# PRIVACY MANAGEMENT CONTRACTS AND ECONOMICS, USING SERVICE LEVEL AGREEMENTS (SLA)

L-F PAU


| ERIM REPORT SERIES *RESEARCH IN MANAGEMENT* | |
|---|---|
| ERIM Report Series reference number | ERS-2005-014-LIS |
| Publication | March 2005 |
| Number of pages | 10 |
| Email address corresponding author | lpau@fbk.eur.nl |
| Address | Erasmus Research Institute of Management (ERIM)<br>Rotterdam School of Management / Rotterdam School of Economics<br>Erasmus Universiteit Rotterdam<br>P.O. Box 1738<br>3000 DR Rotterdam, The Netherlands<br>Phone: +31 10 408 1182<br>Fax: +31 10 408 9640<br>Email: info@erim.eur.nl<br>Internet: www.erim.eur.nl |

Bibliographic data and classifications of all the ERIM reports are also available on the ERIM website: www.erim.eur.nl

ERASMUS RESEARCH INSTITUTE OF MANAGEMENT

REPORT SERIES

*RESEARCH IN MANAGEMENT*

| BIBLIOGRAPHIC DATA AND CLASSIFICATIONS | | |
|---|---|---|
| Abstract | Recognizing the importance of privacy management as a business process and a business support process, this paper proposes the use of service level agreements around privacy features, including qualitative and quantitative ones. It also casts privacy management into a business perspective with benefits and costs to either party in a process. | |
| Library of Congress Classification (LCC) LCC Webpage | Mission: HF 5001-6182 | |
| | Programme: HE 9713+ | |
| | Paper: KF1263.c65 | Privacy |
| Journal of Economic Literature (JEL) JEL Webpage | Mission: M | |
| | Programme : L 63, L 96 | |
| | Paper: K 19 | Basic areas of law: Other |
| Association for Computing Machinery (ACM) ACM Webpage | Programme : | |
| | Paper: K4.1 [Societal aspects] Privacy | |
| | ACM Keywords | Security, Economics |
| Gemeenschappelijke Onderwerpsontsluiting (GOO) | | |
| Classification GOO | Mission: 85.00 | |
| | Programme: 05.42 | |
| | Paper: 86.78 | Informatie- en communicatierecht |
| Keywords GOO | Mission: Bedrijfskunde / Bedrijfseconomie | |
| | Programme: Draadloze Communicatie | |
| | Paper: Privacy, Kwalitatieve methoden, Kwalitatieve methoden, Kwaliteitszorg | |
| Free keywords | Paper: SLA, Service Level Agreement, Privacy Management, Privacy Features | |

# PRIVACY MANAGEMENT CONTRACTS AND ECONOMICS, USING SERVICE LEVEL AGREEMENTS (SLA)

**L-F Pau, Rotterdam School of management, RSM Erasmus University, POBox 1738, NL 3000 DR Rotterdam**

lpau@rsm.nl

## ABSTRACT

Recognizing the importance of privacy management as a business process and a business support process, this paper proposes the use of service level agreements around privacy features, including qualitative and quantitative ones. It also casts privacy management into a business perspective with benefits and costs to either party in a process.

## 1. SCOPE AND INTRODUCTION

Formal Service Level Agreements (SLAs) are increasingly common as a way of ensuring both quality of service (QoS) in information , communication and transport/logistics services , but they are also commonly used to set the commercial and business terms of a service provisioning (e.g. in telecommunications ). They do not replace formal contracts subject to legal review, but allow to reduce the overall number and cost of such formal contracts by making these applicable as framework legal agreements to a diversity of SLA's needed and generated at an operational level, and often subject to dynamic updates.

SLA's can also be defined in areas where QoS as well as business terms must be determined jointly , thus intersecting the main two lines of deployment mentioned above .One such case is on-demand provisioning of content over networks (Internet, wireless) , where obviously the technical content provisioning quality of service attributes can only be matched with QoS dependent tariffs .

The overall issues around privacy, especially in a "Sensor Nation" [1 ] , get increasing attention and the technologies of surveillance even more so ,but it is extremely rare outside the field of privacy and citizen freedom protection legislation, that agreements applying to it are discussed, and even less so when there are costs/benefits of a tangible or intangible nature.

This paper introduced the use of formal SLA's as well to cover the operational dynamic agreements between a privacy protector on one hand, and an information collector on the other hand, as they apply to the provisioning of privacy enhancement technologies PET (or other methods) through which all information exchange between the two parties must take place. At a framework level, a legal framework agreement may exist applicable to all the SLA's between the two parties. What is also essential is that , through its attributes and structure , the SLA's will also include economic and business provisions matching the extent , configuration and efficiency of the PET's ,just as in the case mentioned above in another field . The SLA's may also have to include structural elements to allow a sequence of SLA's between a chain of parties to operate with suitable decision and reporting points.

SLA's generally take the form of:

a) a structured template , which can be specified i.e. in UML
b) one or more specific QoS metrics that are evaluated over a specific time interval to a set of defined objectives. As applied to information systems SLA metrics are often performance-related, such as system availability or transaction response time. SLA metrics are here assumed to be also formulated in terms of higher-level service aspects such as privacy attributes, responsiveness, etc.

This paper discusses techniques for monitoring compliance of SLA's for privacy protection, and displaying results using automated web-based tools.

## 2. THE BUSINESS OF PRIVACY AGREEMENTS: A REVIEW

Economist Robert Hahn gathered data from 17 information-technology consulting firms [2], which said they would charge from $46,000 to $670,000 for a system to track how personal data is handled. "It turns out that's a nontrivial task, as we say in academia," said Mr. Hahn, who heads the Joint Center for Regulatory Studies of the American Enterprise Institute and the Brookings Institution. In total they estimated that Internet privacy rules could cost business as much as $36 Billion (2001), but the business models are also “non-trivial”! The World Wide Web has significantly reduced the costs of obtaining information about individuals, resulting in a widespread perception by consumers that their privacy is being eroded. The conventional wisdom among the technological cognoscenti seems to be that privacy will continue to erode, until it essentially disappears. A study [3] uses a simple economic model to explore this conventional wisdom, under the assumption that there is no government intervention and privacy is left to free-market forces. It finds support for the assertion that, under those conditions, the amount of privacy will decline over time and that privacy will be increasingly expensive to maintain. The study concludes that a market for privacy will emerge, enabling customers to purchase a certain degree of privacy, no matter how easy it becomes for companies to obtain information, but the overall amount of privacy and privacy-based customer utility will continue to erode. In the SICS project “SAITS” on how computational components can acquire and use knowledge about the reliability of other components modeled as agents, consumer agents are only able to observe the external behavior of information gatherers, and the selection can be only be done on the basis of hard facts obtained as part of a trust relation or of an agreement; consumers should also inform peers about their experiences from earlier interactions with information gatherers. This experience sharing is reflected in a joint US/ Singapore study on 268 subjects, all using e-Commerce sites, to determine via conjoint analysis their perceived value of privacy protection offered by these Web sites, which was found to lie in the range US$ 30-44 [13].

In terms of economics, there are models which analyze the relationship between the production of information and the externalities generated by the production of information [4]. There is also a general economic critique of personal privacy [5] with corresponding frameworks; the collection of information without consent of the person is one case which is oppose to when information is obtained through voluntary transactions. There are also simple economic models with no government intervention and free-market forces [3, 6, and 7]; eventually this concept can lead to the creation of a market for privacy, in which a consumer could buy a degree of privacy. In such markets is it expensive to maintain a certain level of privacy and thus the demand for privacy will decline, although managed privacy services and privacy-enhancement technologies maintain and customize needed privacy levels. This last view is the one upheld in this paper, with the use of SLA’s.

Even with the use of SLA`s remain amongst unresolved issues such aspects as:

-the liability of intermediary service providers which act as information gatherers and simultaneously as product or service suppliers to third parties [12]

-compliance of the legal contracts supporting the SLA`s with Data protection and Information privacy laws as studied e.g. by the “Electronic commerce legal issues platform” (ECLIP)

## 3. FRAMEWORK FOR SLA MANAGEMENT OF PRIVACY

Quality of Service in relation to Business is becoming a major concern for enterprises world-wide. So much so that that a number of international professional organizations are looking at the area with the intent of defining standards for the area. Notably, these include The Open Group and the TeleManagement Forum. These two organizations have combined to prepare an SLA Management Handbook [8]. For an overview of some topics being considered, we refer to reference [9]. This paper complements and extends the concepts discussed in the handbook [8], particularly with regard to privacy management, automated monitoring and reporting.

In this section we first offer some definitions, describe the process involved in QoS and SLA Management, and list a selection of metrics frequently used in SLAs. In the second part, we will relate these definitions and tools to privacy management.

## *3.1 Some Definitions*

- ***Service***: measurable result or outcome of a business or technical process involving a *Supplier* / *Server* and *Customer* / *Client*
- ***Supplier*** or ***Server***: Service Provider. These may be internal (e.g., IT Department) or external (Outsourcer)
- ***Customer*** or ***Client***: Service Recipient. Similar to Suppliers, these may be internal or external
- ***Quality of Service*** or ***QoS Objective***: any metric with a set target that shows whether the requirements of a *Service Level Agreement (SLA)* or implied (but measurable) customer and supplier expectations were met over a *Service Period* ;in the context of this paper, the Quality of Service or QoS objectives are the objectives for *Privacy protection* to be achieved in terms of the qualitative and quantitative privacy features (see [ 10 ])
- ***Service Level Agreement*** or ***SLA***: a formal contract between a *Supplier* and *Customer*, formalizing the details of a service (contents, price, delivery process, acceptance and quality criteria, penalties and so on). Informal SLAs exist also and may be as important and binding as the formal ones. However, informal SLAs cause misunderstandings, misinterpretation and disputes to a greater extent then the formal ones and are not recommended. In the context of this paper , the Supplier is equated with the *privacy protector*, and the customer with the *information gatherer*
- ***Service Period:*** a period for assessment of the *Quality of Service*. For business processes that are subject to an *SLA*, it is typically a calendar month. For other processes, it may be a transaction or any other measurable and relevant period of time.

## *3.2 Measurement of the Privacy protection Quality of Service*

By definition, this occurs after the service has been delivered by *Supplier* and used by *Customer*. Examples are:

- *SLA* report is delivered after the end of a *Service Period*
- End-To-End Response Time is calculated once a transaction is completed
- Packet loss and similar Telecommunication metrics are calculated over agreed periods of time
- Privacy protection metrics as described in [10 ]

## *3.3 Privacy Management: reactive vs. predictive*

### 3.3.1 Common (Reactive) Approach

The conventional way of managing service is to measure QoS/Privacy and determine whether the requirements were met. This means that a problem (if any) is detected and reacted to after the event.

This approach presents problems for everybody, for instance

- For a *Customer (Information gatherer)*: Deterioration of service cannot be prevented. Problems must happen, to trigger a corrective action. In the worst cases, on-going conduct of business may suffer.
- For a *Supplier (Privacy protector)*: Penalties (frequently specified in modern SLAs) cannot be avoided. In the worst cases, business continuation becomes problematic.

### 3.3.2 Suggested (Predictive) Approach

By contrast, this paper relies on predicting the result of QoS/Privacy compliance in advance. Therefore, it is frequently possible to take a corrective action before a problem actually occurs, thus eliminating it or, at least, minimizing its impact.

This approach avoids the problems associated with the reactive approach:

- For a *Customer (Information gatherer)*: Deterioration of service may be prevented and business conduct optimized.
- For a *Supplier (Privacy protector)*: SLA Penalties may be avoided and prospects for the business continuation improved.

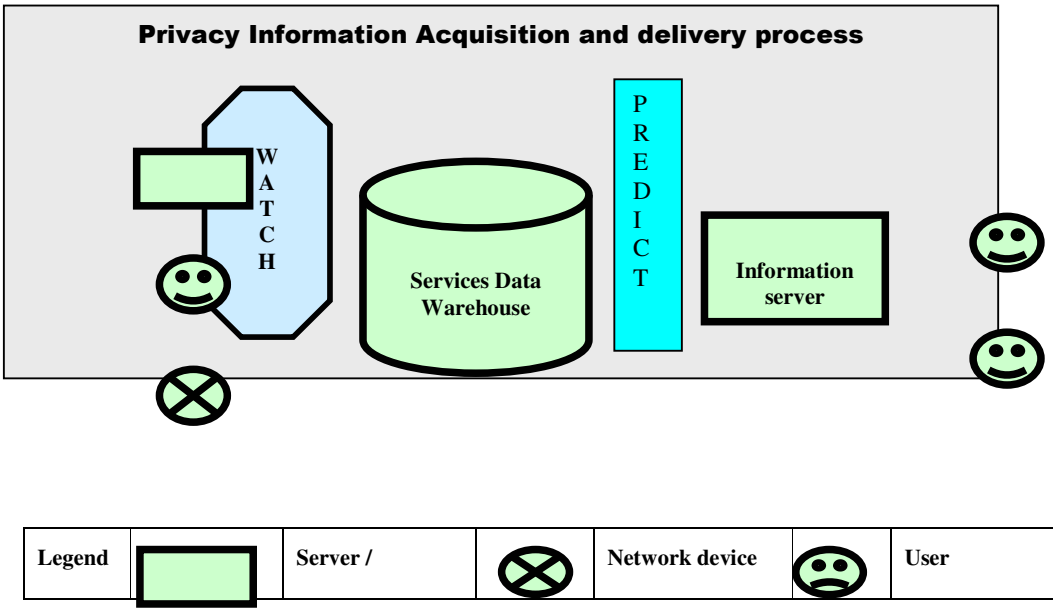
## *3.4. Basic Technical Principle: Near-Real-Time, asynchronous operation*

Any information acquisition and delivery process may be reduced to three basic tasks:

- Data Capture: acquisition of raw data
- Data Processing: transformation of data into information
- Delivery: information delivery to the recipient

A process incorporating these tasks is usually considered to be synchronous: component tasks follow each other in sequence. This is the principle of so-called Real-Time approach: data is captured and delivered to users 'as is' or with minimal transformation. This represents a major problem in System Management, as it leads to either overloading of networks due to the high volume data movements (sub-second cycle) or poor quality of data due to long sampling cycles. That, however, need not be the case.

This paper uses the so-called Near-Real-Time approach: that is, timing of information delivery is dictated by user needs. In other words, Information about privacy is delivered in time to make a difference. For instance, if a user manages a typical IT environment, it is pointless to capture sub-second data on the privacy protection characteristics of a server: network delays will ensure that such data is outdated anyway. Once-a-minute data delivery is fine. However, data can be captured frequently, be buffered up, processed and made available for delivery only when needed. This keeps data movements low while preserving the quality of data. This is accomplished by keeping the three basic tasks, asynchronous – in other words, time-independent.
This principle is illustrated by Figure 1, below.



| | | | | | | |
|---|---|---|---|---|---|---|
| | | **Application / etc.** | | **(router, etc.)** | | |

**Figure 1 :Three *asynchronous* loops for privacy information**

# 4. PRIVACY MANAGEMENT SLA's

## *4.1 Overview*

In real terms, Privacy Management equates to the conventional discipline of Capacity Planning, but with an overriding emphasis on achievement of Privacy objectives (please refer to Definitions in Section 3.1). Thus, it may be safely said that Privacy Management incorporates the following, integrated disciplines:

- Performance Management
- Service Level Reporting
- Cost/benefit assessment

with capacity planning in some rare cases being an added issue.

This paper defines the objectives of Privacy Management as follows:

- Continuous collection and remote storage of Privacy Performance and User data, in order to support the data needs and automation of subsequent processes
- Short-term monitoring of system and application resources to effect:
  - Problem detection
  - Identification of potential problems
  - Prediction of problems
  - Initiation of problem alerts
- Regular Service Level Reporting, including the prediction of results for the next Service Level interval, in accordance with a Service Level Agreement (SLA)
- Cost/benefit Service level reporting reporting , with cost and benefit assessment(s) over the Service Period
- Prediction of potential problems in the medium and long-term time-frame
- On-demand Web-enabled Reporting

## *4.2 Process*

The process of Privacy Management is presented below, in Figure 2. Please refer to reference [11] for more details on the component processes.

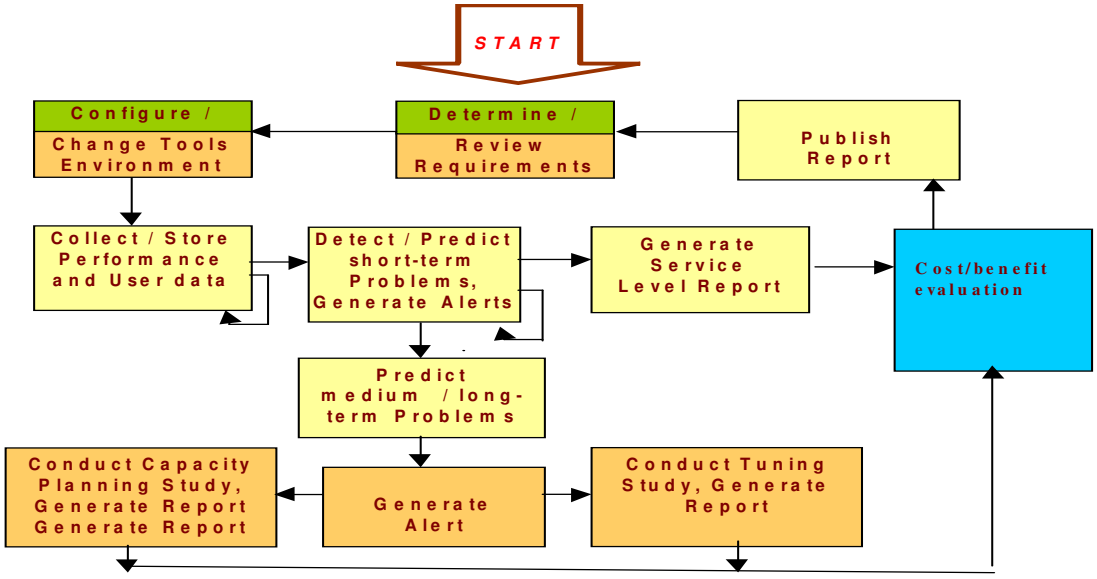



**Figure 2 : Privacy Management process.**

## *4.3 Capabilities of the system*

The capabilities required to support the integrated process shown in Figure 2 are listed below.

- Pervasive measurement and data capture.
  - All the relevant data must be captured for about the privacy feature values across :servers, storage, networks, applications, user interfaces, customer support
  - The time resolution and accuracy must be maximized (to support the Near-Real-Time approach), yet without disrupting operations or imposing undue load upon resources. In other words, the privacy feature collectors must be efficient.
  - It must be kept in mind that most operating systems, network entities and applications these days are instrumented. In order to minimize the overhead of implementing a privacy management system, it must be possible to utilize such existing instrumentation where it exists, instead of replacing it. This means that 'agent-less' data capture' using MIBs, native Windows capabilities and similar approaches must be provided.
  - It must be possible to relate the disparate items of data to each other, to derive End-To-End characteristics of processes
- Data Management capability. For large, distributed systems, volumes of data that are generated by this process may be quite large. Yet, to support historical analysis, they must be available on-line, on demand. Therefore, it must be possible to manage that data: compress, consolidate, age, archive, back up, restore, etc.
- Maximum flexibility. The target users - organizations and individuals mature enough and large enough to be interested in privacy are likely to have complex environments, with many suppliers and/or customers, variety of software and hardware platforms, applications and SLAs. In order to cater to all these requirements, utmost flexibility is necessary.
- Full scalability, no bottlenecks. Production systems are frequently very large. Such systems grow and evolve over extended periods of time as Supplier and Customer may comprise many thousands of nodes. Therefore, the software must be able to scale almost without limit in all respects – no internal bottlenecks are allowed.
- Reliability and recoverability. IT systems are business-critical already and will become even more so in time. It follows, therefore, that the software must be reliable and recoverable, to support this mode of operation.
- Maximum automation. Large-scale systems demand automation. It must be provided at all stages (data capture, management, reporting, problem detection, etc.). Indeed, all the repetitive aspects of operation for the system must be automated.

- Utilization of the best heuristic engine available: the human brain. Privacy Management system must handle routine problems, but leave important decision-making to humans. For instance, the system should handle threshold monitoring (see in [10] the calculation of privacy envelopes) and alerting automatically, but should not take automatic action to resolve problems.

## *4.4 Commonly used metrics and reports*

### 4.4.1 Privacy features

A companion paper [10] proposes a structured set of attributes and associated metrics (quantitative or qualitative) for the different facets of privacy, falling into the following categories of components of the Privacy Vector (V):

1. copy feature
2. transfer, delete, substitute feature
3. role change feature
4. identity change feature
5. time feature
6. risk feature
7. leaking feature

These features are used in the following to characterize any privacy SLA, and together constitute a feature value vector P. From these features a calculation method is also given relying on the overall stress to the privacy holder when facing an information gatherer.

### 4.4.2. Privacy cost/benefit and contractual features

Respectively *Customer* and *Supplier each* have a cost function, and a benefit function, which must include the PET provisioning amortization and provisioning costs or revenues, and each defined for the Service duration. The attributes of these functions are all the Privacy features P, as of course assessed for each Party .Thus, in total, we have four cost/revenue functions:

Cost(Customer) = Cost (Information gatherer)
Cost(Supplier)= Cost (Privacy protector)
Benefit(Customer) = Benefit (Information gatherer)
Benefit(Supplier) = Benefit ( Privacy protector)

Furthermore, this category of SLA Metrics includes the basic references of a contractual nature, a pointer to Framework agreement and the selected Cost/benefit negotiation algorithm:

- Applicable framework agreement reference and version
- Applicable framework agreement validity period
- Identification of Supplier party , responsible and settlement account
- Identification of Customer party , responsible and settlement account
- Third party for authentification
- Validity of SLA
- Cost/benefit negotiation algorithm selected

#### 4.4.3 Management attributes

- Backup/Recovery for Month
  - Privacy Incident Number
  - Date Opened
  - Date Closed
  - Details
- Completed & Outstanding Relocation Requests by Location for Month
  - Reference No.
  - Status
  - Title
  - Details
- *Ad hoc* Third Party Reporting
  - Reference Number
  - Third Party
  - Service Performed
  - Details
- Privacy Administration for Month
  - % of time within SLA requirements
  - Breaches
    - Reference
    - Description
- Change Management for Month
  - Outstanding Change Requests from Last Month
  - Registered Change Requests
  - Change Requests Cancelled this month
  - Change Requests Closed this month
  - Changes Regressed this month
  - Total Outstanding Change Requests at month end
  - Change Requests Outstanding broken down by
    - Assessment
    - Authorization
    - Implementation
    - Contract Changes
    - On Hold
    - Review
    - Signoff
  - New Change Requests
    - CR Number
    - Date Raised
    - Status
    - Description

- Date Implemented
- Schedule met? (Y/N)
- First Attempt Successful? (Y/N)
- Back-out Required? (If Y provide details)

## 5. PREDICTIVE PRIVACY MANAGEMENT PROCESS

For any Privacy Objective that has been defined over a specified service period, the value of the current privacy metric can be calculated for any elapsed sub-interval of the service period. Conversely the required value of the privacy metric for the remainder of the service period can also be calculated, such that the overall privacy metric for the full service period meets the privacy objective. These two facts provide a basis for issuing predictive alerts that can be presented in a GUI interface.

An example of a predictive function within the context of an SLA metric of privacy is the compliance with boundaries, also called privacy envelope ([10]). The purpose of an objective function is to calculate the remainder SLA metric value that is required in order to meet the SLA objective by the end of the service period. The remainder SLA metric value can be the surface between the actual privacy feature values outer surface, and the surface made of the thresholds.

The value of an SLA objective function lies in knowing either that SLA achievement is likely or that it is in jeopardy of being missed. The objective function's results can be evaluated on a daily basis and used for posting predictive alerts that indicate the degree to which achieving one or more privacy objectives is in jeopardy.

## 6. PRIVACY SLA BUSINESS NEGOTIATION

The framework agreement includes a list of cost/benefit negotiation procedures and outcomes in the form of settlements between the parties, to ensure stability and suitable negotiation which SLA settlement may not allow under operational pressures.
The framework must also include stable cost sharing provisions for the SLA feature data collection and monitoring tasks. Examples thereof are:
-either fixed settlement terms, e.g. that the Supplier (Privacy protector) gets payment from the Customer (Information collector) proportional to each of the four quantitative components of the privacy features (quantity of data copied, transferred , deleted, substituted ) ,while the Customer (Information collector) gets a per-Service Duration usage fee from the Supplier (Privacy protector) for the provisioning of privacy enhancement technologies (PET)

-or a true recursive negotiation using past Service Duration as predictive data ,to reach an equilibrium over the current Service duration between the four criterion functions Cost(Supplier), Benefit(Supplier) , Cost (Customer) , Benefit (Customer) ,in that the values from the past duration are the initial bids from each party ,and a simple equilibrium algorithm determines the settlement terms applicable to the yet unknown current Service duration

## References

[1] J.Kumagai, S.Cherry, "The sensor nation", **IEEE Spectrum**, July 2004, 18-44

[2] -Wall Street Journal **,**Internet Privacy Rules Could Cost Business As Much as $36 Billion , **Wall Street Journal** , p. B.5, May 8, 2001; or: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000072539284&svc_dat=xri:pqil:fmt=text&req_dat=xri:pqil:pq_clntid=5072

[3] Rust, Roland T; Kannan, P K; Peng, Na, The customer economics of Internet privacy **Academy of Marketing Science. Journal**, Vol. 30 (2002), no 4 ,p. 455; or :http://proquest.umi.com/pqdweb?index=2&did=000000184803381&SrchMode=1&sid=6&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1088081507&clientId=5072

[4] Gould, John P, Privacy and The Economics of Information, **Journal of Legal Studies**, Vol. 4 (December 1980), 827-842 ; or http://www.journals.uchicago.edu/JLS/journal/

[5] Murphy, Richard S., Property Rights in Personal Information: An Economic Defense of Privacy, **Georgetown Law Journal** 7 (July 1996), 2381-2417

[6] Coleman, James S, An Introduction to Privacy in Economics and Politics **, Journal of Legal Studies** , Vol. 4 (December 1980), 645-648.; or http://www.journals.uchicago.edu/JLS/journal/ but server was down 06-09-2004

[7] Posner, Richard A., The Economics of Privacy, **The American economic review** , Vol. 71 ,no 2(May),1981

[8] The SLA Handbook, **Open Group andTeleManagement Forum** , 2004 (restricted members only distribution)

[9] Jon Saperia, "How SLAs Are Used", **Network Computing**, March 21, 2003, pp. 71-75.

[10] L-F Pau, Privacy metrics and boundaries: a first approach, Rotterdam School of management, July 2004, and EU IST Project "PRIME" URL: www.prime-project.eu.org

[11] Mike Tsykin & James Bouhana, "On Automated Monitoring of SLAs", **CMG Journal of Capacity Management**, summer, 2002

[12] Proc. E-Contract conference, Consumer policy center, Brussels, 18-19 October 2001

[13] Il-Horn Hann, Kai-Lung Hui, Tom S. Lee, I.P.L. Png, "The value of online information privacy: evidence from the USA and Singapore", Research report, National University of Singapore, September 2002

## ACKNOWLEDGMENT

This paper is one public deliverable of the European Union's IST project "PRIME" on privacy enhancement URL: www.prime-project.eu.org.

## Publications in the Report Series Research* in Management

### ERIM Research Program: "Business Processes, Logistics and Information Systems"

2005

*On The Design Of Artificial Stock Markets*
Katalin Boer, Arie De Bruin And Uzay Kaymak
ERS-2005-001-LIS
http://hdl.handle.net/1765/1882

*Knowledge sharing in an Emerging Network of Practice: The Role of a Knowledge Portal*
Peter van Baalen, Jacqueline Bloemhof-Ruwaard, Eric van Heck
ERS-2005-003-LIS

*A note on the paper Fractional Programming with convex quadratic forms and functions by H.P.Benson*
J.B.G.Frenk
ERS-2005-004-LIS

*A note on the dual of an unconstrained (generalized) geometric programming problem*
J.B.G.Frenk and G.J.Still
ERS-2005-006-LIS

A Modular Agent-Based Environment for Studying Stock Markets
Katalin Boer, Uzay Kaymak and Arie de Bruin
ERS-2005-17-LIS

Keywords Lagrangian duality, cone convexlike functions
J.B.G. Frenk and G. Kassay
ERS-2005-019-LIS

---

* A complete overview of the ERIM Report Series Research in Management:
https://ep.eur.nl/handle/1765/1

ERIM Research Programs:
LIS Business Processes, Logistics and Information Systems
ORG Organizing for Performance
MKT Marketing
F&A Finance and Accounting
STR Strategy and Entrepreneurship