Privacy Contracts as an Extension of Privacy Policies

Hendrik JG Oberholzer
Tshwane University of Technology
oberholzerhjg@tut.ac.za

Martin S Olivier
University of Pretoria
http://mo.co.za

Abstract

Individuals are becoming increasingly concerned regarding the protection of their personal information. In an attempt to ease the privacy concerns of individuals, organisations publish privacy policies, promising how they will handle personal information. However, privacy policies as such do not guarantee the protection of personal information and do not offer much customisation on an individual level.

Individual privacy contracts are proposed as a solution to this problem. A privacy contract constitutes a legal base on which to contest privacy breaches, should any occur. Every data subject has to enter into a privacy contract (consisting of privacy agreements) with the data controller, otherwise no transactions can be performed between the two parties. A data subject must consent to a privacy agreement before the data controller can use the data of the transaction associated with the agreement.

This paper presents the principles and a conceptual view of the management of privacy contracts.

1. Introduction

Organisations collect large amounts of personal data about their clients and store some of the most sensitive information in databases [1]. While still allowing 'legitimate' access to this information, organisations must prevent that their clients' personal data are intentionally or sometimes unintentionally misused [2]. Misuse of personal information might implicate privacy breaches and as such lead to unwanted intrusions of the privacy of the client. As an ever-increasing number of privacy violations surface in literature and news articles, individuals are becoming more and more concerned about the privacy of their personal information [3]. These concerns might lead to a situation where the clients do not trust the organisation any more [4, 5] and take their business somewhere else [6].

In an attempt to ease the privacy concerns of their clients and to adhere to new legislative measures, organisations publish privacy policies, stating what they would or would not do with the personal information of their clients. However, privacy policies alone are not sufficient to convince potential clients to disclose their personal information to the organisation – the primary question that has to be answered is therefore: What could organisations do to ensure that their clients trust the organisation to protect their personal information against potential misuse? Secondly, how can clients exercise privacy preferences and as such have control over their personal information?

This paper introduces privacy contracts as a solution to the questions asked. The concept of privacy contracts and the principles on which these contracts are based, are discussed and the management of privacy contracts are described.

The remainder of the paper is structured as follows. Section 2 provides more background on the problem. Section 3 introduces the fundamental concepts on which privacy contracts are based. Section 4 addresses the management of privacy contracts. Section 5 provides a brief summary of the paper. The paper concludes with a brief discussion of possible future application developments, specifically implementation and integration aspects with regard to new and existing applications (see Section 6).

2. Background

Definitions of personal information (sometimes also referred to as personal data) are found in the privacy legislation of many countries [7,8]. The Electronic Communications and Transactions Act of South Africa [9] is a relatively new act that divides personal information into nine categories of information relating to an identifiable individual. Two of these nine categories are most pertinent to this paper. The one category includes information relating

to the race, gender, ethnic or social origin, physical or mental health, disability, religion, conscience, and belief of the individual, while the other category includes information relating to the education, medical, criminal, or employment history of the individual as well as information relating to financial transactions in which the individual has been involved. Some of this personal information might be of a very sensitive nature, for example the HIV status, contraction of contagious diseases, or financial income.

Organisations collect large amounts of personal data about their clients and process this data into supposedly useful information. The term 'supposedly' is used because some of this personal information might be of a very sensitive nature and when such sensitive information is used for purposes that the client did not intend the information to be used for (defined as misuse), this uncalled-for use might lead to unintentional or malicious disclosure [10].

More often than not, organisations do not realise the potential risk associated with the storage and processing of sensitive personal information until an audit reveals who has accessed this information [11]. In addition to audits performed, literature surveys reveal numerous cases where personal information of individuals was misused [12, 13, 14, 15]. It is therefore not unexpected that there is a growing concern among individuals about the ever-increasing list of privacy violations that occur and the realisation that individuals do not trust those that collect and handle their personal information [16]. Consequently, individuals that do not trust an organisation might provide incomplete, inaccurate, or misleading information [17, 13] or might not even be willing to disclose any of their personal information to the organisation [18], in which case the organisation might lose client value. However, individuals might be willing to share their personal information if they trust the organisation and perceive reasonable benefits in return [19].

In an attempt to instil trust, organisations publish their privacy policies to disclose how they will handle the data of their clients. In the context of this article, a privacy policy is one or more statements that a data controller (for example an organisation, enterprise, or any institution or public body that handles data) makes to a data subject (the individual or person whose data will be handled) stating how the data controller will handle the personal information of the data subject.

However, simply publishing a privacy policy does not guarantee trust nor does it comply with privacy laws or regulations [20]. Most importantly, a privacy policy does not guarantee the protection of personal information of data subjects. Privacy policies are merely promises [3, 21, 22] and a promise as such sometimes has no legal grounds on which to contest a privacy breach should the data controller not keep the promise [23]. There is a need for something more trustworthy, more formal, and more legal than a promise - a privacy contract.

This paper introduces a privacy contract composed of a number of formally signed (electronic, digital, or handwritten) privacy agreements between a data controller and a data subject. As the composition of the privacy agreements constitutes a contract, the privacy contract is legally binding and enforceable. The data subject has control over what information may be used for what purpose when performing a specific transaction. Although the enforcement of the privacy contract resides with the data controller, data subjects exercise control over their personal information as they consent to specific transactions performed on their personal data for specific purposes. At any time data subjects can view all changes made against their privacy contracts as well as view all disclosures of their privacy agreements. The data controller still has to define its internal privacy policies, as the agreements of a privacy contract are based on and extracted from the installed privacy policy of the data controller.

3. Privacy contracting fundamentals

The problems related to trust and privacy policies as highlighted in the previous section lead to the proposed solution of privacy contracts. As privacy contracts are based on the concepts and principles of Hippocratic databases, section 3.1 briefly introduces the concept of Hippocratic databases. Where appropriate, the paper will indicate how these principles contribute to the concept of privacy contracting. Section 3.2 describes where the idea of privacy contracts originated from and places the contracts in the context of a complete privacy framework to protect personal information in relational databases. The principles that constitute a privacy contract are described in section 3.3. Following section 3, section 4 discusses the management of privacy contracts.

3.1. Contribution of Hippocratic databases

Agrawal et al. [24] suggest that databases must take responsibility for the privacy of data as a fundamental tenet and that such databases should be called Hippocratic databases. Hippocratic databases are built upon ten principles (from now on referred to as Hippocratic principles) that might become the founding principles to protect and manage personal

information that reside in databases (see [24]). These principles define what a data subject could expect from a database that claims to be Hippocratic. But again, promises and expectations are not good enough to guarantee privacy protection and *"Technology can't create trust where society sows doubt and disbelief, it can only hope to minimise the risk"* [25]. Thus, in order to minimise risk further, privacy contracts incorporate these Hippocratic principles. Further discussions in the remainder of this paper will indicate how these principles support privacy contracts.

The most significant difference between privacy contracts and Hippocratic databases is that privacy contracts are primarily based on transactions as opposed to Hippocratic databases that are purpose-driven [24]. In the context of this paper a transaction is defined as any kind of interaction or action (for example view, display, print, add, modify, delete, audit) that is performed on the personal information (stored in a relational database) of the data subject either by the data subject or the data user (a data user is the person who is authorised to handle the personal information of the data subject). The reason why privacy contracts are associated with transactions is, because whenever a transaction is performed, the transaction is performed on a certain subset of the personal data of a data subject. Once a data subject has consented that the data controller may perform the specific transaction, only then might the data subject consent to one or more specific reasons why the transaction may be performed on his/her personal information.

Consent associated with a transaction (performed for a specific reason) is supported by five of the Hippocratic principles namely: Purpose Specification (purpose is associated with the stored information by consenting to the transaction that uses the stored data), Consent (data subject has agreed to the purposes associated with the transaction), Limited Collection (only data needed by the transaction, for the purpose consented to, will be stored), Limited Use (stored information can only be used by the transactions consented to) and Limited Disclosure (stored information can only be disclosed through disclosing transactions consented to).

The Hippocratic Principle of Safety (i.e. personal information should be protected by security safeguards against theft and other misappropriations) should be addressed as a security issue and is not within the scope of this paper. The rest of the Hippocratic principles not listed here are addressed at later stages when more appropriate.

3.2. Privacy contract origin and context

The idea or concept of a privacy contract was partially derived from a statement that Lau et al. [26] made when they stated, "*Since there is no universal policy appropriate for all users, designers must provide users with a means of specifying their own individual privacy policies*". This means that data subjects not only have to consent or withhold consent to what is presented to or promised to them, but data subjects must be able to customise their privacy preferences at an individual level (see Section 3.3.2). The concept of individual privacy policies, combined with the principles of Hippocratic databases, culminated in the concept of a privacy contract.

Privacy contracts are not the same as privacy policies, but are extensions of privacy policies. From an organisational point of view, a data controller normally publish a general privacy policy stating how personal or private information of the data subjects will be handled. In addition to the privacy statements proclaimed by the data controller, data subjects sometimes have the opportunity to opt-in or opt-out from certain uses of their personal information, but these opportunities are limited and do not allow for fine-grained levels of choices. As an extension to privacy policies, each privacy contract is based on these privacy statements as defined by the data controller in the privacy policy of the organisation. It should be evident that before any privacy contract can be established, the privacy policy must first be defined and installed by the data controller.

However, privacy contracts cannot function isolated from the business applications (mostly transaction processing systems), therefore a privacy contract is a central component of a comprehensive privacy protection framework or architecture.[1] Such a framework also includes two additional components: one component to manage the privacy policies of the data controller and one component to enforce the privacy contracts when business processes are performed. In addition to these three components, privacy auditing plays a fundamental role and is integrated into the components that manage the privacy contracts and enforce the privacy contracts.

3.3. Privacy contracting principles

It is not an easy task to determine how a privacy policy applies to a particular transaction. Various factors and contexts affect the application of the privacy policy, for example who is accessing whose data for what reason [10]. However, this task could be

[1] Development of the complete framework is still in progress and will be reported on at a later stage.

simplified through the concept of privacy contracts.

A privacy contract is based on a minimum set of mandatory privacy agreements without which no privacy contract could exist. In addition to the mandatory privacy agreements, optional privacy agreements could be added when required by the data subject. Without a privacy contract no transactions can be performed between the data controller and the data subject.

The remainder of this section will use the example of a pharmacy to illustrate the privacy contracting principles and to differentiate between transactions and agreements and the relationship between them. Following that, the different levels of privacy agreements are introduced and discussed.

3.3.1. Agreements, transactions and purposes. As stated earlier, a privacy contract consists of a minimum number of privacy agreements. In order to perform a transaction on the data of a data subject, the data subject must consent to the data controller's use of the data associated with the specific transaction. This is done through the establishment of a privacy agreement associated with the specific transaction. Before any transaction can be performed, a privacy agreement associated with the specific transaction must exist, or otherwise a privacy agreement must first be established. Central to the concept of privacy contracts is the distinction between mandatory and optional transactions.

Mandatory transactions are transactions without which the data controller cannot run his business. When a data subject wants to open an account at the pharmacy, a privacy contract must first be created (see Section 4.2) During the process of creating the privacy contract some personal information might be needed in order to check the financial credibility of the data subject. An example of a mandatory transaction therefore might be to 'Capture Credit References'. If the data subject needs to open an account, the data subject has no other choice than to consent to this mandatory transaction, otherwise no account could be opened.

The data subject must close a privacy agreement for each mandatory transaction otherwise no optional transactions could be performed against the database.

An **optional transaction** is a transaction that is not mandatory. It depends on every data subject whether to perform such an optional transaction or not. As soon as the data subject has consented to all mandatory agreements the subject can set privacy preferences for any optional transaction(s) through the closing of an optional privacy agreement associated with each of the specific optional transactions. However, closing of an optional privacy agreement depends on the data subject to consent to the optional transaction at any time, as long as consent is given before the optional transaction must be performed, otherwise the optional transaction would not be possible. An example of an optional transaction might be to 'Capture Home Address' in order to deliver the medicine at home.

Every transaction has one or more purposes that the transaction may be used for, as defined in the privacy policy of the data controller. A purpose may be mandatory or optional.

When consenting to any transaction, the data subject must consent to all **mandatory purposes** (if any) relating to the specific transaction otherwise the data subject is not allowed to perform the specific transaction. An example of a mandatory purpose might be to 'Deliver Medicine at Home Address'. This mandatory purpose relates to the optional transaction 'Capture Home Address'.

In contrast to mandatory purposes, an **optional purpose** is a purpose that is not absolutely necessary for the day-to-day running of the business, but it might be to the benefit of the data controller or the data subject if the data related to a transaction can be used for the specific optional purpose. Therefore a data subject may or may not consent to an optional purpose. An example of an optional purpose might be to use the data of the transaction to 'Purchase Medicine on Account' for the optional purposes of 'Inform Data Subject about Alternative Treatments' and 'Inform Data Subject when Prescription has to be Renewed'. The data subject might consent to the second optional purpose, but not to the first purpose related to the optional transaction 'Purchase Medicine on Account'.

A data controller is allowed to use the data relating to a transaction only for the purposes that the data subject has consented to. These purposes consented to by each data subject are saved in the database.

3.3.2. Privacy agreement levels. People have different perceptions about privacy [27]. Some individuals might view a specific act as an invasion of their privacy while other individuals view the same act as acceptable, and some individuals might not even be aware that they are eroding their own privacy. Based on these perceptions, one can argue that data subjects require their personal information to be treated in different ways. These perceptions induced the concept of agreements to be consented to at different levels of privacy as preferred by each data subject - for every optional transaction, every data subject can decide what level of privacy is preferred for the specific transaction to be performed on his/her data.

Before a data subject can request a specific transaction to be performed on his/her data, or before

a data controller can perform a transaction on the data of the data subject, the data subject must already have entered into a privacy agreement associated with the specific transaction. Furthermore, the data controller can only perform a transaction on the personal data of the specific data subject, when the data subject has entered a privacy agreement related to the specific transaction. As these agreements would be enforced according to the privacy framework (see Section 3.2) it should be clear that data subjects have control over their personal information.

Privacy agreement levels are defined at levels 0,1,2, or 3. The motivation for the four levels is based on two arguments, and because an agreement directly relates to one transaction, the arguments will be stated in terms of transactions and not agreements. The first argument is that central to the privacy protection framework a distinction has been made between mandatory and optional transactions - thus an initial need for two levels or categories. Regarding the level of optional transactions, data subjects have the opportunity to exercise some choices. Based on the different perceptions that data subjects have about privacy and the protection of personal data, Westin [28] divided data subjects into three groups or categories namely the privacy fundamentalists (usually unwilling to share information freely), marginally concerned (willing to share information), and pragmatic majority (people fitting somewhere between the other two groups). Each of these groups is then assigned a level. Therefore four levels are needed – one level (0) for mandatory transactions and three levels (1,2,3) for optional transactions.

Mandatory transactions are defined at privacy **level 0** and their corresponding privacy agreements must be included in the privacy contract of every data subject. A data subject must consent to all mandatory transactions, otherwise a privacy contract cannot be closed and no transactions can commence. Furthermore, every mandatory agreement must be consented to before any other optional transactions can be consented to and/or performed.

Data subjects must specify their own preferred privacy level for every optional transaction. Based on the different perceptions that data subjects have about privacy [27] and their different levels of privacy awareness, optional transactions can be consented to at privacy levels 1, 2, or 3.

Privacy agreements at **level 1** (standard level) aim to support the category of marginally concerned data subjects in protecting their personal information based on fair information practices. In addition to the mandatory transactions defined at privacy level 0, optional transactions can be consented to at privacy level 1. Optional transactions consented to at privacy level 1 are associated with mandatory purposes only. No opt-in or opt-out choices are available, except for the choice whether to allow the data controller to use or not to use the data of the optional transaction for the consented mandatory purpose(s) as specified in the privacy policy of the data controller. Thus, level 1 provides a take-it-as-it-is-or-not option for every optional transaction.

For example, when consenting to a transaction named '*Purchase Medicine on Account*' at privacy level 1, a mandatory purpose for which the transaction data of the purchase may be used, might be '*To Create and Send an Invoice*'. Another mandatory purpose might be '*To Perform Statistical Analysis on Sales Figures to Improve Stock Levels'*. Both these purposes are related to the transaction and the data subject must consent to both before the privacy agreement is closed and the transaction may commence. Mandatory purposes at level 1 should be included in the privacy policy according to fair information practices. At any time an external privacy auditor might inspect the privacy policy to verify that the privacy policy complies with fair information practices.

Privacy agreements at **level 2** (medium level) aim to support the pragmatically concerned data subjects. In addition to mandatory purposes that might be defined for an optional transaction, optional transactions at this level provide data subjects with the choice of opting-in or opting-out of optional purposes relating to each optional transaction. The data controller may use the data on which the optional transaction is performed only for the purposes that the data subject has consented to, whether these purposes are mandatory or optional.

To illustrate an agreement at privacy level 2, the transaction used as an example at level 1 applies again. In addition to the two mandatory purposes that have to be consented to, the data subjects now have the choice to decide whether their data that have been used for the transaction may be used for the purpose of 'To C*ompile a Profile of the Data Subject Regarding his/her Spending Patterns'*, and/or T*o Use his/her Personal Information for Research Purposes*'. The data subject may consent to none of the two optional purposes, or for one purpose only, or for both purposes.

At **level 3** (advanced level) the privacy model aims to support the privacy fundamentalists. In addition to the support that level 2 provides to data subjects, at level 3 data subjects could specify for each optional transaction and for each related optional purpose consented to, what data the data controller may or may not use for that specific optional purpose. Because the purpose is optional it is the prerogative of the data subject to decide what data pertaining to the transaction may or may not be used.

The examples used to illustrate agreements at levels 1 and 2 are extended further to illustrate a privacy agreement preferred at level 3. Let us assume that the purchase is performed for a very sensitive case where the medication purchased is prescribed for HIV treatment. To purchase on account, the transaction might use the following data: product description and quantity purchased. This information might then be linked to the account where the following data is stored (and has been consented to): surname, initials, postal address, city, and date of birth (date of birth is necessary to verify dosages). When a data subject consents that the data of the purchase transaction may be used for research purposes, an agreement at level 3 then gives the data subject the opportunity to specify which of the data can be used for research purposes. The data subject might specify that the data pertaining to the city, product description, and quantity purchased may be used for research purposes[2]. Although all data relating to this transaction may be used for the mandatory purposes consented to, when it comes to the purpose of research, only these three data items may be used, nothing else.

4. Managing privacy contracts

The management of privacy contracts mainly consists of authenticating privacy contracts, creating privacy contracts, updating privacy contracts, viewing and printing privacy contracts, and support for the auditing of privacy contracts.

4.1. Authenticating a privacy contract

Each time a data subject interacts with the data controller the first step is to authenticate the data subject -the objective is to verify that the data subject has a privacy contract and that the contract belongs to the specific data subject and not to anybody else. As soon as the data subject has been authenticated and it has been determined that the contract is active, the data subject must choose the transaction to be performed.

Active contracts are contracts against which database transactions (those agreed to) may be performed. When a contract is inactive, only three transactions are allowed against the contract: reactivating the contract, performing an audit against the contract, archive the contract (retention period has expired).

In case the data subject does not have a privacy contract, a contract must be created.

4.2. Creating a privacy contract

A data subject enters into a privacy contract with the data controller by creating a privacy contract. Creation of a privacy contract mainly consists of three steps: initialising the contract, consenting to mandatory agreements, and compiling the contract (including the privacy agreements consented to).

During initialisation of the contract a contract number and password are assigned to the data subject and the status of the contract is set to '*active*'. Unique identifiers like student numbers, account numbers, etc. might serve as contract numbers.

One of the problems why individuals do not bother to read privacy policies is that privacy policies are boring to read because of all the fine print hidden in the policy [13, 29]. Instead of consenting to a long list of policy statements that cover the whole spectrum of ways the personal information of the data subject will be protected, the data subject initially only has to consent to a small number of mandatory agreements while creating a privacy contract. When the data subject has consented to all the mandatory agreements, the contract is created.

As soon as a contract exists between a data subject and the data controller, and the contract has been authenticated as belonging to the data subject, privacy agreements can be entered into with regard to the optional transactions. The data controller is bound by the privacy agreements to perform a transaction only when the data subject has consented to the privacy agreement relating to the purpose for which the transaction has to be performed.

As soon as the privacy contract has been created, a copy of the contract (including all mandatory agreements and optional agreements, if any) is compiled and signed. At any later stage the data subject has the opportunity to add, modify, view, or print the privacy agreements again. By allowing data subjects to view or print their privacy contracts, the Hippocratic Principle of Accuracy is partly adhered to. Data validation procedures must be in place to fully comply with this principle.

4.3. Updating privacy contracts

As soon as a data subject has been authenticated and it has been determined that the privacy contract is active, the data subject has the opportunity to add, modify, or delete any privacy agreements.

Whenever a data subject requires a transaction to be performed, the first step is to verify that a privacy agreement related to the specific transaction does exist. If the agreement does not exist, an agreement

[2] It is not within the scope of this paper to determine whether the data consented to is useful for research purposes or not. The intention is only to illustrate the choices that data subjects have when consenting to privacy agreements at level 3.

must be added.

It might happen that a privacy agreement must be modified where the data subject wants to lower or increase the level of the privacy agreement. When the level is to be lowered, higher-level fine-grained detail must be deleted. When the level is to be increased, higher-level fine-grained detail must be added (see Section 3.3.2) However, it is also possible that the level stays the same in which case optional purposes may be added or deleted from level 2, or data items added or deleted for a specific purpose at level 3.

When privacy agreements are to be deleted, care must be taken that no mandatory purposes are deleted at level 2, or no mandatory transactions are deleted from level 0. The Principle of Retention (data is kept as long as is necessary) is adhered to through the option to delete privacy agreements and the setting of the status of a privacy contract.

It must be noted that whenever the data controller makes any changes to the privacy policy, all affected privacy agreements stay as they are until consent has been given for the changed (new) agreements. The issue of changing privacy policies is handled by the component that manages privacy policies, and getting renewed consent is handled by the component that enforces privacy contracts (see Footprint 3).

4.4. Auditing privacy contracts

The Hippocratic Principle of Openness requires that data subjects should be able to access all their information stored in the database, especially their privacy contracts. Firstly, provision is made that data subjects can view or print all actions (not limited to additions, updates, deletions, viewing) performed against their privacy contracts. Secondly, supporting the Hippocratic Principle of Compliance, the database allows an auditor to verify that the privacy policy complies with the privacy contracts. However, even these auditing actions should be logged.

An integral part of privacy contracts is the process of logging every instance of access made to the contracts[3], even when a privacy agreement was only viewed or printed. Every time the contract of a data subject is accessed, a record is added to the log. This record stores information about the data subject whose contract is changed (the contract number), which agreement was changed (the id of the transaction associated with the agreement), who made the change, the date and time the change was made, and the action and description of what was done (for example: decreased privacy agreement level from 3 to 2, etc.).

[3] Auditing of the transactions performed against the personal information (excluding contract detail) of the data subject is covered in the privacy contract enforcement component of the comprehensive privacy protection framework (see Section 3.2).

5. Summary

At the beginning of this article the question was raised about what organisations could do to ensure that their clients trust the organisation to protect their personal information against potential misuse. Secondly, the question was asked, how clients could exercise privacy preferences and as such have control over their personal information.

It became evident that privacy policies as such do not really succeed in solving these two problems - too many promises are made and the policies (if existing) are not legally binding. In some cases data subjects have very vaguely stated choices from which they can opt-in or opt-out. At best, solutions like Hippocratic databases allow users to make a choice out of three different levels of protection based on purposes only - when a level of privacy protection is chosen, purposes are automatically allowed or not, irrelevant of the transaction that is performed and what data is used by the transaction.

In contrast to privacy policies, a privacy contract is a legal agreement between a data subject and a data controller, consisting of a number of privacy agreements based on the privacy rules of the data controller and privacy preferences exercised by the data subject. Through privacy contracts, individuals have more control over the use of their personal information, and consequently should trust the organisation to protect their personal information against privacy breaches.

To summarise, data subjects enter into a privacy contract that is based on the privacy policy of the data controller. In order to have a contract, the data subject must first consent to mandatory transactions (privacy agreements) at privacy level 0, otherwise no further transaction processing will be allowed on the data of the data subject. As soon as the data subject has entered into a privacy contract with the data controller, the data subject may decide at any later stage to add agreements for optional transactions to be performed. However, before an optional transaction can commence, the data subject must specify the degree of privacy preferred as a privacy agreement for the specific optional transaction. The degree of privacy for optional transactions ranges from 1 to 3 and provides for different views of privacy as perceived by data subjects. At privacy level 1, optional transactions could be chosen to be consented to, but no further choices will be allowed. At privacy level 2, the data subject consents to purposes for which the data of the optional transaction may or may not be used by the data controller. At privacy level 3, data on which the

transaction is performed, may be opted-in or opted-out from use for each specific optional purpose relating to a specific optional transaction.

6. Conclusion

This article paved the way for a new approach to privacy protection and supports the tenets on which Hippocratic databases are based as this work can be integrated with such databases.

Although it might seem that privacy contracts involve less work for or interaction from the end user, the emphasis should be more likely that the end user controls only the data directly related to the transactions wished to be performed by the end user. No lengthy agreements have to be completed prior to interaction – only a small set of mandatory transactions has to be consented to.

With regard to implicit consent, nothing is left to chance – the concept of mandatory transactions supports this notion. The data controller can only perform those transactions consented to by the data subject. Should new regulatory measures be introduced or privacy laws be enacted, the privacy contracts of those individuals that have not yet consented to these changes could be frozen until they have consented to these changes or their data may not be used.

Lastly, privacy contracting (as mentioned in the title) is an extension of privacy policies. As long as the data controller or his/her employees act or intent to act maliciously, there could be no guarantee that even privacy contracting will solve the privacy problem effectively.

As this article introduced privacy contracting at a conceptual level, algorithms have already been developed at a lower level (based on a relational database scheme) to guide the implementation of the privacy contracts in relational database management systems. Through the algorithms it became clear that with little effort, privacy contracts could also be implemented in existing relational databases. The algorithms developed could also be adapted to implement privacy contracts when developing web applications.

7. References

[1] E. Damiani, S. De Apitani di Vimercati, S. Jajodia, S. Paraboschi and P. Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs", *Proceedings of the 10th ACM Conference on Computer and Communication Security*, Washington, DC, USA, October 27-31, 2003, pp93-102.

[2] J.J. Cadiz and A. Gupta, "Privacy Interfaces for Collaboration", Microsoft Research, Collaboration & Multimedia Group.

[3] G. Karjoth, M. Schunter, and M. Waidner, "Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data", *2nd Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science*, Springer Verlag, 2002.

[4] M. Nykamp and C. McEachern, "Customer Relationship Report: Privacy, CRM and ROI", *DM Review*, February 2001.

[5] T. Vila, R. Greenstadt and D. Molnar, "Why We Can't be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market", *Proceedings of the 5th International Conference on Electronic Commerce*, Pittsburgh, PA, 2003, pp. 403-407.

[6] E. Favilla. "Companies and Consumers Clash on Privacy Issues", *DestinationCRM*, January 29, 2004. Available at http://www.destinationcrm.com/articles/default.asp?articleid=3825.

[7] Republic of Argentine, "Personal Data Protection Act. Act 25, 326. Chapter 1", October 4, 2000.

[8] Upperhouse of the Dutch Parliament, "Personal Data Protection Act (Wet Bescherming Persoonsgegevens)", Stb. 2001, 180, April 5, 2001.

[9] Republic of South Africa, "Electronic Communications and Transactions Act. 2002. Act 25 of 2002. Chapter VIII – Protection of Personal Information, Scope of Protection of Personal Information".

[10] A. Buecker and Y. Watanabe, "Design Considerations For Privacy-Preserving Database Access", *Software Books Paper*, IBM Corporation, 2003.

[11] S.C. Nevins, "Database Security - Protecting Sensitive and Critical Information", *DM Direct*, January 2003.

[12] F. Bowers, "Dept Admits Privacy Breach", *IrishHealth.com*, June 06, 2004. Available at http://www.irishhealth.com/?level=4&id=5992.

[13] A. Jahnke, "Three Things You Don't Want to Know About Your Personal Information", *Darwin Magazine*. July 9, 2003. Available at http://www.darwinmag.com/connect/opinion/column.html?ArticleID=831.

[14] Union-Tribune Editorial, "Stolen Data: Yet Another Financial Privacy Breach", *The San Diego Union-Tribune*, April 17, 2004.

[15] "News Target Network. Senators Want to Investigate Privacy Breach by JetBlue Airlines", October 26, 2004. Available at http://www.NewsTarget.com/000251.html.

[16] T. Claburn, “Report: People Don’t Trust Government to Protect Privacy”, *Information Week*, February 13, 2004. Available at http://www.informationweek.com/story/showArticle.jhtml?articleID=17700220.

[17] D. Groszkruger, “Patient Privacy: Practical Tips to Avoid Being Caught in a Legal Crossfire”, *CAPsules*, Editor JD, MPH. Available at http://www.cap-mpt.com/riskmanagement/patient-privacy.html.

[18] J.A. Cazier, B.B.M. Shao and R.D.St. Louis, “Addressing E-Business Privacy Concerns: The Roles of Trust and Value Compatibility”, *Proceedings of the 2003 ACM Symposium on Applied Accounting*, Melbourne, Florida, USA, pp. 617-622.

[19] A.K. Sinha, “Mixing Privacy and Business Intelligence”, *BI Report*, August 2003. Available at http://www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=7268.

[20] “Financial Privacy Policies and the Need for Standardization”, *IEEE Security & Privacy*, March/April 2004, pp. 36-44.

[21] P. Ashley, C. Powers and M. Schunter, “From Privacy Promises to Privacy Management - A New Approach for Enforcing Privacy Throughout an Enterprise”, *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, September 23-26, 2002, pp. 43-50.

[22] P. Ashley, S. Hada, G. Karjoth and M. Schunter, “E-P3P Privacy Policies and Privacy Authorization”, *Proceeding of the ACM Workshop on Privacy in the Electronic Society*, Washington, DC, USA, November 21, 2002, pp. 103-109.

[23] F.A Lategan and M.S. Olivier, “On Granting Limited Access to Private Information”, *Proceedings of the tenth International Conference on the World Wide Web*, Hong Kong, Hong Kong, 2001, pp. 21-25.

[24] R. Agrawal, J. Kierna, R. Srikant, and Y. Xu, “Hippocratic Databases”, *Proceedings of the 28th VLDB Conference*, Hong Kong, China. 2002.

[25] D. Kearns, “Mostly and Issue of Trust”, *Network World Fusion*, May 17, 2004. Available at http://www.nwfusion.com/columnists/2004/0517kearns.html.

[26] T. Lau, O. Etzioni, and D.S. Weld, “Privacy Interfaces for Information Management”, *Communications of the ACM, Vol. 42, No.10*, October 1999, pp. 89-94.

[27] L. Ishitani, V. Almeida and M.JR.Wagner, “Masks: Bringing Anonymity and Personalization Together”, *IEEE Security & Privacy*, May/June 2003.

[28] A.F. Westin, “Harris-Equifax Consumer Privacy Survey 1991”, *GA:Equifax Inc*, Atlanta.

[29] R. Sullivan, “Privacy Policies and Trust”, *PromotionData.com*. February 17, 2004. Available at http://www.promotiondata.com/print.php?sid=627.

HJG Oberholzer and MS Olivier, "Privacy Contracts as an Extension of Privacy Policies," Proceedings of the International Workshop on Privacy Data Management (PDM 2005), 11-19, Tokyo, Japan, April 2005