

PRIVACY NEGOTIATIONS AND IMPLICATIONS ON IMPLEMENTATIONS

Prof. L-F Pau, Rotterdam school of management, POB 1738, NL 3000 DR Rotterdam
lpau@rsm.nl

Abstract : This position paper stresses that in practice a wide class of privacy protection cases should result from the individual's declared preferences ,and from a negotiation / service-level-agreement with the privacy intruder .Thus implementations impose on the languages and software environments to support a number of features such as negotiation , traceability , and integration of the same capability in diverse service platforms .

0. POSITION

In very many real life privacy protection scenarios, the individual may want to release private information on a lasting or temporary basis, just because the provisioning of a service or capability in a personalized way so mandates.

Examples: location based services, multimedia-on-demand, medical consulting, personal financial services

In many of these cases furthermore, the individual may get access to more or better information which he/she needs by releasing in parts private information found of value to another information seeking party

Examples: access to information aggregators, customer relationship management (CRM), e-Commerce

In line with economic theory as applied to privacy , the pragmatic way to implement this is by allowing the user to declare his privacy preferences by privacy feature classes, by allowing the user to declare limits he is willing to accept, and to negotiate an eventual mutually beneficial agreements with the information seekers . In case of an agreement, a service level agreement (SLA) is generated and activated. The implementation must satisfy the following requirements: no coding by the user (other than declaring his privacy rules), traceability, integration of the same user-centric privacy management in diverse service platforms, and possibly legal compliance .This speaks for the use of a declarative language with application independent inference capabilities (such as PROLOG) with full IDL.

The key goal of this position is to help finding viable solutions to the security and privacy challenges faced by the current and future collaborative systems and infrastructures.

1. PRIVACY PROCESSES AND NEGOTIATIONS

Most privacy enforcement situations rely on a set of processes which the parties involved must manage (knowing or not about them, having influence on them or not):

- security management processes
- identity management processes
- information protection processes
- knowledge and information value appraisal processes
- negotiation processes
- monitoring for traceability and liabilities

- delegation of authority
- complaint and legal appeals processes

In general, the negotiation processes rely on SLA's established in the context of contracts between multiple parties; these SLA's have high dynamics and exception handling and result in economic or social utility trade-offs.

The key reason is that, in the real world and in most fields, the handling of private information is not just between one individual (or organization) (with/without economic interests) and another individual or organization, because both are entangled into webs of sometimes contradictory obligations and opportunities which must simultaneously be complied with or modified

Different metrics /values and dissemination processes attached to all these SLA's, obligations or opportunities, create breaches in privacy to all or some parties without they even know about such risks.

For business acceptance and compliance the privacy regulations should not be looked upon as just a cost, but as a way to balance information assets, customer satisfaction, customer loyalty, etc.

2. PRIVACY ECONOMICS

Privacy economics is not just about costs of compliance (technology, legal measures, enforcement) but equally importantly about benefits (soft values, economic or social rewards) which together allow an individual to accept or refuse solicitations of access to his/ her private information .As the identification of benefits is highly context and situation dependent, there are almost always:

- identification of the privacy attributes of importance to each party, and a communication process (complete, incomplete) around them
- benefit and cost evaluations according to the attributes; metrics are often indirect, derived, and almost always qualitatively defined
- risk evaluation linked to trust evaluation between the parties
- negotiation , ranging from a one step accept / refuse / opt-out decision , to n-step negotiations with termination rules
- monitoring and escalation processes

Negotiation is key! As each party has preferences, capabilities, and requirements, negotiation algorithms are needed to automate service discovery. The negotiation of an SLA requires much more than simply choosing one SLA out of some offered static policies or SLA templates. Current work, such as P3P, APPEL, WS-Policy, WS-Agreement, WSLA, SLAng is therefore too limited, as it cannot handle negotiations where the value of one attribute is lowered in favor for another attribute.

Examples: the content distribution networks, the insurance industries, real estate/mortgage credits, specific inter-operator transmission services, and some value-added mobile services, have SLA negotiations which take place all the time

3. CONTRACTS vs. PRIVACY SLA's

There are key differences between SLA's and contracts, as well as in the reporting/ decision authority structure permitting deviations from them as well as their execution.

Most SLA's have exceptions from the general terms and conditions set in the contract (either stricter or weaker wrt privacy, liabilities, risks, delays, etc); these exceptions result from a quasi-real time negotiation between the individual (or organization) and the other

parties, taking the individual's privacy preferences and limits explicitly into account.

As a result, not only must SLA consistency be verified, but known processes or procedures must pre-exist their execution (rooted in delegation of authority, overriding or escalation powers).

4. PRIVACY SLA NEGOTIATION LEVELS AND STEPS

The basic steps/layers in a privacy SLA negotiation are (see Figure 1):

- 1. A legal contract (or law /regulation) allows generating SLA templates, and default privacy attributes / metrics with sometimes some explicit bounds
- 2. SLA Negotiation in a specific context and situation:
 - ° Negotiation about specific privacy attributes, and measurement values for contractual as well as specific attributes
 - ° Privacy verification against contract bounds
 - ° Authoring of exceptions and trade-off, with traceability for permissions/authorities
 - ° Negotiation to reach equilibrium decisions, opt-out or escalation
- 3. SLA execution:
 - ° Reformatting of SLA for distribution and execution; no editing
 - ° Recording SLA attribute values for monitoring and compliance once executed

To check the consistency of all the SLA's in place, even for one individual (or organization) is an open research question, but the essential one. There exist approaches akin theorem proving, logic predicates, and information graph properties which can analyze a set of formalized SLA's. In practice, the individual will declare his rules explicitly and want a privacy management client to manage them for him / her across application fields and services.

5. PRIVACY FEATURES AND ATTRIBUTES

The individual will define the coverage of his privacy (e.g. not on some identities and identification data, but on some others; e.g. not on life style characteristics but on assets owned). Attribute values defined on qualitative or quantitative scales, for each class of features, pertaining to a specific information disclosure instance, include:

- 1. copy attribute
- 2. transfer, delete , substitute attribute
- 3. role change attribute (individual has different rules for same feature in different contexts)
- 4. identity attribute and multiple identities
- 5. time preference attribute
- 6. risk attribute
- 7. leaking feature (leakage of data to third parties without SLA)

6. IMPLEMENTATION IMPLICATIONS

- The individual wishing to protect his/her privacy will want to express different stated preferences to be accounted for in different application or service scenarios .Also this individual will want to have only such privacy protection client environment. This

imposes a requirement for the easy and full integration of the same client within a wide range of environments, via at least (ISO) IDL.

- The negotiation algorithms at this stage are not supported in languages such as P3P, and one issue will be the declarative rule-based nature of the user's preferences, combined by the need not to customize the algorithms. This speaks for declarative languages with backtracking and inference, with PROLOG as formalization.
- During a negotiation, or to find out why the privacy protection client released (or did not release) some specific information, the user will mandate traceability on the negotiation outcomes. The traces should lead back to his stated/declared preference rules, so that he features, rules or attributes can be modified.
- It should be noted that the three aspects addressed above are in line with the July 31st, 2006 release of the OMG Service Modelling Language (SML) Workgroup available from <http://serviceml.org/>. They can also be specified and implemented in native (ISO) UML 2.0
- Longer term, the privacy protection client may include third party declarative knowledge, such as applicable laws /regulations /procedures

ACKNOWLEDGMENTS and REFERENCES

This position is in part derived from work within the PRIME project www.prime-project.eu.org, in part from industry and government work.

Pau, L-F (2004a), Privacy management contracts and economics using service level agreements (SLA's), Research report ERIM, Rotterdam school of management, <https://ep.eur.nl/items-by-author?author=Pau%2C+L-F>.

Pau, L-F (2004b), Privacy metrics and boundaries : a first approach, Research report ERIM, Rotterdam school of management, <https://ep.eur.nl/items-by-author?author=Pau%2C+L-F>.

Pau, L-F (2006), Privacy management contracts in communications and content distribution networks using service level agreements (SLA's), IEEE Conference on Electronic commerce, San Francisco

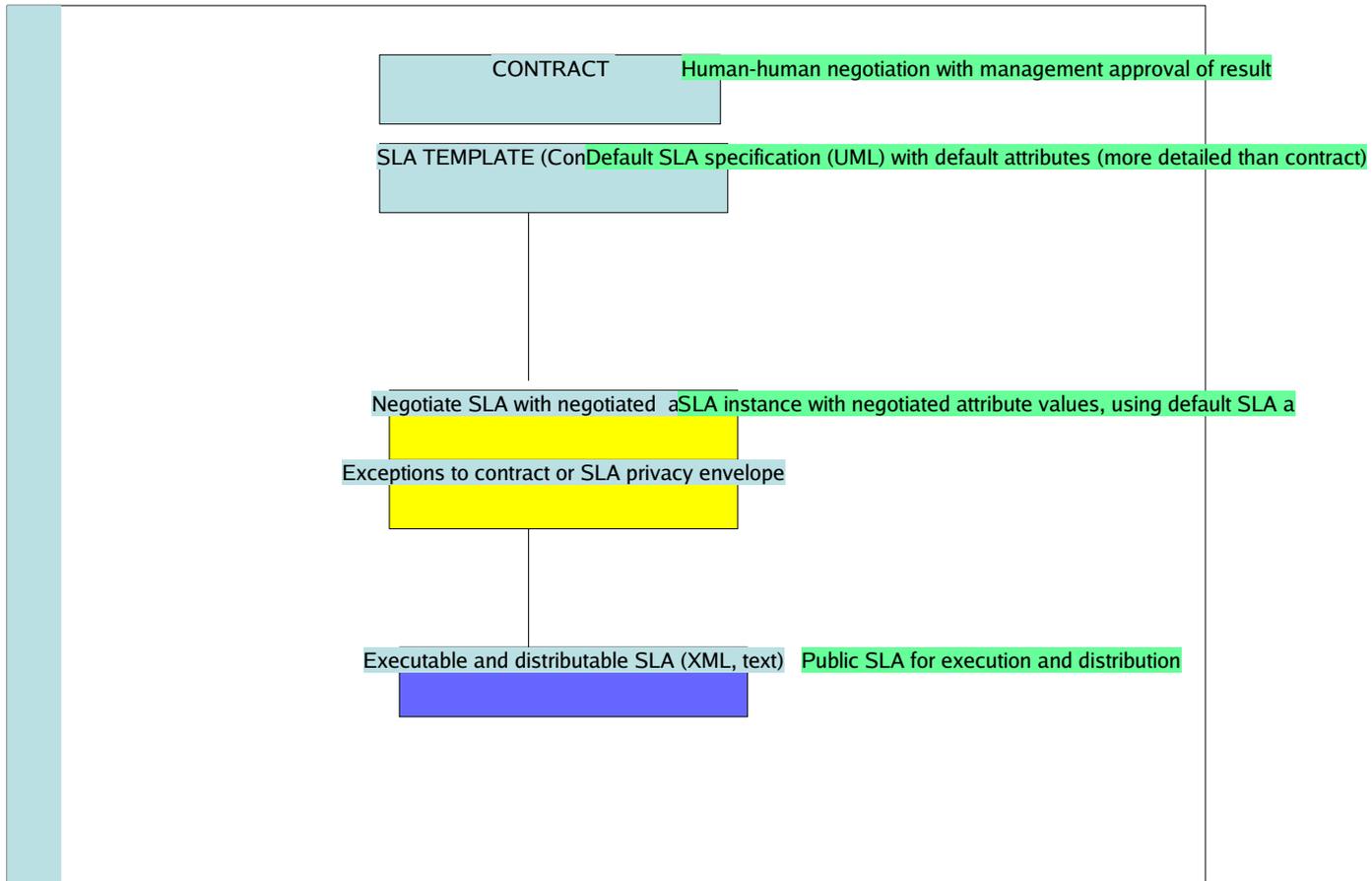


Figure 1: Privacy SLA negotiation layers and steps