Norton, 1996) enables organisations to track financial results while monitoring the progress in building capabilities and acquiring the intangible assets needed for future growth. In short, the Scorecard links the organisation's long-term strategy with the short-term actions required to achieve that strategy. This cause and effect relationship is illustrated below.

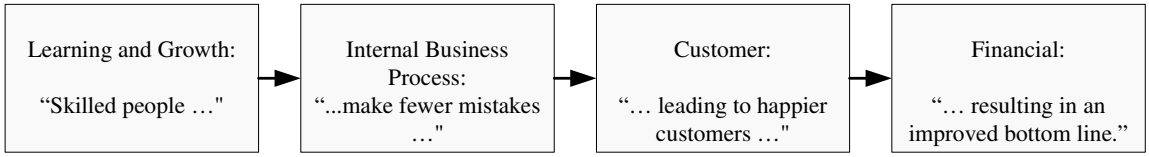

Figure 3: The Cause and Effect Relationship

For the increasing number of customer-facing and other organisations that handle data subject information, it is imperative to adopt processes and initiatives that support them achieving a trusted reputation. The implication of the arguments made is that if the customer's perception of trustworthy behaviour on the part of the company improves, better customer loyalty is available which leads to an improved bottom line. All organisations, not only those that are customer facing and organised around their customer information, need to integrate the aspects of protecting data subject data while instantiating legitimate processing on that data, throughout all aspects of their organisation. Using the Balanced Scorecard would be one such way to ensure that such initiatives are properly linked and measured for an improvement in the medium term bottom line of the organisation.

9.Comparative Legal Privacy Landscape

In Europe, privacy is a human right, defined in Article 8 of the 1950 European Convention of Human rights, and one of the most important human right issues of our evolving information age (Banisar, 2000). Today, informational privacy[17] is defined for individuals through two European Union Data Protection Directives 95/46/EC (The Directive)[18] and 97/66/EC[19]. The Directive places an obligation on member states to ratify national laws so implementing the requirements of The Directive. The Directive defines a set of rights concerning personal data accruing to individuals and rules of lawful processing on the part of processors applicable irrespective of sector of application. The implicit principles and constructs of The Directive, once applied interdependently, populate the enforcement and representation of privacy. Such activities are termed data protection. While privacy is a concept whose definition may range from complete

anonymity to control over one's data, it is on the such grounds we occasionally use the terms data protection and privacy interchangeably, as privacy rights and pursuant responsibilities are set under the auspices of The Directive. Further, while one recognizes that privacy may be viewed from both legal and control (behavioural) perspectives, our focus herein is largely on the former.

To some degree, then, we are taking a two-phased approach of compliance first, and additional value over that investment threshold second. That there is overlap is clear. Gartner G2 (n.d) acknowledges the level of privacy a person seeks varies partly related to the use of ones data (74% of online American adults disagreed that failing dot coms could sell their personal data for instance). That this is analogous to the EU data protection right of defined and controlled purpose specification illustrates one symbiosis of rights and perceived data subject need for control. This symbiosis embodies the connection between legal rules and consumer demand, demand born out of the need for trust, which may imply that data protection capital requirements considered *expenses* by financial controllers are in fact *investments* to which economic returns may justifiably be expected.

The Directive must be implemented effectively in an organization in order to give proper support to the consumer's right to privacy with respect to personal data. One would expect within the EU that organizations would have devised a proper system of general processing measures and procedures that should be present in order to protect company processes in connection with specific protective measures for the processing of personal data. Generally speaking this not the case. Article 17 of The Directive requires data controllers, those accountable for implementing data protection, to adopt 'appropriate technical and organizational measures' to protect personal data. Recital 46, in augmenting the meaning of Article 17, highlights the requirement that these measures should be taken 'both at the time of the design of the processing system and at the time of the processing itself', thus indicating that security cannot simply be bolted onto data systems, but must be built into them. Although this provision mainly concerns data security, it is generally intended as a safeguard against other forms of unlawful processing.

Like the EU, nations such as Norway, Switzerland, Hungary, Hong Kong, Australia and Canada have adopted data protection legislation. In the US, however, the situation is rather different[20]. The US constitution itself does not recognize an individual's right to privacy. The US Supreme Court has ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights (Banisar, 2000, p.229). Although there is a federal privacy law[21] from 1974 (Banisar, 2000, p.230), there is no independent federal privacy commissioner policing its application. The result has been the application of sectoral laws and self-regulation. Although the Federal Trade Commission (who hold no oversight mandate over Banking and Internet backbone operators) promote key concepts such as notice and choice, its enforcement powers are weaker than those of the European data protection authorities. Though it has received thousands of complaints it has issued opinions in only a handful of cases (Kemna, 2001) [22]. Although no official EU decision has been taken to determine the level of protection in the US as being inadequate, it is true to say that the American data protection framework was in itself considered not sufficient by the EU.

In the US, corporate management appear to recognize increasingly that civil law will hold them accountable for failing to meet their fiduciary responsibilities with respect to protecting the information assets of their organizations (Wright, 2001). However, this trend seems to be independent of any significant change in enforcement culture regarding privacy. Rubin and Lenard (2001), in exploring the commercial value of personal information, discuss the need for regulation, typically, from the existence of market failure. In acknowledging (ever-present) asymmetric information as a sole example of market failure, the exemplar of transactions costs required to discover web site privacy policies is given[23].

Because networked commerce facilitates global data transfer, and because The Directive in principle prohibits the processing of EU citizen data in nations whose privacy laws are not as strong as those in the Union, an understanding was required between the EU and US (see for instance Reidenberg, 2001, 717-749). Article 25 of The Directive states the Commission may, after both concluding a country does not offer adequate protection and receiving a mandate from the Council, enter into negotiation with a view to remedy the situation. In 1998, the EU and US commenced negotiation of the 'safe harbor' agreement, to ensure the continued flow of personal data from the EU to the US. US companies would voluntarily self-certify that they fulfill the privacy requirements as stated in the safe harbor agreement. This would lead to the presumption of adequacy and as a consequence it would allow them to continue processing (defined in the broadest sense of the word in The Directive) the personal data of EU citizens. The Commission issued a positive decision regarding safe harbor arrangements on July 26 2000[24]. The effect is that safe harbor signatories become equivalent to European processors in that though signatories still need to establish grounds for legitimate processing under The Directive, they do not need to establish grounds for data transfer[25].

10. The Cultural Juxtaposition of Privacy Engineering

Today there exists a paucity of technical assistance available to firms attempting to implement data protection. Before specifying an approach taken by the PISA Consortium to this situation, we will examine what assistance there is, after examining what underlies this current, predominant and unrealistic situation given the arguments this article has so far made.

Consider the table below, identifying where recourse is sought to deal with the risks that arise in evolving corporate informatics architectures.

	Package Acquisition		**System Selection**		**System**
Build / Integration		**System Operation**			
Risk Identification		Tactical RFP	Risk Assessment	IT Controlling	Tactical
Security Assessment		Key Performance Indicators			
Risk Management		Sourcing	Strategic Risk Assessment		Change
Requests	Change Requests				
Risk Mitigation	Governance	Governance	Governance	Governance	

Table 1: Risks and Recourses in Corporate Structures

What is illustrated here is a cultural *modus operandi*, which may hinder effective implementation of data protection. Because data protection is relevant to external system acquisition, internal system selection, development and integration as well as running operational systems, one is not to be surprised that compliance with data protection is at present most frequently sought through extensions to governance frameworks such as Control Objectives for Information and related Technology (COBIT). This will we feel be especially the case where risk management functions are in operational reality subservient to Audit functions[26]. This is an inappropriate situation where the avoidance of negative reputation requires not the periodic application of an adapted compliance toolkit, but the mandate from the top of an organisation for decisive *ex-ante* action. Clearly, in the context of privacy, risk management has a responsibility directly affecting business viability.

Those risk managers tasked with implementing data protection naturally harbour some propensity to apply what is effectively an inappropriate mindset to the area. That mindset, a product of incumbent skills and experience, is generally convention bounded[27] by security norms. Conceptually, the composition of data protection is associated with but is in fact far richer than that of conventional security and compliance concerns as we illustrate below (adapted from PISA Consortium, 2001).

Relation	**Key**
congruent	
strongly related	
moderately related	
weakly related	
unrelated	

Figure 4: How Data Protection Principles Encapsulate Security and Auditing Convention

Above we illustrate how nine data protection principles traceable to The Directive encapsulate security and auditing convention[28]. Therefore, if vendors and implementers are to comprehensively manage data protection implementation, an educational component from board level down appears necessary to bridge this conceptual disparity.

Such cultural and educational inappropriateness regarding data protection implementation is compounded by the current lack of effective data protection guidance. Clearly the persistence of this situation at time of writing is a root of data protection reputation and liability risk and thus a key enabler of the juxtaposition of exposure and social cost onto the European citizenry[29]. Currently, most available assistance for data protection is policy orientated[30] and this is not particularly helpful in terms of system adaptation to The Directive. Perhaps the two most relevant guidance mechanisms available today are the Privacy Impact Assessment (PIA), and the Privacy Diagnostic Tool (PDT). Both approaches were evaluated by the PISA project in order to assist its implementation of legal requirements.

Flaherty (2000) [31] defines a PIA as follows:

> 'a PIA seeks to set forth, in as much detail as is required to promote necessary understanding, the essential components of any personal information system or any system that contains significant amounts of personal information'.

PIA Guidelines (2001) state that a PIA should be executed when a service proposition requires one to design a new program or service. The PIA is commonly based on the OECD code of fair information practices and its objective is the assurance that all privacy issues have been identified and personal information is being properly protected, frequently in the context of (e-government) service proposals. Executing a PIA is in principle a three-step process commencing with a high-level process flow exhibition of the system of interest - using for instance a Unified Modeling Language Collaboration Diagram. This model can be drilled down for useable granularity through data flow tables for which various parameters can be assigned[32]. Step two involves understanding exposure with questionnaires providing templates for what could be described as challenge and response privacy analysis. Step three takes a documented evaluation of privacy risks as its input, and guides interpretation of the implications, resulting in a mitigation strategy.

The PDT[33] is based on 10 principles consistent with the OECD fair information practices for the management of personal information. Appended to a description of each principle is an instantiation where related objectives may be compromised. A series of questions relating to implementation of a principle are then described. These questions are divided into two categories and alert users to both implementation steps and best practices associated with a principle. Because a yes or no answer is requested by an accompanying software tool, a privacy report is generated computing a gap analysis conclusion, specifying the work an organization has to do to mitigate residual privacy risks. This report also outlines steps needed to be taken for those questions that were answered no or left unanswered.

In considering the PIAs added value for practical assistance to new system architectural planning, we consider the approach to be strong on both organizational and implementation mandates. The PIA is very much a product of a compliance mentality, thus making it accessible for many practitioners. However, the PIA incremental data-then-risk-then-(re) design approach is bereft of method driven system level privacy implementation guidance, which in terms of whiteboard development will lead to sporadic like design decisions and poor repeatability[34]. This, a weak process orientation and apparent limited portability can, we feel, lead to incomplete coverage of Data Protection requirements. It is also worth noting however that these observations imply a PIA is better suited to configuration management data protection application (where roles and processes are mapped back into some effective instantiation of data protection law) than whiteboard application.

Although the PDT was not designed explicitly for new system architectural development, it is conceivable that system developers would use a PDT to help them to assess the privacy 'compliance' of a new system under development with respect to design

documentation. To this end the PDT is an education experience with value, exposing systems people to the 'why' of data protection as an *apéritif* before dealing with the 'how'. However, the central PDT problem is that it leaves too many interpretive questions unanswered when considering design.

From an design perspective, both the PDT and PIA deal with legal granularity (ultimately that is the problem of associating legal code with programming code) through a series of questions, which effectively parameterize principles of legal interest. Relative to the PIA, the PDT does a better job dealing with legal granularity through its implementation guidance. However, what the PDT represents here is essentially the same process as employed by the Australian and Canadian Data Protection Commissioners when assessing Web Seals in 1999 <<http://www.privacy.gov.au/publications/seals.html#416>>. These Commissioners needed a way to measure deltas in conformance to OECD privacy principles from different seals - hence a series of questions were developed to articulate and score conformance. Clearly, this is indicative of compliance / project management thinking which, in combination with an insubstantial methodology, leads in both PIA and PDT cases to a *descriptive* generation of recommendations.

11. DEPRM as Whiteboard Privacy Engineering 2002

The PISA project integrates privacy from two perspectives. First, if all personally data were removed from a system's data subject representation - the limit of traditional definitions of PET - then The Directive no longer applies. Because some personal data will always be processed somewhere in a distributed system, PISA will implement traditional PET system components such as identity protectors. DEPRM supplies a conceptual and organizational platform for such activities. The second PISA privacy integration strategy is the *raison d'être* of DEPRM - driving the delivery of lawfully defined superdistributed rights and responsibilities in distributed object / Multi Agent System (MAS) design - so that we may say in a limited sense PISA is empowered as a Directive 95/46/EC enacting agent[35].

DEPRM is system level, Directive driven guidance from knowledge engineering roots emanating *prescriptive* recommendations. Such an approach will reduce the implementation risk in terms of rigor, compliance and speed of poor execution[36]. DEPRM is intended for whiteboard application[37], carefully positioned within the development lifecycle.

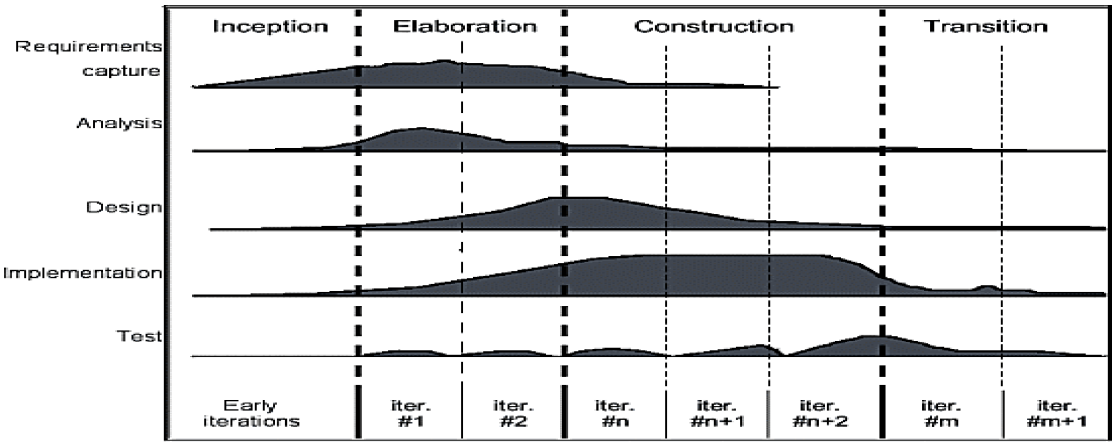

Figure 5: DEPRM Applied in the Elaboration: Construction Phase in the PISA Project

The PISA project has developed and applied DEPRM in the elaboration : construction phase depicted above. Because a tenant of PET is that requirements capture ends inside the construction phase, the DEPRM process is concluded no later than iteration #n+1, so minimizing re-work. In its application, DEPRM has been designed to demonstrate such critical success factors as a manageable overhead, repeatability and of course high utility for system building. Such attributes dovetail with the spirit of Recital 46 and Article 17 from The Directive, and Recital 14 from Directive 00/31/EC[38].

DEPRM distills legal knowledge engineering into a risk management carapace as illustrated below. Gray boxes refer to the process of knowledge engineering, purple boxes refer to the process of risk assessment and the blue boxes refer to the risk mitigation.

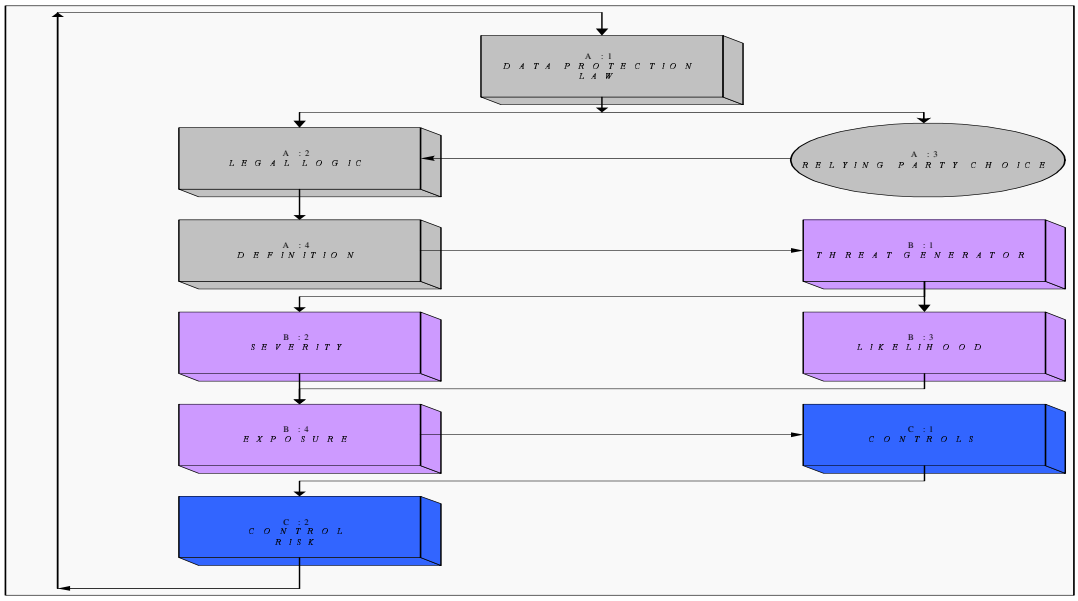

Figure 6: DEPRM Distills Legal Knowledge Engineering into a Risk Management Carapace.

The DEPRM philosophy is instantiated into a suite of mutually supportive modules, which in combination aim to ensure implementation of The Directive, effective in business and compliance terms. The DEPRM - management module is a control self assessment based module, necessary to establish the DEPRM implementation prerogative. Formal specification for terms of reference, reporting responsibilities, relationship and accountability structures as required by privacy engineering may piggyback pre-existing processes as found in IT Risk Management for instance. The DEPRM - co-ordination module tracks commitment, milestone and management reporting for specific activities, enforces system integration and would act as the platform for business value seeking initiatives.

The DEPRM - system module assumes that deployment environments are clean. DEPRM is applied to system design through modeling extensions to collations of functional requirements. Database dependencies are also relevant here with partial responsibilities for data subject identification, data structures, audit trails, data security and data manipulation. In the PISA project this module is focused on agent environmental design. The DEPRM - security module considers security and lawfulness of processing from the explicit requirement of Article 17 in The Directive. This module is an extension to basic security architecture work. The DEPRM - interface module relates interface engineering to the aspects of the Directive that require visual expression - and doing so in a manner which conveys implicit trust[39] to the data subject.

DEPRM - control risk module as the concluding module provides the development team with a structure to evaluate the effectiveness of design decisions through a process of creative problem solving and threat modeling. This results in design patches so improving the robustness of design decisions, and revisions. All modules may therefore be considered as extensions to generic processes influencing most development environments.

12. Legal Knowledge Engineering

The Directive itself is deemed too abstract to directly generate technical specifications. Abstraction equates to the degree of interpretation one may apply to a legal specification. Interpretation capacity leads to primary design risk. National implementations of The Directive reduce abstraction and interpretation. They, like The Directive, are conceptual frameworks, but also possess explicit implementation structures, which collectively reduce complexity. National enforcement tools such as Spanish Regulation 994 derived from national implementations reduce granularity further. Reduced interpretation capacity reduces specification risk.

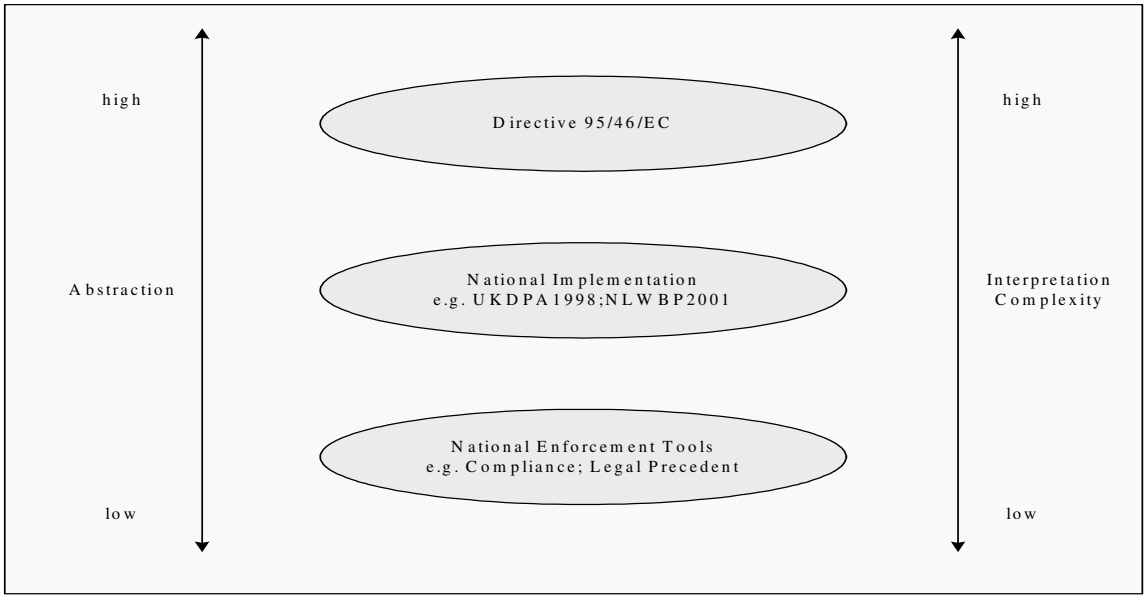

Figure 7: How A Conceptual Framework Such as The Directive Can Reduce Abstraction and Interpretation.

The solution is therefore to work with a simplification of data protection, while retaining the capacity to integrate more interpretative aspects of law as they would be applied when assessing a scenario. A simplification of the law is applied through the concatenation of select Directive Articles into what may be termed principles. Various intermediate implementation tools construct these principles, such as the Dutch privacy Audit (Leerintveld and van Blarkom, 2000, pp.32-50).

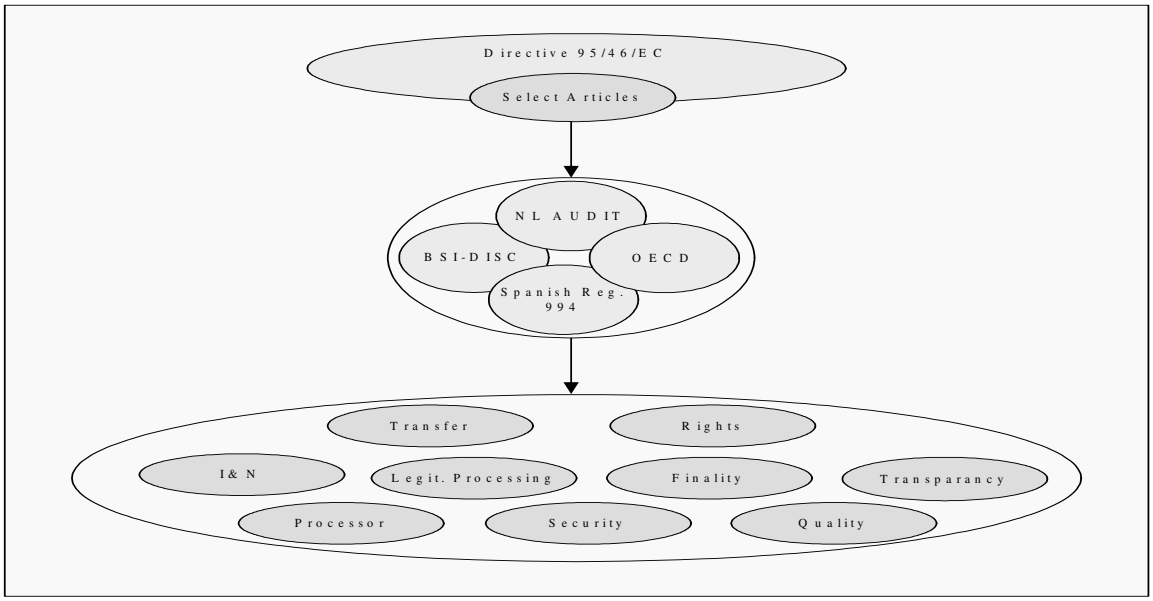

Figure 8: Concatenation of Select Directive Articles into Principles

We are now at the principle level. Let us take the example of the principle of Transparency, which may broadly be defined as: The data subject must be informed about what is done with her personal data. Such a principle is considered in anatomical terms

emphasizing context and goal orientation. Subdivisions are made which possess orthogonality and regularity. Each subdivision is attached a numerical identifier, nesting as appropriate, affording documentation and controlling benefits, plus eases modeling work item interdependence. We term each subdivision a work item.

We have now effectively found the limit of a knowledge engineering approach to generating technical requirements from the law, as one may consider in a systems thinking sense non-concatenated residual Articles to supply the framework legal professionals apply when considering the parameters of a particular scenario. We have now also reached the final possible level of granularity applicable to any kind of system. It is also the most elementary rendering possible for a 'specification' of The Directive. This holds as system characteristics differ sufficiently, hence it is not possible to define an intermediate conceptual framework in application-type-independent terms. The conceptual instantiation we discuss from this point on is therefore MAS specific[40].

13. Conceptual Instantiation

The DEPRM co-ordination module holds a repository of work items, which possess either discipline characteristics or design - contextual implications. Discipline characteristics relate to what are the three fundamental areas of computational data protection expression - logic, security and interface engineering[41]. Design contextual implications are what the work item 'communicates' to the designer in terms of system architecture - perhaps the need to consider superdistributed cryptographically protected audit logging mechanisms so ensuring accountability in a service liability driven scenario for instance. This is a counterbalancing realisation of an ethical governance culture: the software industry is of course pushing for service liability application to new business models - such a realisation eases the burden of proof on the victim of a data protection infringement, as well as potentially generating goodwill. Such reasoning, often through analogy, in both discipline characteristics and design-contextual implications, simultaneously accounts for the general semantics of the work item's parent principle and application specific knowledge, which in the PISA case is agent technology.

In terms of logic, the first step is to find the ontology for a principle as a reflection of its child work items. Such an ontology can be used to output a Resource Description Framework Schema (RDFs)[42]. This result is a simplified intermediate conceptual model of a principle with respect to the application area at hand - MAS behaviour in the PISA case. This may then be imported into PISA agents and used as a backbone in conversations regarding static principle issues[43]. However, to be in a position to model a architecture realistically reflective of our simplified legal model, the logic implicit in certain work items needs to be described in a format understood by our application type - agent technology. We may therefore use the ontological output noted as the representational basis of legal logic formulation. In essence, we are upgrading our simple ontological instantiation of The Directive with a *knowledge base*. For instance:
Work Item: 2.1.1.2: If personal data (PII)and/or purpose specification sensitivity is medium or high then my agent requests: APS from interacting agent

This rule modeled in Protégé Axiom Language (PAL) may be formulated as:

```
(defrange pii_exch :FRAME PIIExchange)  (defrange aps :FRAME APS) (defset
  Is_sensible :STRING High Medium)  (forall ?pii_exch (=> (element_of (level (sensitivity
  (pii ?pii_exch))) Is_sensible)              (exists ?aps (aps (processor (sender ?pii_exch))) ?
  aps)))
```

Figure 9: Work Item: 2.1.1.2, modeled in Protégé Axiom Language (PAL)

which in turn may output:

```
<a:_pal_constraint rdf:about='andTransparency;Transparency_00036'  a:_pal_name=
  'Has_Sender_A_Policy'  rdfs:label='Has_Sender_A_Policy'>  <a:_pal_range>(defrange
  pii_exch :FRAME PIIExchange)  (defrange aps :FRAME APS) (defset Is_sensible
  :STRING High Medium)</a:_pal_range>  <a:_pal_statement>(forall ?pii_exch (=>
  (element_of (level (sensitivity (pii ?pii_exch))) Is_sensible)              (exists ?aps (aps
  (processor (sender ?pii_exch))) ?aps)))</a:_pal_statement> </a:_pal_constraint>
```

Figure 10: Output of Work Item: 2.1.1.2, modeled in Protégé Axiom Language (PAL)

The collective result is design input for our content framework of communicative acts and triggers for what we have termed data protection protocols in agent technology. All rule output is used as input to produce and interpret queries between MAS components and to the general transfer rule. The general transfer rule is the decision an agent representing the data subjects' controller makes to agree personal data transfer to another agent acting as a processor, or to another agent under the same controller but where purpose specification differs sufficiently.

We are now in a position to consider design contextual decisions. From a broad definition of the principle of Transparency being - the data subject must be informed about what is done with her personal data - one is now in a position to abstract an implementation scenario in the application for a holistically considered principle. An attractive solution for this in the PISA case can be a 'monitor agent'. In a given implementation scenario, every time personal data is transacted between two agents of different controllers, the monitor agent would be informed of the data exchange. The monitor agent keeps a log of all information exchanges together with the receiving Controller Identity and Purpose Specification. The data subject can exercise her access rights through consulting the monitor agent whenever she wishes, and the monitor agent can dynamically inform her when it considers appropriate.

In terms of security let us consider a work item we identify as 2.1.2.1: The data subject shall be informed of the Identity of each Controller to whom personal data is sent and the Purpose Specification for which the information is sent to this Controller. We are considering here the agent representation of the data subject in the context of controller or processor interaction. The controllers or processors may be represented by other agents or interfaces on the same untrusted platform, or remotely located. Our fist task is therefore to consider in discipline characteristic terms which security characteristics are implicated by this work item. Clearly, security attributes here relate to the presentment of Controller

Identity and Purpose Specification as credentials. As such the attributes of authentication and integrity are implicated.

Authentication in PISA uses the asymmetric crypto of a Globalsign Public Key Infrastructure, with each actor owning a certificate signed by our trusted third party. Conventionally, one or both entities must authenticate each other, hence one or both certificates are exchanged - if the authentication has been successful a communication session is started. As the X.509 extension mechanism permits a party to send optional data during the authentication protocol, we may send Controller Identity and Purpose Specification with integrity provided by a digital signature.

Below we show the two-pass two-way authentication protocol standardized by X.509 where A sends B one message, and B responds with one message. The result is mutual entity authentication and key transport, with key authentication.

$D_A=(t_A, r_A, B, data_1*, P_B(k_1)*)$
$D_B=(t_B, r_B, A, data_2*, P_A(k_2)*)$
* = optional data

Where parameters $data_1$ and $data_2$ may be used for Controller ID and Purpose Specification[44].

Figure 11: Two-pass Two-way Authentication protocol

Given the design contextual implication of a monitoring agent, the protection of log files collated by this agent on an untrusted platform becomes an important design issue. As the monitoring agent is receiving logging data in an open format, there is a need to protect it against the agent platform at the time of receipt, therefore an operation such as hashing data at the data subject representing agent before it is sent to the monitoring agent is required. Because the agent platform delivers resources, it is the element executing encryption algorithms. Therefore the issue becomes how to provide integrity for the encryption algorithm, and more generally, the provision of integrity for function execution. This design question can be addressed in three phases; first through function execution where integrity of data is provided (e.g. if the function is a signing function and the data is a private key); second extending this into general data and general functions and third finding the integrity of the function.

In terms of interface engineering discipline characteristics, there in an obvious correlation between the construct of feedback, which has been empirically established as being conductive to trust (Norman, 1997), and the Transparency principle which may broadly

be defined as the data subject being informed about what is done with her personal data. There is hence a need to illustrate transparent processing throughout the MAS. This realization leads to system requirements for the user interface being embellished and formalized into a set of interface functional descriptions, demonstrating properties such as visible affordance (Norman, 1990), which means that the function of an interface component should be clear from its visible appearance.

Further, consider work item 2.1.1.1: before the data are collected, the data subject is informed of: Identity of controller and Purpose Specification for which the data are intended. What is documented here, in terms of applied cognitive science, is a content requirement of the interface environment which describes two data elements which should be provided to users in a manner conveying relevant human factor tools. For instance using pastel colours with symmetrical page layouts - prior to any information being requested from the data subject. Also note the implied temporal sequencing of visual cues from the work item, which can be modeled by a Unified Modeling Language sequential substate diagram[45].

The design-contextual implication, given the scenario of a monitoring agent as a visual representation of transparent processing, is an interface functional description supplying this powerful construct, reporting transparency from multiple use cases as we embellish below.

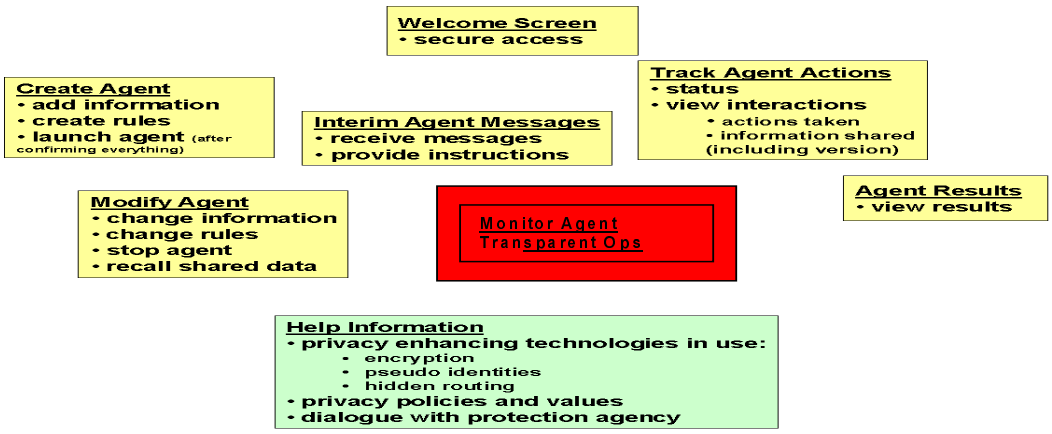

Figure 12: Funtional Interface

Finally, systems integration fuses discipline characteristics and design contextual decisions together as a roadmap for design. Trade-offs here likely revolve around maximizing what can be enforced against that which must be detected - through technology. For instance, using a mirrored audit trail as an agent credential, so indicating correct past use of data subject data.

14. Summary and Conclusion

The description given in this section has described how knowledge engineering has related a simplified subset of The Directive's requirements for an agent system in terms of three scientific disciplines. In terms of development effort, it is important to consider

the juxtaposition of risk management thinking into the design : elaboration - construction phases of a project development, and this may be practically achieved using a conceptual approach such as the generation of libraries of Schneier's Attack Trees (Schneier, 2000) - an effective control risk tool for self administration. What may be assessed here are both conventional security risks such as those to confidentiality, and threats to the privacy *rights* of the data subject, as they relate to design decisions.

This paper has emphasised that privacy and data protection can form the basis of an ethical corporate strategy to which revenues are attributable. We have introduced the notion of privacy engineering to implement this realisation, and demonstrated a dedicated approach to interjecting data protection requirements into a complex system development. Clearly, as knowledge advances, an implication of this research is that significant computational codification of legal doctrine is expected within the next 10 years. The conduits of this development clearly will be the semantic web and dispute resolution solutions. Such implications governments, society and commerce will do well to increase their awareness of.

Notes and References

1. Most service providers are small scale and policy orientated. Pricewaterhouse Coopers has perhaps the most formalized privacy practice of the 'big 4' at time of writing.

2. For instance, Microsft in 2001 was fined by the Spanish Data Protection Authority over employee data transfers (see <<http://www.ihrim.org/about/commit/privacy/updates/apr01.cfm>>) for a relatively small financial sum compared to cases of competition policy has failed (see <<http://www.lawexchange.org/news/papers/new_comp_law.htm>>). Though this paper does not explicitly compare for instance the *second* order financial repercussions attributable to loss of reputation from anti-competitive behavior verses data protection violation - the value of reputation is discussed.

3. The ability to execute perception, in a statistically constrained optimization, is discussed by Kenny and April, 2002.

4. Reputation also exhibits an interesting self-enforcing characteristic. Standifird (8) notes that because reputation is ultimately established by party's external to the firm, an organization with a positive reputation is inclined to persist acting reputably because loss associated with a damaged reputation is augmented by the limited effectiveness with which that reputation may be repaired. It is also interesting to consider

5. It is not the intention of this article to deconstruct the characteristics of perceived trust - clearly a human factor area grounded in cognitive science, leveraged through an interface-engineering carapace. This is the direction one needs to pursue to answer intrapsychic questions such as what is consumer trust, who builds it, where does it feed from and what kills it?

6. The Dutch Data Protection Authority is developing a certificate for privacy auditing:

see <<http://www.cbpweb.nl/>>.

7. Milton Friedman, founder of the Monetarist school of economic thought.

8. A Double Click case is illustrative. Double Click set off widespread public outrage when it began attaching personal information from a marketing firm it purchased to the estimated 100 million previously anonymous profiles it had collected (see Banisar, 2000, p.233). Lotus Marketplace, jointly developed with Equifax contained profiles of 120 million people in the United States stored on a CD-ROM. As soon as this product was announced privacy advocates were up in the arms. The New York Times, The Boston Globe among others voiced the same opinion: it was a threat to personal privacy. Thirty thousand telephone calls and thousands of letters of complaint resulted in canceling the product in which many millions of dollars had been invested (see Rothfeder, 1992). Yet another example is negative publicity Intel endured for the unique numerical identities embellished in individual Pentium processors (McCullagh, 2000).

9. In the Henningen v. Bloomfield Motors Inc. case the New Jersey Supreme Court in 1960 said '…the burden of losses consequent upon use of defective articles is borne by those who are in a position to either control the danger or make an equitable distribution of the losses when they do occur.' Risks may lead to liability and information systems (seeWesterdijk, 1995).

10. For instance, the average cost increment of finding and retrieving misfiled paper documents in a Swiss Bank was around 50CHF in 1999.

11. For a radical departure from capital budgeting convention, see the Value Planning model demonstrated by Kenny and April 2002..

12. Exchange, auction and Peer-to-Peer (P2P) business models do not fit such a generalization especially well.

13. Other categories, depending on business model, could be fulfillment, customer / supplier collaborative and content management.

14. See Borking, 2001 # 5 p. 6-7. There are seven design principles in order to realize PET proof information systems: the use of 1. fewer bits, 2. functional authorization, 3. less identifying data i.e. incomplete ZIP codes etc., 4. pseudo-identities, 5. encryption, 6. encrypted biometrics, 7. logging in order to detect unlawful processing of personal data.

15. Interested readers on this regulation are referred to: *Nothing Sacred: The Politics of Privacy* <<http://www.publicintegrity.org/nothing_sacred.html>>.

16. Finally, its useful to add a little analytical sophistication to the resultant data - see for instance Johnson, 1999.

17. Besides informational privacy, one can discern bodily, territorial and communicational privacy.

18. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281 , 23/11/1995 p. 0031 - 0050.*

19. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal L 024 , 30/01/1998 p. 0001 - 0008*.

20. The scope of this section is to generally highlight the contrasting approaches to data privacy held by European and American policy makers, not to examine the underlying logic of the American approach nor consider at depth comparisions with the European perspective. Readers interested in approaching the issue at greater depth are recommended to consult Charlesworth, 2000, 253 - 274 and Schwartz and Reidenberg, 1996.

21. This is considered to have a narrow interpretation compared to The Directive.

22. It is also true to say that the FTC has also become more proactive over time. Readers interested in considering a potential symbiosis of transatlantic policy in data protection are referred to Shaffer, 2000, 1-88.

23. Without contradicting earlier argumentation of this paper, it is worth questioning assumptions such reasoning makes regarding the effectiveness of self-regulation, where no explicit profit incentive exists to act in accordance with expressed consumer wishes regarding their personal data.

24. It is not the intension of this article to consider in depth an analysis of safe harbor. It is worth noting however the limited number of US companies that have implemented it. Further, concerns persist regarding the lack of US government deterrents if a firm breaches the requirements for data subject rights - notably the right of access.

25. A firm may become a Safe Harbor signatory if appointed by the FTC or the safe harbor panel. Online businesses may also be accepted on the basis of control self-assessment driven approaches such as those offered by BetterWeb etc.

26. Based on experience with risk management in the Swiss banking sector, we are convinced of the value found in risk managers setting their agendas independently or in collaboration with, as opposed to in deference to, group level internal audit.

27. Through education this need not be a case of the late Herbert Simons' Bounded Rationality! See Simon, H. *Sciences of the Artificial*. 3rd ed. Cambridge, MA : The MIT Press (1996).

28. This is not to imply in any way that security concepts are non-relevant for data protection implementation, only to impress the point that security is only one of many Articles referenced in The Directive. Perhaps the most comparable piece of American

legislation to The Directive in terms of processor requirements and subject rights is the Health Insurance Portability and Accountability Act (HIPPA), regulating the treatment of hospital patient records. Digital signatures should prove invaluable for requirements such as the chain of trust in HIPPA - which requires that patient information shared with partners maintain the same level of security they enjoyed with the initial responsible party. The same, quite fundamental, security rule is also required by The Directive.

29. See <<http://www.cenorm.be/isss/Projects/DataProtection/IPSE/IPSE-DOC2.pdf>>.

30. As an exception, BSI DISC in co-operation with the Information Commissioner in the UK has produced a set of guidelines. Though an incisive step by those concerned, and an occasionally insightful presentation of analysis, these guidelines are typically weak on methodology. 0012-4: 2000 for instance recommends DBMS' are considered in terms of risks from data protection without offering a methodology repeatable through technological advancements such as the shift from relational to object orientated DBMS'.

31. Flaherty writes 'Ultimately, a privacy impact assessment is a risk assessment tool for decision-makers that can address not only the legal, but also the moral and ethical, issues posed by whatever is being proposed'.

32. Illustrating how and by whom personal information will be collected, used, disclosed and retained, for instance.

33. Privacy Diagnostic Tool Workbook version 1.0. Developed by The Office of the Information Commissioner Ontario (<<http://www.ipc.on.ca/>>) in collaboration with PricewaterhouseCoopers Canada.

34. It has also been mentioned that the actual implementation of a PIA is quite arduous, and to date few successful implementations have been documented.

35. Indeed, this has two advantages over the first standpoint - traditional PET definitions are limiting with respect to the practical distribution of data subject control, and provoking to law enforcement with respect to social control.

36. DEPRM was for the first time presented by Steve Kenny at the IPSE (Initiative on Privacy standardization in Europe) open meeting on 27 September 2001 in Paris organized by CEN/ISSS. See Final report p.67 Recommendation 1.

37. As opposed to the re-design of systems currently in operation, testing, implementation or configuration management - all of which may currently or potentially be exposing their controllers to risk. Clearly this is a more significant issue for society in the medium term. Though the subject of another paper, the best forward here at this is to adapt a tool such as the PIA to the situation at hand.

38. In that the PISA project demonstrator is an e-commerce application, the e-commerce Directive 00/31/EC identifies its implementation to be in necessary collaboration with The Directive where personal data is processed.

39. Explicit trust in human factor terms then refers to the tangible security infrastructure in operation.

40. We would expect that experiences in multiple application environments would identify classes of intermediate level legal application granularity that were, however, universally applicable.

41. Noting that this instantiation is MAS specific, it is our opinion that these three disciplines supply the 'guts' of an application independent data protection driven initiative - be it whiteboard or configuration management.

42. The ontology - knowledge base modeler used in the PISA project is Protégé 2000. See: <<http://protege.stanford.edu/index.shtml>>.

43. All ontologies related to The Directive are to be submitted to the Foundation for Intelligent Physical Agents (FIPA) standards initaitve for approval and feedback. See: <<http://www.fipa.org/activities/lausanne2002.html>>.

44.

t_A	Timestamp obtained by A
t_B	Timestamp obtained by B
cert	Certificate
k	Symmetric key/ session key
$P_B(k)$	Encryption of k using B's public key
$S_A(x)$	Signature on *x* using A's private key
r_A, r_B	Never re-used numbers, random numbers

45. And implemented through a WYSIWYG (What You See Is What You Get) editor such as Dreamweaver, adding JScript as appropriate.

Bibliography

Barney,J, and Hansen, M (1994), *Trustworthiness as a Source of Competitive Advantage,* Strategic Management Journal, 1994, 15.

Banisar D (2000), *Privacy and Human Rights* ,Washington/London.

Borking, J (2001), *PET, het privacyprobleem structureel opgelost,* in Infromatiebeveiliging 2001 # 5 p. 23.

Borking, J and Raab, C (2001), *Laws, PETs and Other Technologies for Privacy Protection,* Refereed Article, *The Journal of Information, Law and Technology* (JILT) 2001 (1). <<http://elj.warwick.ac.uk/jilt/01-1/borking.html>> .

Centre for Public Integrity (1998), *Nothing Sacred: The Politics of Privacy*

<<http://www.publicintegrity.org/nothing_sacred.html>>.

Charlesworth, A (2000), *Clash of the Data Titans: US and EU Data Privacy Regulation,* European Public Law, 2000 (6), ISSN: 1354-3725.

Deck, M (1999), Managing Ethical Risk in Financial Services <http://www.pwcglobal.com/extweb/indissue.nsf/2e7e9636c6b92859852565e00073d2fd/84252b8fac16f7e28525682b00734205/$FILE/merf1199.pdf>.

Dutch Data Protection Authority (2002) A Certificate for Privacy Auditing <<http://www.cbpweb.nl/>>.

Flaherty, D (2000), *Privacy Impact Assessments: An Essential Tool for Data Protection,* In Privacy Law and Policy Reporter (PLPR), October 2000, Vol 7, No.5.

Gartner G2 (RPT - 0102-0001).

Hes, R and Borking, J (1998), *Privacy Enhancing Technologies: The Path to Anonymity*, Revised Edition, The Hague, Registratiekamer.

Johnson, H (1999), *Making Capital Budgeting Decisions*, Financial Times 1999.

Kaplan, R and Norton, D (1996), *The Balanced Scorecard*, Harvard Business School Press.

Kemna, A (2001), *Privacy verdient ook na 11 September bescherming,* in De Volkskrant, 2 October 2001.

Kenny, S and April, K (2002), *Bottom Line Knowledge Management,* Butterworth-Henderson, New York.

Leerintveld,P and van Blarkom,G (2000), Registratiekamer, WBP Raamwerk Privacy Audit. The Hague, Samenwerkingsverband Audit Aanpak.

McCullagh, D (2000), ‘’Intel Nixes Chip-Tracking ID <http://www.wired.com/news/politics/0,1283,35950,00.html>, Wired New report, 3:00 a.m. Apr. 27, 2000 PDT.

Nash *et al (2001), PKI: Implementing and Managing E-security,* McGraw-Hill.

Norman, D (1990), *The Design of Everyday Things,* Currency/Doubleday.

Norman, D (1997), *How Might People Interact with Agents,* .in Bradshaw, J (ed). *Software Agent,* Menlo Park, CA and Cambridge, MA, AAAI Press/The MIT Press <<http://www.jnd.org/dn.mss/agents.html>>.

The Office of the Information Commissioner Ontario, Privacy Diagnostic Tool

Workbook version 1.0, developed by the Office of the Information Commissioner Ontario (<<http://www.ipc.on.ca/>>) in collaboration with PricewaterhouseCoopers Canada.

Perri, 6 (2001), *Can we Become Persuaded to be PET Lovers?.* Paper given at OECD Session on Privacy Enhancing Technologies, Paris 8 October 2001.

PIA Guidelines (2001), Draft Version 3.0. Page 3, *Privacy Impact Assessment Policy*, of 22 May 2001, Treasury Board, Canadian Federal Government.

PISA - the Privacy Incorporated Software Agent; see <<http://www.cbpweb.nl/bis/top-1-1-9.html>>.

PISA Consortium (2001), *Privacy Threat Analysis* - Work Package #D2.1, The Hague.

Reidenberg, J (2001), *E-commerce and Trans-Atlantic Privacy*, Houston Law Review 2001, 38.

Rothfeder, J (1992), *Privacy for Sale*, New York.

Rubin, P and Lenard, T (2001), *Privacy and the Commercial Use of Personal Information,* Kluwer Academic Publishing.

Schneier, B (2000), *Secrets and Lies: Digital Security in a Networked World,* John Wiley and Sons.

Shaffer, G (2000), *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards*, Yale Journal of International Law, 2000, 25: 1-88.

Simon, H (1996), *Sciences of the Artificial*, 3rd ed,. Cambridge, MA, The MIT Press.

Standifird, S (2001), *Reputation and E-commerce: eBay Auctions and the Asymmetrical Impact of Positive and Negative Ratings,* Journal of Management, 2001, 27.

Standifird, S, Weinstein, M. and Mayer, A (1999), *Establishing Reputation on the Warsaw Stock Exchange: International Brokers as Legitimating Agents,* Chicago, IL: Academy of Management Proceedings.

Schwartz, P and Reidenberg, J (1996), *Data Privacy Law: A Study of United States Data Protection*, New York, Mitchie.

Van Blarkom, G (1998), *Guaranteeing Requirements of Data Protection Legislation in a Hospital Information System with Privacy Enhancing Technology* by The British Journal of Healthcare Computing and Information Management, 1998 (4) Volume 15.

Von Solms, B (2001), *Corporate Governance and Information Security* Computers and Security, 2001, 20.

Westerdijk R J J (1995), *Productaansprakelijkheid voor software*, Deventer.

Wright, M (2001), *Keeping Top Management Focused on Security,* Computer Fraud and Security, p12-14 (2001). (2001