

The Role of Policy and Stakeholder Privacy Values in Requirements Engineering

Annie I. Anton¹, Julia B. Earp², Colin Potts³, Thomas A. Alspaugh¹,

¹ College of Engineering, North Carolina State University, Raleigh, NC 27695-7534

² College of Management, North Carolina State University, Raleigh, NC 27695

³ College of Computing, Georgia Institute of Technology, Atlanta, GA 30332-0280

¹ {taalspau,aianton}@eos.ncsu.edu ² Julia_Earp@ncsu.edu ³ potts@cc.gatech.edu

Abstract

Diverse uses of information technology (IT) in organizations affect privacy. Developers of electronic commerce, database management, security mechanisms, telecommunication and collaborative systems should be aware of these effects and acknowledge the need for early privacy planning during the requirements definition activity. Public concerns about the collection of personal information by consumer-based web-sites have led most organizations running such sites to establish and publish a privacy policy. However, these policies often fail to align with prevalent societal values on one hand and the operational functioning of web-based applications on the other. Assuming that such misalignments stem from imperfect appreciation of consequences and not an intent to deceive, we discuss concepts, tools and techniques to help requirements engineers and IT policy makers bring policies and system requirements into better alignment. Our objective is to encourage RE researchers and practitioners to adopt a more holistic view of application and system specification, in which a system or application is seen as an engine of policy enforcement and values attainment.

1. Introduction

Consumers are increasingly concerned about invasions to their privacy due to the prevalence of data collection and targeted marketing via various web-enabled information technology (IT) in arenas such as electronic commerce (e-commerce) and electronic mail. New information appliances are increasingly merging communication features with computing and commerce. As a result, societal values, such as those regarding personal privacy, are being challenged and are rapidly changing. The attitudes and concerns of online consumers have been the focus of several recent studies [CRA99, Cul99, EM00, BEP00, FTC98, FTC00, KPM99, SMB96].

Privacy affects consumers or stakeholders in other domains. Consider, for example, the role of a patient's information privacy in the health care industry as explored in a recent study [BEP00]. The study measured privacy perceptions of employees having daily exposure to information processing activities. The findings concluded that employees are torn between their respect for personal privacy and the need, whether imposed by management or through individual thinking, to collect personal information.

Because consumers are a primary factor in growth of online commerce, consumer values that concern online privacy substantially shape the development of requirements and privacy policy. In particular, it is important to align system function with consumer values as far as possible.

Studying the values and perceptions of online consumers in conjunction with a requirements methodology can assist in achieving such an alignment.

A group of distinguished scientists and technologists recently reported that issues of privacy would be one of the top 10 challenges in Information Technology (IT) over the next decade [CER00]. The design of the technologies influencing these changes often leave privacy as something which is considered and addressed as an afterthought [AE01]. Instead, the guarantee and assurance of privacy must be included in the design of information technologies from the onset. Furthermore, policies and regulations must be in place to guide the design of these technologies.

Those of us who can offer a systems engineering perspective must assume more responsibility for aligning systems and their respective policy. In this paper we discuss the need to apply the rigor which requirements engineering principles and best practices offer to privacy policy analysis. From the perspective of system design, software engineers need methods and tools to enable them to design systems that reflect those values pertaining to how we use and protect our personal information. Policy makers need mechanisms to ensure that systems comply with IT policy.

Section 2 provides an overview of the pertinent issues surrounding privacy and privacy policies. In Section 3 we discuss the need to apply principles from requirements engineering to ensure holistic consideration of systems and their respective policies. Section 4 presents an approach for mapping privacy policies onto physical metaphors. Section 5 discusses privacy ontologies and their specification whereas privacy teleologies and their discovery are discussed in Section 6. Finally, in Section 7 we provide a summary and discussion of future work.

2. Background and Rationale

In this section we briefly discuss privacy and privacy policies within the context of challenges facing IT professionals.

2.1 Privacy and Privacy Policies

Clarke describes privacy as the "interest individuals have in sustaining personal space free from interference by other people and organizations" [Cla99]. Privacy is often characterized as a moral or legal right, but cultures differ in their attitudes toward privacy, and legal protections vary greatly among jurisdictions and applications. To allay public concerns, many organizations running e-commerce web sites now publish a privacy policy. A privacy policy is a comprehensive description of a Web site's practices that is located on the site itself and may be easily accessed by visitors [FTC98]. It describes the kinds of information collected by the web site and the way that information is handled, stored, and used.

2.2 Common Policy Problems

Laudable though it is to specify an organization's privacy policies, several common problems with published policies as we discuss below.

2.2.1 Nonconformance to standard

The Organisation for Economic Co-operation and Development (OECD) is an international organization comprised of 30 countries that provides their governments a setting in which to discuss and develop economic and social policy. In 1980, the countries adopted the OECD Privacy Guidelines to help establish legislation [OECD80]. In 1998, the organization revisited the guidelines to assess their appropriateness in electronic environments and concluded that the role of the private sector is to adopt clear privacy policies for disclosure on the Internet [OECD98]. Similarly, in 1998 the Federal Trade Commission (FTC), while promoting self-regulatory efforts of online privacy, published a *Federal Register* Notice requesting that trade associations and industry groups voluntarily submit their online information practice guidelines and principles [FTC98]. The recommendation of the FTC suggests a privacy policy that follows the code for fair information practices [FIP73], which overlaps with the OECD Privacy Guidelines. Although the efforts of the OECD and the FTC are venerable, they are merely suggestions to guide the private sector and legislators. Despite these publicized suggestions, the Georgetown Internet Privacy Policy Survey [Cul99] found that Internet privacy disclosures do not always conform to this standard.

2.2.2 Ambiguity and misplaced trust

Policies are also often ambiguous, difficult to find and interpret. Consumers, understandably, often trust indirect and abbreviated indicators of privacy protection rather than reading the full privacy policy. For example, TRUSTe, an independent, non-profit initiative, leases its policy seal to member companies that adhere to a set of online privacy guidelines. However, this gives most consumers a false sense of security since they do not realize that a web site may display this seal regardless of whether or not a privacy policy truly protects consumer privacy. Often these practices are buried deep in pages of legalese that many consumers cannot digest.

Earp et.al. [EM00] recently conducted a study designed to explore various privacy issues, including the perceived user value of a site privacy policy. Their study revealed that 51% of respondents read a privacy policy on an initial web site visit, regardless of site category or brand status. However, 70% of the respondents reported their level of confidence in a web site increased if a privacy policy was simply available. This contradiction suggests that some Web users maintain the naïve belief that someone else will ensure that a web site respects their consumer privacy. Although there exist privacy protection seals (e.g. TRUSTe) and privacy legislation, these measures do not provide adequate protection for consumer privacy.

2.2.3 Failure to implement

Few e-commerce systems are designed from the outset with privacy in mind. As a result, privacy policies are seldom fully effective either because the organization's own technology does not follow it, or because information "leaks" to other organizations who are under no obligation to follow it. A recent report [GHS00] compared the privacy policies of 21 of the most visited health-related Web sites on the Internet with the sites' practices and concluded that

inconsistencies were common. For example, despite the policies' commitments to patient anonymity, the report cites cases in which personally identifiable information (PII) is vulnerable. Similarly, a recent analysis of 24 e-commerce privacy policies found inconsistencies across a number of site privacy policies and their corresponding systems. This study surfaced the tendency to sometimes misrepresent a system's functionality to those whose personal information is processed and/or stored on those systems [AAE01]. These problems emphasize the need for IT professionals to gain experience in developing proper privacy policies and for practitioners to have access to prescriptive guidance for specifying the corresponding system requirements.

3. The Role of Policy in RE.

Researchers are beginning to recognize the role of RE in policy analysis and formulation. Lichtenstein's framework for developing Internet security policy promotes a four-phase strategy to engineer information security: requirements definition, design, integration, and certification or accreditation [Lic97]. Unfortunately, the framework offers no specific methods to address the requirements definition phase. Similarly, the PFIREs (Policy Framework for Interpreting Risk in e-Commerce Security), developed at the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security), provides a framework for managing information security policy for electronic commerce applications [PFI99]. The PFIREs framework employs a lifecycle model that consists of the following phases: Assessment, Planning, Delivery and Operation. While each phase of the model is marked by specific exit criteria that must be met before proceeding to the next phase, it does include feedback loops that reflect the iterative nature of policy development in e-commerce systems. The framework addresses the need to unify security policies in a manner consistent with organizational electronic commerce objectives. Security policies must be continually reviewed and updated to respond to changes in technology as well as the business environment; the PFIREs lifecycle model supports this iterative process by managing risks as an organization adopts new technologies which may compromise its existing security and/or privacy policies. While the PFIREs planning phase does include a requirements definition step, it does not currently offer systematic prescriptive guidance to the analysts who are actually responsible for translating policy recommendations into requirements. Nor does it provide adequate support for translating policy recommendations into system requirements [PFI99]. Although researchers in the requirements engineering community are beginning to focus on electronic commerce applications [ACD01, AP98, Rob97] there remains a need to apply proven requirements analysis methods (a routine activity in software engineering) and demonstrate how to best apply these methods within the context of establishing policy.

Antón and Earp have introduced strategies for specifying privacy and security policies [AE01, AAE01] that extend the Goal-Based Requirements Analysis Method (GBRAM) of [Ant97] and build upon the PFIREs approach [PFI99] for assessing risk in e-commerce systems. Risk assessment is built into the PFIREs lifecycle and policy changes are classified along a "change continuum"; *tactical changes* involve short-term goal achievement whereas *strategic changes* involve long-term, broad-based initiatives. Our strategy for policy formation [AE01] focuses on goals that

reside along this change continuum. In requirements engineering, “strategic goals” are those that reflect high-level enterprise goals. Since these goals are typically more stable than requirements [Ant97], they are a beneficial source for requirements derivation. Similarly, one can safely assume that strategic goals are more stable, due to their long-term nature, than tactical goals.

3.1. Policies vs. Requirements.

Policies and requirements are similar in some respects, but different in three crucial ways. They are similar in that they both express desire or worth rather than fact. As Hume [Hum1739] famously observed, values and facts occupy irreconcilable domains of discourse: “is” propositions derived from observation and reason can never imply the “ought” propositions of ethics. This distinction is of great practical significance when considering the relationship between policies and requirements. To question whether a policy is just and whether it is feasible given some facts about the world is to ask two types of question. Similarly, when analysts ask their customers whether they really want a system to have a certain feature, or when they ask themselves what are the implications (e.g. for cost or reliability) of including the requirement, they are engaging in two different forms of inquiry. The difference is not one of precision: One can be dogmatic in one’s policies but uncertain in one’s predictions. Nor is it a difference of topic: Both types of question are about the same situations or behaviors. What is different between the two types of question, as Michael Jackson [Jac95, Jac01] has articulated in the case of system requirements, is the mood of the questions. Using the terminology of classical grammar, Jackson refers to questions and statements of fact as being in the *indicative* mood, whereas questions and statements of desire are made in the *optative* mood.

Thus, as a first approximation, we might say that policies and requirements are both primarily statements in the optative mood, because they specify what must or ought to be done. Now we come to the differences between policies and requirements. First, the scope of policies is broader than requirements, including existing and conceivable future requirements within their purview. This is more than a difference in scale: Policies are really meta-requirements, because the subject matter governed by policies is the information management practices that are implemented by system requirements. In this respect, the relationship between a policy and the detailed system requirements that fall within its scope is similar to the relationship that exists in the US Constitution between constitutional provisions and items of legislation. A constitutional challenge amounts to accepting the details of a law as given and asking whether the consequences of applying it would violate the constitution. In other words, the policy remains an optative statement, but now an indicative question is raised about the requirement. Similarly an IT requirement may be challenged on the grounds that it violates a privacy policy.

The analogy between policy observance and constitutionality starts to break down, of course, when we consider who makes “constitutional” challenges in the case of privacy policies and IT requirements, and how such challenges are resolved. Business goals that drive IT requirements may take priority over the high-minded sentiments expressed in a privacy policy. The IT professionals responsible for developing technological assets for an organization and the organizational units that

reap value from these assets may be quite separate from and not answerable to the group that drafted the privacy policy. *Alignment* simply means bringing policy and requirements into agreement and does not necessarily imply the priority of policy. It is for the stakeholders involved (for example, regulatory agencies, industrial associations, management of the enterprise in question, etc.) to decide whether to change the requirements to comply with the policy or vice versa and the grounds on which this decision is to be made.

A second difference between policy and requirements is that policies are inevitably more charged with societal values. This, indeed, is their purpose: Policies exist to fill in the gaps, iron out inconsistencies, and overrule locally desired but globally inappropriate specifics in such a way that broader values are preserved. In contrast to requirements, which express operational goals, policies are expressed more in terms of values to be promoted.

Finally, policies are inevitably more open-ended than requirements. It is tempting to consider a policy and a set of requirements as two sets of rules or optative statements that are subject to formal specification and analysis for consistency. But this is no more practical in the case of quickly evolving IT services than it is in law. Just as “due process” and “States’ rights” defy axiomatic definition, so privacy policies must refer to such nebulous entities as “personal information” or “transaction history”, leaving it to the requirements of specific technologies to refer to specific elements of information and transactions. However, these requirements will usually not make the connection between the terminology appropriate for the specific business function being supported and the more open-ended terms in which the policy must be expressed.

3.2. Goal-Based Specification of Requirements.

In software engineering, practitioners develop and communicate their understanding of existing and envisioned systems by constructing models, such as in object-oriented development [JCJ92, RG92, Wir95]. However, none of these approaches provide direct support for uncovering values. It is not clear how the values afforded by a system are revealed by the objects it contains, the functions it performs, or the synchronization constraints that it obeys. For our purposes, the recent trend toward teleological modeling [AP98] is more promising. Goal and scenario analyses [DvLF93, RGK99, RSB98, vLDM95, VL98] offer methodical and systematic approaches both for formulating policy goals and guaranteeing that a system’s requirements are in compliance with these policies and users’ values.

A teleological model consists of a directed network of goals, in which some goals are sub-goals of higher-level goals [Ant97, AP98, DvLF93]. Also included in a teleological model are the actors who perform goal-achieving tasks, and any obstacles or situational factors that block goals from being achieved [Pot95]. High-level goals represent business objectives or high-level mandates. Lower-level refinements consist of achievement goals that are associated with the performance of tasks either by the system or its users. Goal-driven approaches address why systems are specified and implemented as they are, expressing the rationale and justification for specific features. Focusing on goals, instead of specific requirements, allows analysts to communicate with stakeholders, in terms of their values, using a language based on concepts with which they are both comfortable and familiar. Similar approaches have been adopted in human-computer interaction (HCI) for modeling

user tasks, including task-analytic models for design [HH93], reliability analysis [Kir94], and predictive performance models, such as the GOMS family [SMN83], in which user operations are mapped onto higher level unit-task goals that are ascribed to the user. In business planning, task/goal breakdowns, and the operational definition of goal-achievement conditions have been a standard practice since the 1960's Management-by-Objectives movement [KT76].

What all these modeling approaches share in common is the assumption that the question "whose goals?" is unproblematic. In requirements engineering, the goals for the system are the customer's stated or inferred goals; in human-computer interaction, the goals are the goals ascribed to the rational, motivated, experienced user; and in business planning, the goals are those of the organization. In many situations, however, the reality and determinative role of goals has been questioned. Writers of organizational theory have questioned whether organizations are rational entities to which goals can coherently be ascribed [Mor86]. And critics of the symbolic cognition paradigm have questioned whether actors ever formulate and execute goal-directed plans [Suc90]. While these are reasonable criticisms that have not been taken seriously enough by the research efforts outlined above, we believe that stakeholder disagreements can be incorporated into the goal-based framework simply by admitting multiple sets of goals, indexing each set with the stakeholder that wishes to achieve them. We leave it to the politics of the situation to determine which set of goals (which stakeholder) will prevail.

3.3 Scenario-Based Analysis of Policy and Requirements.

Use cases and scenarios have emerged as prominent analysis tools in requirements engineering, owing to their richness and informality [WPJ98]. During a system's early design stages, designers, users and other stakeholders may not fully appreciate the implications of many proposals. Use cases, introduced by the object-oriented development community (e.g. [JCJ92, Fow97, JCJ92]), describe the possible interactions between external actors and the proposed system. In UML (Unified Modeling Language) [Fow97], use cases and scenarios figure prominently and are represented at multiple levels of detail in several separate notations. Concrete scenarios are essential for developing an understanding of the customer's needs and the operational concept for the system [LPR93], and they provide a rich and expressive representation with which stakeholders can communicate [AP99, Mai98].

Scenarios are also useful in other design and planning disciplines, including human-computer interaction (HCI), organizational process design [AP99], and strategic planning [Hei96, Rin98, Sch91, Wal96]. Scenarios are used in these disciplines to stimulate thinking [JBC98]. In HCI, scenarios aid communication between users and developers about task descriptions, user interface specifications, and prototypes or mockups of interfaces. In organizational planning, they support the analysis of workflow designs. And in strategic planning, they are used to explore the consequences of alternative future circumstances. In this last capacity, scenarios are also used to envisage how technical systems may change as the result of sociotechnical changes [AP98]. Thus, scenarios may be applied at both strategic and tactical (operational) levels, but as we have observed previously

[AMP94], scenario analysis aids in bringing tactical goals into alignment with the organization's strategic goals.

Scenarios describe narrative sequences that can be real (as in incident reconstruction), desired (such as illustrating a satisfactory application of a policy), or imagined but undesirable (such as an illustration of a policy violation that is to be avoided). In software engineering, scenarios are usually developed for the desired cases, as suggested by the term for the more general concept "use case." For dependable systems, however, there has also been recent interest in the representation of "abuse cases" [McD98], that is undesirable scenarios. We therefore distinguish between *use cases*, which are narratives that illustrate actual or designed sequences of satisfactory events; *abuse cases*, in which there is an exogenous intervention that leads to a policy violation (e.g. a security intrusion) or the information user participates in the violation (e.g. by disclosing personal information to a third-party without permission); and *misuse cases*, in which there is some willful undermining of a policy (e.g. by using information for a purpose other than that for which it was gathered). It is misuse cases that most clearly illuminate misalignment between policy and system requirements [Pot01].

3.4. Aligning Privacy Values with Systems and Policy

More often than not, privacy and security policies are developed as an afterthought to a system or not at all, leading to the introduction of evolutionary electronic commerce systems that fail to adequately address consumers' privacy values and concerns. Moreover the relationship between societal values concerning the privacy of PII and the policies and technical mechanisms of IT has been obscured and poorly addressed within the software engineering community. Software engineers have paid very little attention to how values affect the evolution of systems and IT policy. This is due, in part, to the difficulty in applying traditional software requirements engineering techniques to systems in which policy is continually changing due to the need to respond to the rapid introduction of new technologies which compromise those policies.

The first step in aligning IT requirements and privacy policy is to articulate what strategic goals the policies actually support. We are currently engaged in a *goal-mining* exercise. *Goal mining* refers to the extraction of goals from data sources (in this case privacy policies) by the application of goal-based requirements analysis methods [Ant97]. The extracted goals are expressed in structured natural language. 24 e-Commerce Privacy Policies from non-regulated industries have been evaluated thus far. The goal-mining effort yielded over 800 goals. The primary emphasis of this preliminary investigation was not on the kind of goal a particular goal is, but upon that goal's implications as far as privacy protection and invasions are concerned. Goals were later refined into subcategories within a preliminary taxonomy that more closely mirrors the functionality of goals strictly for ease of analysis. The identified goals are useful for analyzing implicit internal conflicts within privacy policies and conflicts with the corresponding web sites and their manner of operation. These goals can be used to reconstruct the implicit requirements met by the privacy policies.

Analysts begin the goal-mining process by first exploring any available information sources such as existing security and privacy policies, or requirements specifications and design documentation, to identify both strategic and

tactical goals. These goals are documented and annotated with auxiliary information including the responsible agents. Goals are then organized according to goal type and in this case keyword and subject. Detailed techniques and heuristics for each of these operations are described in two theses [Ant97, Dem00]. Once goals are identified, they are elaborated; goal elaboration entails analyzing each goal for the purpose of documenting goal obstacles, scenarios, constraints, pre-conditions, post-conditions, questions and rationale. Goal refinement consists of removing synonymous and redundant goals, resolving any inconsistencies that exist within the goal set [Dem00], and operationalizing the goals into a requirements specification.

We broadly classify privacy goals into two categories: privacy protection goals and those that suggest the potential for privacy invasions, where privacy protection and privacy vulnerability goals Jackson's distinction between optative and indicative requirements [Jac95, Jac01, ZJ97]. Privacy protection goals are those related to the *desired* protection of consumer privacy rights; privacy vulnerability goals are those related to *existing* threats to consumer privacy. Privacy protection goals are those which relate to the five Fair Information Practice Principles 1) notice / awareness; 2) choice / consent; 3) access / participation; 4) integrity / security; and 5) enforcement / redress. In contrast, privacy vulnerability goals are those that represent statements of fact that suggest the existence of vulnerabilities for privacy invasions. The privacy goals are eventually operationalized into system requirements and checked for compliance with the respective policies. A full analysis and report of this study is forthcoming; however, a preliminary overview of the optative and indicative privacy goal taxonomy is available in [AAE01].

4. Mapping Privacy Policies onto Physical Metaphors.

Because the documentation of policies serves different functions from the documentation of requirements and is less amenable to precision and closure, we propose different strategies for expressing and representing policies and requirements. For policies, we propose Lakoff and Johnson's perspective from research into the centrality of metaphor in cognitive semantics [LJ99], arguing that privacy policies can be mapped onto several physically grounded metaphors such as containment, force and location. Metaphor is usually regarded as an exceptional and figurative use of language in contrast to the normal use of language to convey meaning literally. There is certainly one area within IT in which such a role for metaphor is well recognized, the user interface, but the "metaphors" there (such as desktops and trash cans) are rather trite and iconic. Lakoff and Johnson argue that figurative language, whether verbal or iconic, is the exception, and that unrecognized metaphors are *fundamental* to our understanding of all abstract concepts and shape how we talk about them. Such ubiquitous metaphors map abstractions onto simple concepts of physical embodiment, such as proximity, spatial location, visibility, etc. For example, even something as basic as the passage of time is mapped onto spatial concepts when we speak of moving "into" the future or putting something "behind" us. And yet, although sometimes we think of the past as spatially behind, we also regard it as "before" (i.e. in plain view in front). These conceptualizations of time are truly metaphorical rather than straightforward isomorphisms from the temporal domain to the spatial precisely because they provide *several* ways of

conceptualizing time that are individually only partly successful. Sometimes we need to think of the past as given and therefore visible and in front, and sometimes we need to think of the passage of time as a forward trajectory into the future, thus placing the past at our backs. It is futile to ask which is the "correct" view: depending on the question you are answering, either one may be adopted.

What this all has to do with IT and privacy is that although information has become an everyday concept it lacks a basic vocabulary being abstract in essence. We claim that it is therefore impossible to reason about privacy (or any other complex value-laden policy domain related to information) without recourse to physical metaphors that color our thinking. It could be argued that an alternative is to develop formal, axiomatic theories of policy that free us from potentially misleading metaphors. Indeed such attempts have a long history in rule systems as legislation, policies and design guidelines including the use of deontic logic [MW93], modal logics [FP86] and speech-act theory [Sea69] to formalize the notions of rights, obligations and commitments. But, in no case is there a model (i.e. a concrete interpretation of the formal theory) that seems able to reflect how we actually talk and think about these concepts. In contrast, Johnson [Joh93] presents a strong case that ethical theories and policy domains can be presented and disputed in terms of such individually incomplete but collectively compelling metaphors as "moral interactions are commodity transactions" or "rights are rights-of-way." It would seem that we can no more do without these metaphors for moral and policy issues than we can stop talking about the past and future as if they were places or spatial directions. Rather than admitting this shamefacedly and nevertheless proposing to adopt an abstract semantic theory for privacy rights and obligations, we take the perspective that metaphor should be placed front and center [*sic.*] and that appropriate physical mappings be used for depicting privacy policies and the related aspects of required system operations.

What might be some examples of privacy metaphors? Here are some suggestions that we are exploring:

Private information is on my land. Information occupies a "space" and the information subject is its legitimate tenant. There is a boundary around the property delimiting PII from innocuous information in the "commons". Disclosure of PII is equivalent to inviting someone into the private space.

Private information is stuff that belongs to me. Information is a substance that can be bought, sold and stolen. When I own it, I have it; when you buy it or steal it, you have it. This metaphor applies to all intellectual property, including trade secrets or copyright-protected works. According to the property metaphor, "if the information belongs to me, I can do what I want with it". Unlike the aforementioned real estate metaphor, where agents move relative to the property, in this property metaphor it is the property itself that changes hands.

Private information is only visible to me. Information can be seen or not depending on how clear the view is from your perspective or whether it is hidden. Information surveillance is like using a telescope or microphone. Firewalls are like heavy curtains. Encryption is a form of camouflage.

Policies are forces. An agreement not to disclose information is a force in competition with other forces. An unfeasible, rescinded or overridden policy has been overcome by a greater force.

As explained earlier we must often adopt multiple metaphors for abstract domains. It is where the metaphors clash or analogies break down that we should look for non-obvious implications that are of interest to the practitioner. For example, hiding a physical object in an opaque container is not the same as rendering it invisible: it is still clear that something is hidden, even though its nature is not accessible, and the opaque object hides objects behind it as well as those in it. If we use this metaphor for information objects, with visibility and viewpoints corresponding to capabilities and rights with respect to the information, what are the analogs of being hidden but still manifestly present, or occluded but not deliberately hidden? Examples of such issues are the use of data mining techniques to identify data subjects even though each data record is anonymous in isolation.

In computing, an ontology is the set of basic categories that are fundamental to developing a description of a system. Problems occur when different systems that are to be integrated or that inter-operate in a wider business context nevertheless have subtly conflicting underlying ontologies. An organization's privacy policy and a jurisdiction's laws might embody different ontologies. For example, the law might treat an identifier as a fundamentally different kind of thing from an arbitrary item of information about the entity that the identifier denotes; whereas the policy might regard identifiers and other PII simply as "personal information." In such a case, a policy that had no way of expressing the distinction would inevitably run afoul of any law that distinguished between unauthorized disclosure of identifiers (e.g. social security numbers) and disclosure of other information that could be used to identify individuals (e.g. credit-card transaction history). Recovering the implied ontology underlying the wording of policies and features is therefore important if we are to be able to identify points of conflict.

5. Privacy Teleologies and their Discovery

A policy states what should be done if the sites in its scope operate as they are expected and promised to do. But sites exist in a more informal and less legalistic context of users' intentions. Intentions are less amenable to formal description than policy in principle. A visitor's intent, viewed as a micro-policy, might be plausibly stated as "buy the cheapest computer that I can find". However, this goal is not only tacit as opposed to documented explicitly, it is also defined only through the moment-by-moment unfolding of interaction at the site, rather than being pre-specified. What people say they value with respect to personal privacy is not necessarily what their actions reveal are their highest priorities online [EM00].

IT Policies and the Privacy Values they Ascribe to Subjects

The first step is to turn policy specifications around and parse them from the point of view of information subjects. Suppose a policy promises not to disclose information to a third-party without the information subject's permission. Explicitly, the policy says what the technology on the site will and will not do in various situations. However, it is also implying something about the information subject: perhaps that the standard visitor to the site values personal sovereignty or veto power over the use of his or her PII. Such an ascription of values to users by policies does not require that the designers of the site's technology or the authors of the policy consciously thought this, and it certainly does

not suggest that the site's technology is constructed to use a teleological model of its users. In fact, the accidental emergence of such ascribed values is what makes the technique of value ascription so powerful: we have a benchmark against which we can compare what users actually say and what they actually do, neither of which are necessarily the same as what the values ascribed to them in a site's policy would predict.

7. Summary and Future Work

The objective of this paper is to encourage RE researchers and practitioners to adopt a more holistic view of the systems they specify and to consider the relationship (and impacts) of policy (be it security or privacy policy), stakeholder values and system requirements. We have argued that requirements and privacy policies should be aligned and that these, in turn, should be aligned with societal values toward policy. Both forms of alignment are important for the effective evolution of IT/e-commerce, because concerns with privacy are consumer-driven. This is a real problem, because as we have reported, many existing e-commerce applications fail to implement the privacy policy stated on the organization's site. Moreover, many consumers misunderstand the policies that are supposed to apply and are complacent about what they really say.

Addressing the alignment problem requires acknowledging that policies are not merely vague, umbrella requirements, but are different in type. Although, both requirements and policies may be reduced to goals, policies cannot generally be formalized at the same level, as discussed in Section 3.1. We have described several ways in which goal-based, scenario-based, and metaphor-based requirements engineering can be extended to address the alignment problem.

References

- [AAE01] T.A. Alspaugh, A.I. Antón, & J.B. Earp. Examining Online Privacy and Policies: User Perceptions vs. System Requirements, submitted to *IEEE International Symposium on Security and Privacy*, 2001.
- [AE01] A.I. Antón & J.B. Earp. Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems. To appear in *Recent Advances in Secure and Private E-Commerce*, Kluwer Academic Publishers, 2001.
- [ACD01] A.I. Antón, R.A. Carter, A. Dagnino, J.H. Dempster, D.F. Siege. Deriving Goals from a Use-Case Based Requirements Specification, To appear in *Requirements Engineering Journal*, Springer-Verlag, May 2001.
- [Ale98] R. Alexander. E-commerce Security: An Alternative Business Model, *Journal of Retail Banking Services*. (20)4, pp. 45-50, 1998.
- [Ant97] A. I. Antón. *Goal Identification and Refinement in the Specification of Software-Based Information Systems*, Ph.D. Dissertation, Georgia Institute of Technology, Atlanta, GA, 1997.
- [AMP94] A.I. Antón, W.M. McCracken & C. Potts. Goal Decomposition and Scenario Analysis in Business Process Reengineering, *Advanced Information System Engineering: 6th International Conference, CAiSE '94*

- Proceedings*, Utrecht, The Netherlands, 6-10 June 1994, pp. 94-104, 1994.
- [AP98] A.I. Antón & C. Potts. The Use of Goals to Surface Requirements for Evolving Systems, *International Conference on Software Engineering (ICSE '98)*, Kyoto, Japan, pp. 157-166, 19-25 April 1998.
- [AP99] A.I. Antón & C. Potts. A Representational Framework for Scenarios of Systems Use, *Requirements Engineering Journal*, Springer-Verlag, 3(3-4), pp. 219-241, 1999.
- [ATW98] R.J. Alberts, A.M. Townsend & M.E. Whitman. The Threat of Long-arm Jurisdiction to Electronic Commerce, *Communications of the ACM*, 41(12), pp. 15-20, December 1998.
- [BEP00] J.D. Baumer, J.B. Earp & F.C. Payton. Privacy of Medical Records: IT Implications of HIPAA. *ACM Computers and Society*, 30(4), pp. 40-47, Dec. 2000.
- [Bor96] N.S. Borenstein. Perils and Pitfalls of Practical Cybercommerce, *Communications of the ACM*, 39(6), pp. 36-44, June 1996.
- [CER00] CERIAS Security Visionary Roundtable Call to Action, CERIAS (Center for Education and Research in Information Assurance and Security) White Paper, Accenture and Purdue University, West Lafayette, IN, http://www.cerias.purdue.edu/events/accenture_cta_1q2001.pdf, December 2000.
- [Cla99] R. Clarke. Internet privacy concerns confirm the case for intervention, *Communications of the ACM*, 42(2), pp. 60-67, February 1999.
- [CRA99] L.F. Cranor, J. Reagle and M.S. Ackerman. Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, *AT&T Labs-Research Technical Report TR 99.4.3*, <http://www.research.att.com/library/trs/TRs/99/99.4/99.43/report.htm>, April 1999.
- [Cul99] M.J. Culnan, *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*. Washington, DC: Georgetown University, The McDonough School of Business, 1999.
- [Dem00] J.H. Dempster. *Inconsistency Identification and Resolution in Goal-Driven Requirements Analysis*. M.S. Thesis, North Carolina State University, 2000.
- [DvLF93] A. Dardenne, A. van Lamsweerde & S. Fickas. Goal-Directed Requirements Acquisition, *Science of Computer Programming*, 201(1-2), pp. 3-150, April 1993.
- [EM00] J.B. Earp & G. Meyer. Internet Consumer Behavior: Privacy and its Impact on Internet Policy, *28th Telecommunications Policy Research Conference*, Sept. 23-25, 2000.
- [EP00] J.B. Earp & F. C. Payton. Information Privacy Concerns Facing Health Care Organizations in the New Millennium, *Submitted to Decision Sciences*, Oct., 2000.
- [Fow97] M. Fowler. *UML Distilled: Applying the Standard Object Modeling Notation*, Addison-Wesley, 1997.
- [FIP73] The Code of Fair Information Practices, U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, http://www.epic.org/privacy/consumer/code_fair_info.html, 1973.
- [FP86] A.C.W. Finkelstein & C. Potts. Building Formal Specifications Using Structured Common Sense, *Proc. 4th Int. Workshop Software Specification and Design*, Monterey, CA, IEEE Comp. Soc. Press, 1987.
- [FTC98] *Privacy Online: A Report to Congress*, <http://www.ftc.gov/reports/privacy3/>, Federal Trade Commission, June 1998.
- [FTC00] *Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress. Federal Trade Commission*, 2000.
- [Ger97] C. Germain. *Summary of the City University Security Survey 1997*, <http://www.city.ac.uk/~eu687/security/summary.html>, 1997.
- [GHS00] J. Goldman, Z. Hudson & R.M. Smith. Privacy Report on the Privacy Policies and Practices of Health Web Sites, Sponsored by the California HealthCare Foundation, Jan. 2000.
- [Hei96] K.v.d. Heijden. *Scenarios: The Art of Strategic Conversation*. Chichester, UK: Wiley, 1996.
- [HH93] D. Hix & H.R. Hartson. *Developing User Interfaces: Ensuring Usability through Product and Process*. New York, NY: Wiley, 1993.
- [Hum1739] David Hume, *A Treatise of Human Nature, Book 3* [See, David F. Norton and Mary J. Norton (eds.): Hume, David, *A Treatise of Human Nature (Oxford Philosophical Texts)*, Oxford: Oxford University Press, 2000.]
- [Jac95] M. Jackson. *Software Requirements and Specifications*. Addison-Wesley, 1995.
- [Jac01] M. Jackson. *Problem Frames: Analyzing and Structuring Software Development Problems*, New York: Addison-Wesley, 2001.
- [JBC98] M. Jarke, X.T. Bui & J.M. Carroll. Scenario Management: An Interdisciplinary Approach, *Requirements Engineering Journal*, Springer Verlag, 3(3-4), pp. 154-173, 1998.
- [JCJ92] I. Jacobson, M. Christerson, P. Jonsson & G. Övergaard. *Object-Oriented Software Engineering: A Use-Case Driven Approach*. Reading, Massachusetts: Addison-Wesley, 1992.
- [Joh93] Mark Johnson, *Moral Imagination: Implications of Cognitive Science for Ethics*. Chicago: Chicago University Press, 1993.
- [Kir94] B. Kirwan. *A Guide to Practical Human Reliability Assessment*. London: Taylor & Francis, 1994.
- [KPM99] C. Kehoe, J. Pitkow and K. Morton. Results of GVU's Tenth World Wide Web User Survey. http://www.gvu.gatech.edu/user/surveys/survey_1998_10/, 1999.
- [KT76] C.H. Kepner and B.B. Tregoe. *The Rational Manager: A Systematic Approach to Problem Solving and Decision*

- Making*, Second ed. Princeton, NJ: Kepner-Tregoe, Inc., 1976.
- [Lic97] S. Lichtenstein. Developing Internet Security Policy for Organizations. *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol 4, p. 350-357, 1997.
- [LJ99] G. Lakoff & M. Johnson, *Philosophy in the Flesh: The Embodied Mind and its Challenge to Western Thought*, New York: Basic Books, 1999.
- [LPR93] M. Lubars, C. Potts & C. Richter. Developing Initial OOA Models. In *Proc. 15th Int'l Conference on Software Engineering*. ACM/IEEE Computer Society Press, 1993.
- [Mai98] N.A.M. Maiden. CREWS-SAVRE: Scenarios for Acquiring and Validating Requirements, *Automated Software Engineering*, vol. 5, pp. 419-446, 1998.
- [McD98] John McDermid and C. Fox. Using Abuse Case Models for Security. *Proc. 15th Annual Computer Security Conference*, 1998.
- [Mor86] G. Morgan, *Images of Organization*: Sage Publications, 1986.
- [MW93] J.-J.Ch. Meyer and R.J. Wieringa. Deontic logic: A concise overview. In J.-J.Ch. Meyer and R.J. Wieringa, editors, *Deontic Logic in Computer Science: Normative System Specification*, pages 3-16. Wiley, 1993.
- [OECD80] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, September, 1980. <http://www.oecd.org/dsti/sti/it/secur/prod/PRIVEN.HTM>.
- [OECD98] *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*, OECD, May 1998. <http://www.oecd.org/dsti/sti/secur/prod/re97-6e.htm>.
- [PFI99] *Policy Framework for Interpreting Risk in eCommerce Security*. CERIAS Technical Report, <http://www.cerias.purdue.edu/techreports/public/PFIRES.pdf>, Purdue University, 1999.
- [Pot95] C. Potts. Using Schematic Scenarios to Understand User Needs. *Symposium on Designing Interactive Systems: Processes, Practices, Methods and Techniques*, Ann Arbor, Michigan, pp. 247-256, August 1995.
- [Pot01] C. Potts. Scenario Noir. *Symposium on Requirements Engineering and Information Security*, Indianapolis, March, 2001 (in press).
- [RG92] K.S. Rubin & A. Goldberg. Object Behavior Analysis. *Communications of the ACM*, 35(9):48-62, September 1992.
- [RGK99] C. Rolland, G. Grosz & R. Kla. Experience with Goal-Scenario Coupling in Requirements Engineering, *IEEE Fourth International Symposium on Requirements Engineering (RE'99)*, University of Limerick, Ireland, pp. 74-81, 7-11 June 1999.
- [Rin98] G. Ringland. *Scenario Planning: Managing for the Future*. Chichester: Wiley, 1998.
- [Rob97] W.N. Robinson. Electronic brokering for assisted contracting of software applets, *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol. 4 , pp. 449-458, 1997.
- [RSB98] C. Rolland, C. Souveyet & C.B. Achour. Guiding Goal Modeling Using Scenarios, *IEEE Transactions on Software Engineering*, 24(12), pp. 1055-1071, December 1998.
- [Sch91] P. Schwartz, *The Art of the Long View*: Doubleday, 1991.
- [Sea69] J.R. Searle. *Speech Acts*. Cambridge, UK: Cambridge University Press, 1969.
- [SMB96] H.J. Smith,, S.J. Milberg and S.J. Burke, Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly*, June 1996, pp. 167-196.
- [SMN83] S. Card, T. Moran & A. Newell. *The Psychology of Human-Computer Interaction*. Hillsdale, NJ: Erlbaum, 1983.
- [Suc90] L. Suchman. *Plans and Situated Action: The Problem of Human-Machine Interaction*. Cambridge, UK: Cambridge University Press, 1990.
- [vLDM95] A. van Lamsweerde, R. Darimont & P. Massonet. Goal-Directed Elaboration of Requirements for a Meeting Scheduler: Problems and Lessons Learnt, *Proc. 2nd International Symposium on Requirements Engineering (RE'95)*, York, UK, pp. 194-203, March 1995.
- [VL98] A. van Lamsweerde & E. Letier. Integrating Obstacles in Goal-Driven Requirements Engineering, *20th International Conference on Software Engineering*, IEEE Computer Society Press, Kyoto, Japan, 1998.
- [Wal96] M. Waltre. *Scenario Analysis: An Approach to Organisational Learning*, Department of Computer and Systems Sciences. Stockholm, Sweden: Stockholm University/Royal Institute of Technology, 1996.
- [Wir95] R. Wirfs-Brock. Designing Objects and their Interactions: A Brief Look at Responsibility-Driven Design, in John M. Carroll (Ed.) *Scenario-Based Design: Envisioning Work and Technology in System Development*, New York: Wiley, 1995.
- [WPJ98] K. Weidenhaupt, K. Pohl, M. Jarke & P. Haumer. Scenarios in System Development: Current Practice. *IEEE Software*, 15(2), pp. 34-35, March 1998.
- [ZJ97] P. Zave & M. Jackson. Four dark corners of requirements engineering. *ACM Transactions on Software Engineering and Methodology* 6(1), pp. 1-30, 1997.