Using Organisational Safeguards to Make Justifiable Privacy Decisions when Processing Personal Data

Martin S Olivier

Department of Computer Science,University of Pretoria, Pretoria http://mo.co.za

Abstract

Privacy-enhancing technologies can be used to enhance the privacy of individuals who interact with information processing systems. This paper considers such technologies that can be used by the organisation to safeguard personal information it processes. The paper focuses on how access control could be used to protect the individual against misuse of personal data inside the organisation. More specifically the paper considers how such a privacy-enhancing technology can make a just choice when deciding whether an access request to personal data should be allowed or not.
Access control decisions in this paper are based on the regulations that govern the interaction, the organisational policies that apply and the individual's privacy preferences.
The proposed model forms part of the organisational safeguards layer (OSL) of the Layered Privacy Architecture (LaPA) proposed earlier.
Keywords: *Personal privacy, privacy architecture, privacy-enhancing technologies*
Computing Review Categories: *K.4.1, H.2.7, H.3.5*

1 Introduction

Ever since machines were first used to store information about individuals in large databases, concerns were voiced about the possible negative impact this held for the individual's privacy [13]. In Europe and the United states this led to the introduction of laws to limit harm to the individual from the power gained by the use of such technologies [13, 8, 16].

As a modern democracy, South Africa's first step was more basic — and therefore possibly further reaching — than focussing on technology: the individual's right to privacy was guaranteed in the constitution [27, §2.14(d)] — albeit in forms that are not always easy to apply specifically to the computerised processing of individuals' data. This was supported further by the South African *Electronic Communications and Transactions Act* [28] that states in article 51 that "A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law." In addition, the South African *Regulation of Interception of Communications and Provision of Communication-related Information Act* [29] initially protects an individual (in article 2): "Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

However, once the individual has been given such rights, it soon becomes clear that the individual's rights need to be balanced by, amongst others, the interests of society [19]. In practice this means that the individual's interests need to be balanced with those of her employer, businesses with whom she interacts and the state. To illustrate, consider an example in the field of short-term insurance. If privacy rights imply that an insurer cannot investigate and identify attempted or actual insurance fraud, fraud is likely to increase and the costs of such an increase can only be borne by those who are insured. An increase in costs is, in turn, likely to lead to more fraud. And so the vicious circle continues until insurance can no longer be afforded by anyone other than the very rich. On the other hand, if a party entrusted with sensitive personal data can simply declare that the individual has no right to expect the protection of his or her data, the costs of errors on the side of the insurer, are likely to be borne by individuals. As has been argued elsewhere [5], due to the vulnerability of the individual, if errors regarding privacy are to be made, the situation should be such that the error should be in the direction of too much privacy, rather than too little privacy.

To deal with such requirements of society, laws are used to limit the extent of privacy. Perhaps the most widely known current example is the US Patriot Act that was introduced after the incidents of 11 September 2001 in New York, that limits the individual's privacy in a bid to improve the country's ability to identify possible terrorists. This law has been widely defended and criticised [5, 34].

Rather than discussing the international case further, this paper will endeavour to demonstrate the local relevance of the research described below. The South African *Electronic Communications and Transactions Act,* 2002, has already been used above as an example of an act that holds the individual's privacy in high regard. However, in

article 50(4), the effect of breach of the privacy principles referred to above ('express written consent') "are governed by the terms of any agreement between" the organisation and the individual whose information is being processed. In the case of the *Regulation of Interception of Communications and Provision of Communication-related Information Act* quoted from above, it soon becomes clear that the intention of the act is not primarily to protect the privacy of the individual, but to enable interception of messages, given certain condition. For example, already in article 5 interception is permitted "if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence." And some communications can be intercepted (article 6(2)(d)) if the organisation "has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system."

In many cases, personal privacy in Information Technology therefore becomes a matter for an agreement between the individual and those parties who process his or her personal information. Often the 'agreement' may be prescribed with the organisation with which one deals. This probably explains the clause at the bottom of the recently received schedule to the author's short term insurance contract, that essentially states that, in order to eliminate insurance fraud, the insured has *no* right to privacy [17]. (The full text of the clause is reproduced in the appendix of the paper to show the exact extent in which the insured's right to privacy is limited.) While an authoritative legal opinion is required to determine the enforceability of the clause, it will clearly — at the very least — complicate the individual's task to protect his or her privacy if any of the sensitive details about the individual ever ends up in the wrong hands by actions of the insurer, whether such actions were deliberate, negligent or accidental. Note that the insurer has details about the personal assets of the individual, as well as a detailed list of measures taken by the individual to protect such assets. This clearly constitutes sensitive personal information, that the insurer should protect as such. In fact very little policy information is actually required to limit fraud, and only then under very specific conditions. A one-sided general denunciation of privacy rights is neither necessary nor acceptable.

In a comparison between a just war and business, Rossouw [31] points out that business differs significantly from war because "business has the possibility of engaging with those who might be affected by the foreseeable negative side-effects of its actions." He continues, "when the opportunity exists of engaging with those who might be harmed by one's actions, it is morally preferable, if not imperative, to involve those affected by one's action in the process of moral deliberation."

If such deliberation is to occur when private data is processed, questions arise on how decisions should be reached, represented and enforced. Against this backdrop, the goal of the current paper is to consider the basis for making just decisions in such an environment. The question is approached by modelling the decision process mathematically to gain insight into the decision-making process on the fine-grained level of accessing individual data fields about some individual in order to process the data for some specified purpose.

The modelled solution is of a form that can be implemented as part of the organisational safeguards layer (OSL) in the Layered Privacy Architecture (LaPA) that we proposed elsewhere [20]. As such a layer it is intended to authorise (or audit) any processing of personal data; its operation should in turn be subjected to external audit to ensure that it is properly implemented by the organisation. Stated differently, suitable mechanisms and procedures should be in place to ensure that the trust placed by individuals in it is indeed warranted. However, due to space limitations, issues of trust are not considered further in the current paper.

The remainder of the paper is structured as follows. Section 2 provides more information about LaPA to explain where the proposed work fits in. Section 3 then gives more information about the OSL, develops the required model and uses the model to consider decision-making. Section 4 considers a number of issues that stem from our work and compares our work to other work that fits into the OSL. Section 5 concludes the paper.

2 Background

The Layered Privacy Architecture (LaPA) [20] positions the various technologies that may be used to protect (or enhance) the privacy of individuals when they interact with another party. The other party will typically be an organisation (but need not be); for this reason we will refer below to the *individual* and the *organisation* as the first two parties involved in the interaction. Note that our primary concern is interaction that stretches over longer periods of time — as is typically the case when an individual frequently shops at a specific shop or uses a specific airline. This is especially important if the individual subscribes to some loyalty program of the organisation, but also applies when the individual is seemingly almost anonymous: in the real world, use of a credit card may link one transaction to the next; on the Internet, an IP address or cookie may be used for the same purpose. Additionally, the architecture applies when the interaction occurs only once and only for a brief time.

The architecture is depicted in Figure 1. It consists of four layers (1–4) and identifies six viable combinations of technology (a–f). It has been shown that the four layers are fully ordered in the sense that the lower layers inform the higher layers, while the higher layers control the lower layers [20].

The remainder of this section briefly reviews exist-

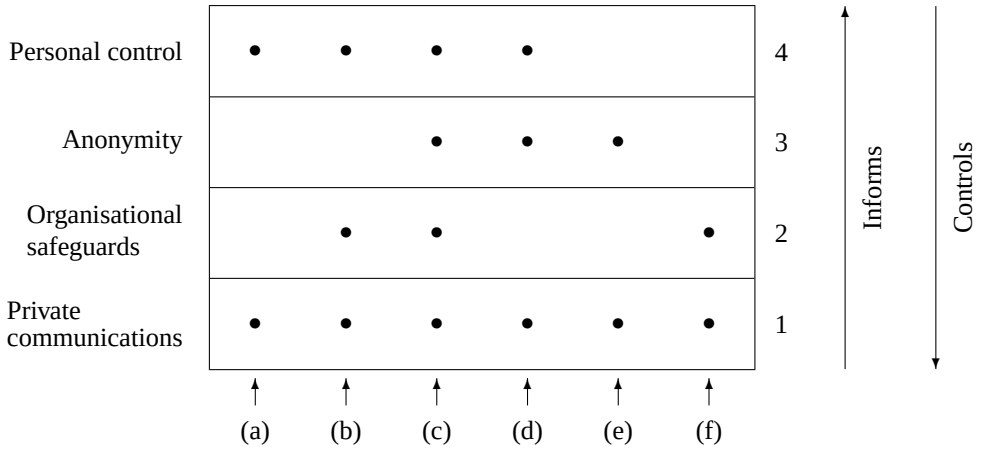

Figure 1: The Layered Privacy Architecture (LaPA)

ing privacy-enhancing technologies that fit into three of the layers of the architecture. It draws heavily on our review of the same technologies in another recent paper [20]. For alternative reviews of privacy-enhancing technologies see the OECD inventory of such technologies [18], the progress overview by Goldberg et al [10], an overview from a technical and legal perspective by Froomkin [8] or the review paper by Seničar [32].

Private communication — layer 1 of LaPA — is inherently an aspect of the right to privacy and is explicitly enshrined in the South African Constitution [27, §2.14(d)]. Encryption is clearly one well-established technology to ensure privacy of communications, with steganography currently receiving some renewed interest. Note, in addition, that private communication extends beyond the channel: The old Hush-a-Phone [33, p.4] was a mechanical device that fitted over a telephone handset to enable the 'sender' not to be overheard when talking. Rewebber (previously Janus) [30] is one technology that ensures that the user's surfing habits cannot be established from the logs that clearly falls outside the traditional communications channel.

Layer 3 of LaPA is the anonymity layer. Various schemes to ensure anonymity (or pseudonymity) have been proposed (see, for example, [26,9,4,11,30]). Most of these schemes are based on Chaum's so-called *mix* [6] — using public key encryption — or, alternatively, based on the notion of a proxy.

Personal control — LaPA's layer 4 — refers to the use of technology to ensure that an individual's personal information is only used in a manner commensurate with the individual's privacy policy. The goal is usually to compare the individual's privacy policy to that of the organisation the individual is dealing with, and only to release private information about the individual to the organisation if the two policies are compatible (or can be negotiated to a level of agreement). The best-known example in this category is P3P [25].

Organisational safeguards — layer 2 of LaPA — refer to the use of technology to ensure that the organisation complies with its own privacy policy as well as the preferences of the individual. Since the contribution made by this paper fits into layer 2, work previously done that can also be categorised in this layer will be considered in section 4 below.

3 The Organisational Safeguards Layer

The OSL contains those technologies that are used by the organisation to enhance the privacy of the individual whose information it has collected. To do this properly, this layer has to

1. Be informed about the individual's preferences;
2. Make justifiable decisions given the individual's preferences, applicable laws and regulations, and the organisation's goals;
3. Be in a position to enforce its decisions (or, at least, be in a position to notice and flag actions that are counter to its own decisions, if it cannot proactively enforce them);
4. Produce an audit trail that can be used by external parties to verify that the technology works as claimed; and
5. Communicate the four preceding abilities to individuals in a reliable manner that allows them to use this communication to make decisions about their interaction with the organisation.

This paper only considers the second of these requirements — making justifiable access control decisions.

3.1 Preferences, policies and regulations

It is clear that decisions in the OSL need a representation of the three factors on which such decisions are to be based (preferences, policy and regulation). In actual fact, the situation is somewhat more complex. Firstly, organisational

policies are not immune to change, and the version of the policy against which preferences were expressed by the individual, might not be the most recent policy. Moreover, when data is processed in an international context, multiple regulatory contexts might be applicable. Finally, given the fact that the database schema is unlikely to be forever static, the question needs to be posed to what extent an individual's preferences could be (validly) derived.

At first glance it seems that the appropriate solution to the first two problems is maintaining different versions of policies and regulations and linking each data record to the appropriate policy version and regulation. This, unfortunately, already causes a problem when a new data field is inserted in the schema: should the new data records now be dealt with according to the latest policy (even though the individual might not be aware of the existence of a new policy) or should the old policy be used (even though that policy might not cater for fields such as the new field)? This clearly demonstrates the requirement that policies should apply to data fields rather than entire data records.

On the other hand, associating each and every field with its own policy would clearly be inefficient. This is similar to an old problem in database security and is easily solved by considering the data record as a hierarchy [24]. Various policies can then be associated with different nodes in the hierarchy, and be inherited by nodes lower in the hierarchy, until inheritance is overridden by a node with which a different policy is associated.

A similar approach may be followed in the case of regulations: It is possible that new regulations only apply to data collected after a certain date. It is also possible that a regulation depends on the location where the user was when he or she supplied the data. As yet another example, a given regulation may only apply to certain categories of data. In all such cases, associating a policy with a node in the hierarchy addresses the immediate problem.

Viewing a record about an individual as a hierarchy also addresses the third problem we have alluded to: inferring a user's preferences when the schema changes. To illustrate this, consider a record where the individual can opt-in or opt-out of receiving various forms of communication from the organisation. If a new form of communication is added (and a corresponding field is added in each record, to record the individual's preferences regarding such communication), it might be possible to infer a preference for the field if the individual has already indicated a preference on a higher layer of the hierarchy: If, for example, the individual has already opted-out of receiving *any* information from the organisation, it clearly applies to the new form of communication (at least, until explicit instructions about the new form of communication are received from the individual). Does the same apply for the case where the individual has opted-in to receive communications from the organisation and a new form of communication is added? The answer depends on exactly what the individual has opted in to. If the individual opted-in to receive communications in general, the new form of communication is a special case of what has already been assented to and the preference can be inherited (until specifically modified); if the individual has, however, opted in to receive various other forms of communication, the preferences of the individual for such forms will be siblings of the preference of the individual for the new form and, as is standard practice, inheritance does not occur from siblings. The hierarchical structure of data therefore has definite implications for both the formulation of organisational policies and the expression of personal preferences. We do not discuss such implications in detail in the current paper, however.

3.2 Formalisation

Of more interest for the current discussion is the possible interaction between such various policies, preferences and regulations.

To formalise the discussion let the set of decisions that can be reached when a specific action is to be performed on an individual's data be $D = \{Y, y, N, n, uc, c, s\}$. In other words, when the question is asked whether, for example, the appropriate policy allows some specific operation to be performed on some specific data, the answer can be any one of the elements of D.

Here Y indicates a strong *yes*, while y indicates a weak *yes*. The difference between the strong and weak positive decisions will be discussed below. Similarly, N and n, respectively, denote a strong and weak *no*. uc indicates that the *user's choice* should be honoured (or obtained and then honoured). c denotes that the specific policy, regulation or user preference explicitly allows a *choice* — in other words, the policy, regulation or user preference specifies that it does not matter — as far as it is concerned — whether the operation is allowed or not. It is possible, for example, that regulations explicitly allow a user and a company to agree on a specific matter between them. Finally, s indicates that the policy, regulation or user policy is *silent* on the matter.

Next we need to consider the factors that are to be taken into account when an access request is submitted. We contend that the purpose for which the data is to be accessed is one of these factors. Let P be the set of purposes for which data can be accessed. This implies that a list of legitimate reasons are defined a priori. One may question whether it is possible to define such a set. We assume it is, based on the fact that ontologies are currently being developed in many subject areas. As one specific example, consider the ICD-10 classification system for medical diagnoses [36]. If something as complex as human health problems can be described with a finite set, it seems likely that the same can be done for valid purposes for using personal information. In the current paper we do not explore the details of P.

Let F be the set of (data) fields that the organisation stores (that is, the schema). Suppose a request is submitted to access a field $f \in F$ with purpose $p \in P$. When the purpose and field are known, we assume that it is possible to determine the access mode from this. The access mode

can be the traditional *read*, *write* and related modes; or it can be a method in an object-oriented system [22]. We therefore do not consider access mode as one of the explicit factors to be specified when requesting access.

In addition to F and P, two other factors will determine whether access should be granted or not. Clearly, whether a request should be granted or not, depends on the subject who makes the request. Let S be the set of subjects known in the system. Finally, access depends on whose information is to be accessed. There are valid reasons why a given subject $s \in S$ should (not) be allowed to access information about some specific individual [7]. Let I be the set of individuals about whom information is maintained. Note that both S and I can be structured; subjects (S) are typically structured in terms of roles, but other schemes may also be considered. Individuals could be structured in various groups; a regulation or policy may, for example, make provision for *vulnerable groups* or *children*, where the latter is a subgroup of the former. However, since this paper does not consider the detailed operation of the functions that determine whether a subject should, according to regulation or policy, (not) be allowed to access information of an individual, we do not elaborate here on such structuring.

Now suppose a subject s requests permission to access individual i's data-field f for purpose p. Represent this as the function

$$q : S \times I \times F \times P \rightarrow D - \{s\}$$

. The outcomes should be interpreted as follows:

Y, y: Allow the request. (See below for the difference between the weak and strong results.)

N, n: Deny the request. (Again, see below for the difference between the weak and strong results.)

uc: Get the individual's preference before proceeding. (See below how to deal with cases when it is not practical to (timeously) determine the individual's preference.)

c: The organisation is free to decide whether the request should be allowed or not.

The access request function q will be defined by considering three functions q_{op}, q_r, q_{ip} that will, respectively, determine what the organisational policy, regulations and the individual preference say about the request. This will be useful to model inheritance below.

In order to formally define the operation of q_{op}, q_{ip}, q_r and, eventually, q, it is useful to introduce the notion of an ancestor pair.

Definition 1 *If n is a node of a tree with a parent p, then the ancestor pair of n will be denoted by $\langle \pi, n \rangle$, where π is the ancestor pair of p. If n is the root node of a tree, its ancestor pair will be denoted by $\langle \epsilon, n \rangle$.*

Consider the set of all data fields, F, maintained in the system. Let $\mathbb{F}$ be the set of all ancestor pairs defined over the hierarchy of data field nodes.

Next we define a 'helper' function, q'_{op}, to aid in the definition of the original q_{op}. This function determines the organisational policy that applies at a sequence of nodes working up from the node towards the root, until a policy is found for the node under consideration. If a given node is *silent* on the matter, the function is applied recursively up the tree until a policy is found.

$$q'_{op} : S \times I \times \mathbb{F} \cup \{\epsilon\} \times P \rightarrow D$$

Let $s \in S, i \in I, f \in F, p \in P$. Then

$$\begin{aligned} q'_{op}(s, i, \langle a, f \rangle, p) &= q_{op}(s, i, f, p) \text{ if } q_{op}(s, i, f, p) \neq s \\ q'_{op}(s, i, \langle a, f \rangle, p) &= q'_{op}(s, i, a, p) \text{ if } q_{op}(s, i, f, p) = s \\ q'_{op}(s, i, \epsilon, p) &= s \end{aligned}$$

where $< a, f > \in \mathbb{F}$.

The intention of the definition above is to traverse the tree from the node concerned towards the root of the hierarchy until a node is found that has a policy associated with it that makes a specific statement about the request. The first such node found will be the lowest node in the hierarchy that applies to the node concerned — and hence the most specific policy applicable to the node. Note that an s result differs significantly from c: The former means that no definite answer has been found and it is therefore necessary to traverse the tree further to find an answer; the latter explicitly allows a choice that implies the decision should be based on other issues (regulation and/or individual preference).

The operation of

$$q'_r : S \times I \times \mathbb{F} \cup \{\epsilon\} \times P \rightarrow D$$

is similar to q'_{op} above, and we omit the formal definition. Also

$$q'_{ip} : S \times I \times \mathbb{F} \cup \{\epsilon\} \times P \rightarrow D - \{uc\}$$

operates in a similar manner (but clearly a result of uc is not meaningful in this case).

3.3 The consolidated decision

In order to define q (the function that yields the final answer whether access should be allowed or not in light of the applicable regulations, policies and preferences) we introduce yet another helper function, d, below. q is then defined as follows, using d.

$$\begin{aligned} q(s, i, f, p) = d\big(& q'_r(s, i, \langle a, f \rangle, p), \; q'_{op}(s, i, \langle a, f \rangle, p), \\ & q'_{ip}(s, i, \langle a, f \rangle, p) \big) \end{aligned}$$

where $\langle a, f \rangle$ is the ancestor pair for f. Clearly, the three functions determine whether the requested operation should be allowed, based on regulation, policy and individual preference, respectively. It is then the purpose of d to combine the three answers into a single answer.

To consider $d : D \times D \times D - \{uc\} \rightarrow D - \{s\}$, it is necessary to consider the $|D| \times |D| \times |D - \{uc\}| = 7 \times 7 \times 6 = 294$ individual cases. Fortunately, the majority of the individual cases are relatively easy to deal with, leaving one with a handful of special cases. All 294 cases are represented in Figure 2. The principles used to compile the tables were (1) strong regulations (Y and N) should be complied with, and (2) the user's choice is seen as relatively important — especially if the regulations indicate that user choice should form the basis of the decision. A Y entry indicates that the operation should be permitted. A y entry indicates that the operation should probably be permitted, but an argument may be made in some cases not to allow it. These are typically cases where the organisation can choose not to allow it, but in such cases the exception should be noted in the privacy policy of the organisation. An N entry indicates that the operation should not be allowed. An n entry indicates that the operation should probably not be allowed, but again with the same provisos given for the y case above. A uc entry indicates that the individual's preference should be established before proceeding. A $?$ entry indicates that the case is far from clear, and should be referred to an appropriate party for a decision. (Note that such a party may sometimes also have to make the decision when the result of the calculation is uc, but a decision is required before the individual's preference can be established.) Dealing with such special cases are considered below. A c entry indicates that the organisation is free to proceed in whichever manner it prefers in the particular case.

The simplest cases to deal with are cases such as $d(Y, Y, Y)$, $d(Y, y, y)$ or even $d(y, y, y)$. In these cases policy, preference and regulation agree, and the operation should clearly be allowed (ie Y). Similarly, if all three dimensions agree that the operation should not be allowed, N is the clear answer.

Also simple to deal with, are those prescribed by regulation. Since they are prescribed $d : N, a, b \mapsto N$ and $d : Y, a, b \mapsto Y$ for any values of a and b.

The cases where regulation prescribes that the user should have a choice are slightly more interesting. In most cases this would imply that $d : uc, a, b \mapsto b$, since the third parameter to d expresses the user's preference. However, care should be taken in a number of cases: If the user has not yet expressed a choice (ie $b = s$) d should indicate this (ie $d : uc, a, s \mapsto uc$), so that the user will be given an opportunity to express a choice. (See the meaning of uc in the definition of q above.) There are also the cases where the user has allowed a choice; in these cases the user has allowed the policy to apply even though regulation gives the user a choice. Therefore, in general, $d : uc, a, c \mapsto a'$, where a' is the most appropriate equivalent to a in the range of q.

Next, consider cases where one of the parties allows a choice (c) or is silent on the matter (s). In general, these cases are easy to deal with, as long as there is not a strong disagreement between the remaining two parties. In other words, if the two remaining parties prefer Y and y, respectively, the result of d will be Y. If the two remaining parties prefer Y and n, the stronger preference will override the weaker preference; in this case the result of d will be Y. If one of the remaining parties also allows a choice (c) or is silent on the issue (s) the other party's preference will determine the final result.

The cases discussed above are mostly straightforward to deal with. However, when parties disagree (for example, Y versus N), or the user should have expressed a preference, but has not (yet), or all parties are silent (s), are more difficult to deal with — and will potentially lead to different answers in different contexts. Some of these special cases are discussed next.

3.4 Special cases

As one of the special cases, consider $d(n, N, Y)$. Here regulation expresses a bias towards a negative response, policy expresses a definite negative response, but the individual has indicated a strong positive preference. In the majority of cases this is likely to indicate an incompatibility between the organisation's and the individual's goals. If that is indeed the case (and both parties have reconsidered their positions on the specific case) it probably indicates that ties between the individual and the organisation should be severed. The issue becomes more tricky if the ties cannot easily be severed, for example when the individual is forced by law to be connected with the organisation (as is the case with the national income tax authority) or if the organisation has a monopoly for the service(s) it offers. In such cases the long term solution for the issue is for the organisation to lobby to get regulations changed (to strong support) to override the individual's preference. At the same time the individual can try to garner support for his or her position and put pressure on the organisation to change its policy.[1] The individual can also attempt to get the regulatory authority to change the applicable regulation, but in this specific case this is unlikely since the authority has already expressed a negative bias. (Clearly lobbying and garnering support could also be considered when the organisation is only one of a series of providers of a service — but in such a case one at least has the option of choosing another service provider. Lobbying and garnering support should also be considered when all organisations in a given sector have the same policy in some respect.) The question, however, remains how should the issue be dealt with until the regulation and/or policy is changed or the ties between the individual and the organisation have been severed. Clearly, ignoring the individual's strong preference could render the individual vulnerable. On the other hand, going against the organisation's strong policy may prevent the organisation from protecting its legitimate interests. (It

[1] When expecting the individual to garner support for his or her privacy position, one should remember Jung's [14, p.78] warning about collective means to support individual positions: "Anxiously we look round for collective measures, thereby reinforcing the very mass-mindedness we want to fight against. There is only one remedy for the levelling effect of all collective measures, and that is to emphasize and increase the value of the individual."

$q_{ip}(s,i,f,p) = Y$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	Y	Y	?	Y	Y	Y	Y
N	N	N	N	N	N	N	N
n	Y	Y	?	n	Y	Y	Y
uc	Y	Y	y	Y	Y	Y	Y
c	Y	Y	?	Y	Y	Y	Y
s	Y	Y	?	Y	Y	Y	Y

$q_{ip}(s,i,f,p) = y$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	Y	Y	N	y	Y	Y	Y
N	N	N	N	N	N	N	N
n	Y	Y	N	N	Y	Y	Y
uc	Y	Y	?	Y	Y	Y	Y
c	Y	Y	N	y	Y	Y	Y
s	Y	Y	N	y	Y	Y	Y

$q_{ip}(s,i,f,p) = N$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	?	N	N	N	N	N	N
N	N	N	N	N	N	N	N
n	?	N	N	N	N	N	N
uc	n	N	N	N	N	N	N
c	?	N	N	N	N	N	N
s	N	N	N	N	N	N	N

$q_{ip}(s,i,f,p) = n$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	Y	y	N	N	N	N	N
N	N	N	N	N	N	N	N
n	N	N	N	N	N	N	N
uc	?	N	N	N	N	N	N
c	Y	n	N	N	N	N	N
s	Y	n	N	N	N	N	N

$q_{ip}(s,i,f,p) = c$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	Y	Y	n	c	Y	Y	Y
N	N	N	N	N	N	N	N
n	y	c	N	N	N	N	N
uc	Y	Y	N	N	c	c	c
c	Y	Y	N	N	c	c	c
s	Y	Y	N	N	c	c	c

$q_{ip}(s,i,f,p) = s$

Regulation \ Policy	Y	y	N	n	uc	c	s
Y	Y	Y	Y	Y	Y	Y	Y
y	Y	Y	n	?	uc	y	uc
N	N	N	N	N	N	N	N
n	y	?	N	N	uc	N	uc
uc	uc	uc	uc	uc	uc	uc	uc
c	Y	y	N	n	uc	uc	uc
s	y	uc	n	uc	uc	uc	uc

Figure 2: The values of d.

is possible that the individual has expressed a strong preference in opposition to the organisation's policy to protect his or her privacy; it is also possible that this strong opposition is a bid by the individual to mislead the organisation or even to commit fraud. Similarly, the organisational policy might be strong to protect its legitimate interests, or it might simply be caused by a profit motive. If the organisation and the individual continue to disagree on this point, neither of them would be able to arbitrate the matter.) The prudent approach for such cases is the appointment of a privacy ombudsman (by the appropriate regulatory authority) to whom such cases can be referred.

Other cases that pose problems similar to that discussed in the previous paragraph include $d(y, N, Y)$, $d(c, N, Y)$, $d(s, N, Y)$, $d(uc, N, y)$, $d(y, Y, N)$, and others.

Referring cases where the individual has not yet expressed an opinion (for example $d(uc, Y, s)$) can, in some cases, also offer a solution. In the given example, regulation states that user choice should determine the decision. If it is impractical to obtain the individual's preference (such as when contact with the individual has been lost), arbitration by the ombudsman could be the only alternative.

In the case of $d(y, n, s)$ the situation is somewhat different. Here strong indicators are absent. One possibility is to accept the regulatory positive bias. Another possibility is to clearly state that the particular case is a policy exception — ie, whereas the policy is normally n, when the individual preference is s, the policy becomes N, leading to an answer without the aid of parties outside the organisation. A third possibility is referring the matter to the ombudsman. Clearly the best alternative is to establish the individual's preference.

While not ideal in all respects, the second alternative (using a policy exception to determine the decision within the organisation) provides a practical solution to another problem inherent in the proposed approach: the effort and cost (and, in general, the viability) associated with achieving the preference of the individual for each and every purpose for which a data field could be accessed could be prohibitively high. Using this alternative could be a cost-effective way of dealing with many day-to-day operations. The requirement that the case should be published as a policy exception is one aspect that justifies such an approach. If it is published, it should be communicated as part of the privacy negotiations when the personal control layer (such as P3P) is offered options. Further justification lies in the fact that, if a given situation is exploited by organisations, the regulatory authority has the option of changing the regulation to Y, N, or uc to force the organisation to deal with the matter differently. Note that policy exceptions could be highly specific: there are no reasons why an exception cannot be published for specific values (or sets) of s (subject), i (individual), f (data field) or p (purpose) — although exceptions for specific values of i should be questioned.

4 Discussion

This section considers a number of aspects that need to be addressed before the paper can be concluded. Specifically, we need to consider possible alternatives to the d that was specified in Figure 2; we also need to consider the remarks in the previous section that policies and regulations are actually forests, rather than one permanent document each; finally the work needs to be compared to other work that fits on the OSL.

To what extent is the definition of d in Figure 2 set in stone? While it was argued that in most cases the value of d is obvious, given the principles, it is very likely that another party may come to a different decision for a specific case. There are two ways to deal with such variations. The first is to accept the definition in Figure 2 as the baseline, and simply treat (and publish) specific differences as policy exceptions. Another alternative is to enumerate meaningful definitions of d, with the definition in Figure 2 referred to as, say, Possibility-1. If such names are assigned by the ombudsman, a simple name would uniquely define the scheme used by a particular organisation. Since not too many variations are likely, enumeration should not present serious problems.

In the previous section it was pointed out that policies and regulations are typically forests. The strategy described in the previous section explicitly traversed the data hierarchy until an applicable policy or regulation is found. The question is whether the policy (or regulation) hierarchy should be traversed before or after (or even simultaneous with) traversing the data hierarchy. We contend that, when traversing the data hierarchy and a node is found that is associated with a policy (or regulation) the policy (or regulation) hierarchy should be traversed at that point. If an appropriate policy (or regulation) is found, the traversal stops and the policy (or regulation) decision is determinable. If no appropriate match is found in the policy (or regulation) hierarchy, traversal of the data hierarchy proceeds. The process continues until a match is found during the traversals, or the root of the data hierarchy is reached. If this happens without a match, the decision is s (silent). The logic behind this order is that children nodes in policy (and regulation) hierarchies represent amendments to the parent nodes. If an amendment is associated with some data item, it is logical that the amended policy should also apply (with proper application of the amendments). If P' amends policy P, but individual i has previously agreed to policy Q', one either has to get i to agree to both P and P', or produce an amendment Q' that applies to i's policy, or produce a new policy R and get i to accept R, or to let i continue under Q. Therefore policy (and regulation) traversal is merely intended to find the appropriate item in a sequence of policy (or regulation) amendments. Hence traversal has to happen at the data node that identifies the policy (or regulation).

Finally, we have to compare the work of the previous section to other work that deals with organisational safeguards.

Agrawal et al [1] use the analogy of the Hippocratic oath to explain how databases should treat private data entrusted to them. A set of principles is identified that such a database should adhere to. These principles are then translated to a 'strawman' design. Similar to our approach, purpose for which data was collected plays a central role and is used to label all database fields, but no hierarchical ordering of fields (and hence no inheritance) is assumed. A validator is used to compare the organisation's policy and the individual's preferences. (Regulations are not explicitly considered.) Details of the decision process (the heart of the current paper) are not given, but it seems that individual preferences always take precedence. The paper raises many relevant questions that still need to be answered.

Despite these differences, our work is fundamentally compatible with the notion of a Hippocratic database: It can form a significant part of the Record Access Control component of the Hippocratic database strawman design [1], where access decisions to records are made in such a database.

E-P3P [15, 2] uses P3P as its analogy, but focuses on using technology to backup the policy presented to the user. While an architecture to implement this functionality is presented, the major emphasis is the presentation of a comprehensive language that can be used to represent appropriate privacy policies, with a formal semantics for the language. Similar to our approach, policies are associated with data on a 'per-person and per-record basis' — something that Karjoth et al [15] refer to as a *sticky policy paradigm*. Policies are, however, not associated with nodes as such, but with data categories (such as *financial data* and where the data categories form a hierarchy). While using data categories is inherently different from using the instantiated structure of the data as we have done, both approaches have their advantages and disadvantages, which are not discussed further in this paper.

Apart from the different major goals, the most significant difference between E-P3P and our approach is the manner in which policies, regulations and preferences are combined to make decisions. In our approach the three factors are orthogonal. In E-P3P, regulations are considered, but play no direct role (as was the case for Hippocratic databases). Personal preferences in E-P3P only become relevant where the policy allows the individual explicit options; based on the individual's choice, the policy then allows or disallows an access request. While this approach simplifies matters, it suffers from two drawbacks:

1. If policies are based on regulation and regulation changes, the policies need to be updated. Since this is orthogonal in our approach, just the policies need to be updated. Furthermore, our model caters for different policies to apply to different data elements, and for replacement of regulations on parts of the data hierarchy (which will be useful if a new regulation applies to data collected after a certain date, for example).

2. If a user expresses a preference for an aspect that the organisational policy does not explicitly cater for, our approach will be able to deal with it, while E-P3P will require the organisation to ignore the individual's preference or to change its policy. (Note that our approach does not require the organisation to invite individual preferences for all data stored, but it does cater for cases where individuals on their own initiative express preferences.)

In the case of inconsistent rules in E-P3P, the request is rejected. (We contend that rejection is not always to the individual's benefit: Suppose that permission is sought from a user to sell his or her address to a mailing list; if the request to notify the user is denied due to inconsistent rules, but the sale proceeds, the user is denied making the final decision.) An interesting facet of the presentation of E-P3P is the explicit distinction that is made between (security) access control and privacy (access) control.

Another interesting facet of E-P3P is support for obligations: accessing private data is not merely a matter of allowing or preventing access; accessing personal information may oblige the accessor to perform some action.

The OSL has also seen some initiatives on the business front. IBM's Tivoli Privacy Manager [35] uses P3P as basis and associates P3P preferences with data at the collection point. Policies are then enforced when data is accessed, and an audit trail is created. PrivacyRight [23] argues that letting the individual control the use of personal information in the organisation's database makes economic sense. Their TrustFilter permissions management system enables consumers to verify the integrity of their data and record permissions for the use of their data. The PrivacyWall family of products [12] enables organisations to monitor and audit compliance of their web practices with their privacy policies.

Note that trust seals (such as TRUSTe [3]) provide some of the listed requirements of the OSL listed earlier (see item 5 in section 3). However, we contend that privacy seals will be able to offer much more specific guarantees if the details of the OSL are fully developed and implemented.

5 Conclusion

This paper extended the LaPA privacy architecture [20] by considering how just privacy decisions should be made on the OSL. This was done by modelling the appropriate aspects on that layer and by considering the various scenarios that can occur. It was shown that most cases are not complex to deal with, and strategies for dealing with complex cases were suggested.

As noted in section 3, decision-making is just one aspect of the requirements to build a comprehensive OSL. The remaining aspects identified in section 3 are left for further research.

Other aspects that have been identified for future research include a study of the implications of the data structure on the formulation of policies and personal preferences, the establishment of an ontology of reasons (or

purposes) why access to data may be required, and trust through auditing (or other means) of the decision-making process presented in this paper.

Appendix

This appendix contains the full text of the insurance policy clause [17] referred to in the introduction of this paper. The clause is quoted verbatim, as received, in Afrikaans, to avoid changing meaning when translating.[2] Note that the emphasis in the final statement does not occur in the original. Since that statement forms the crux of the matter, the English translation of that statement is given after the quotation for the benefit of those readers who do not understand Afrikaans.

> **Uitruil van Inligting**
>
> "Die Polishouer erken dat die uitruil van eise- en onderskrywingsinligting (met inbegrip van kredietinligting) deur Versekeraars noodsaaklik is om die versekeringsbedryf in staat te stel om polisse behoorlik te onderskryf en risiko regverdig te evalueer en om in openbare belang en met die doel om premies te beperk, die voorkoms van bedrieglike eise te verminder. Die Polishouer doen hiermee namens homself en namens enige persoon wat hy hierin verteenwoordig afstand van enige reg op privaatheid van enige eise-inligting wat deur hom of namens hom verskaf is ten opsigte van enige versekeringseis deur hom ingestel en verleen hiermee toestemming dat sodanige inligting aan enige ander versekeringsmaatskappy of sy agent geopenbaar mag word. Die Polishouer erken ook dat die inligting deur hom verskaf deur enige ander wettige bronne of databasisse gestaaf kan word. *Die Polishouer doen hiermee afstand van enige reg op privaatheid en verleen toestemming dat enige inligting van toepassing op enige versekeringspolis of -eis wat op hom betrekking het, geopenbaar mag word.*"

"The Policy Holder herewith waves any right to privacy and grants permission that any information applicable to any insurance policy or claim relating to him may be disclosed."

References

[1] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippocratic databases. In *28th Int'l Conf. on Very Large Databases (VLDB), Hong Kong*, 2002.

[2] Paul Ashley, Satoshi Hada, Günter Karjoth, and Matthias Schunter. E-P3P privacy policies and privacy authorization. In *Proceedings of the ACM workshop on Privacy in the Electronic Society*, pages 103–109. ACM Press, 2003.

[3] Paola Benassi. TRUSTe: an online privacy seal program. *Communications of the ACM*, 42(2):56–59, 1999.

[4] Michael A Caloyannides. Encryption wars: Shifting tactics. *IEEE Spectrum*, 37(5):46–51, 2000.

[5] David Chadwick, Martin S Olivier, Pierangela Samarati, Eleanor Sharpston, and Bhavani Thuraishingham. Privacy and civil liberties. In Ehud Gudes and Sujeet Shenoi, editors, *Research Directions in Database and Application Security*, pages 331–346. Kluwer, 2003.

[6] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[7] Lucas C J Dreyer and Martin S Olivier. An information-flow model for privacy (InfoPriv). In Sushil Jajodia, editor, *Database Security XII: Status and Prospects*, pages 77–90. Kluwer, 1999.

[8] A. Michael Froomkin. Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases. *University of Pittsburgh Journal of Law and Commerce*, 395(15), 1996. `http://www.law.miami.edu/~froomkin/articles/oceanno.htm`.

[9] Eran Gabber, Phillip B Gibbons, David M Kristol, Yossi Matias, and Alain Mayer. Consistent, yet anonymous, web access with LPWA. *Communications of the ACM*, 42(2):42–47, February 1999.

[10] Ian Goldberg, David Wagner, and Eric A Brewer. Privacy-enhancing technologies for the Internet. In *IEEE COMPCON '97*, pages 103–109. IEEE, February 1997.

[11] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Onion routing. *Communications of the ACM*, 42(2):39–41, February 1999.

[12] IDcide. IDcide introduces corporate privacy compliance software. Press release, February 2001. `http://www.idcide.com/pages/press_releas.htm#6`.

[13] Deborah G Johnson. *Computer Ethics*. Prentice Hall, third edition, 2001.

[14] Carl Gustav Jung. *Flying Saucers — A modern myth of things seen in the sky*. Routledge, 2002.

[15] Günter Karjoth, Matthias Schunter, and Michael Waidner. Platform for Enterprise Privacy Practices: Privacy-enabled management of customer data. In

[2] The fact that the clause was communicated to the author in his home language is to be commended; too often such important information is communicated to individuals in a language they have not fully mastered.

Roger Dingledine and Paul Syverson, editors, *Privacy Enhancing Technologies: Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002, Revised Papers*. Springer, 2003.

[16] Jeff Langenderfer and Don Lloyd Cook. Oh, what a tangled web we weave — the state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research*, 57(7):734–747, 2004.

[17] Multinet Makelaars. Versekeringskedule. Persoonlike korrespondensie, 24 Februarie 2003.

[18] OECD. Inventory of privacy-enhancing technologies (PETs). Report DSTI/ICCP/REG(2001)1/FINAL, Working Party on Information Security and Privacy, Organisation for Economic Co-operation and Development, 2002.

[19] Martin S Olivier. Database privacy. *SIGKDD Explorations*, 4(2):20–27, 2003.

[20] Martin S Olivier. A layered architecture for privacy-enhancing technologies. In Jan H P Eloff, Hein S Venter, Les Labuschagne, and Mariki M Eloff, editors, *Proceedings of the Third Annual Information Security South Africa Conference (ISSA2003)*, pages 113–126, Sandton, South Africa, July 2003. Journal version also published [21].

[21] Martin S Olivier. A layered architecture for privacy-enhancing technologies. *South African Computer Journal*, 31:53–61, 2003.

[22] Martin S Olivier and Sebastiaan H von Solms. A taxonomy for secure object-oriented databases. *ACM Transactions on Database Systems*, 19(1):3–46, 1994.

[23] PrivacyRight. Control of personal information — the economic benefits of adopting an enterprise-wide permissions management platform. White Paper, 2001. `http://www.privacyright.com/info/economic.html`.

[24] Fausto Rabitti, Elisa Bertino, Won Kim, and Darrell Woelk. A model of authorization for next-generation database systems. *ACM Transactions on Database Systems*, 16(1):88–131, 1991.

[25] Joseph Reagle and Lorrie Faith Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2):48–55, February 1999.

[26] Michael K Reiter and Aviel D Rubin. Anonymous web transactions with Crowds. *Communications of the ACM*, 42(2):32–48, February 1999.

[27] Constitution of the Republic of South Africa, 1996. Act 108 of 1996.

[28] Republic of South Africa, Electronic communications and transactions act, 2002. Act 25 of 2002.

[29] Republic of South Africa, Regulation of interception of communications and provision of communication-related information act, 2002. Act 70 of 2002.

[30] Andreas Rieke and Thomas Demuth. JANUS: Server anonymity in the world-wide web. In U E Gattiker, editor, *Conference Proceedings EICAR International Conference*, pages 195–208, 2001.

[31] Gedeon Joshua Rossouw. Business is not just war — transferring the principle of double effect from war to business. *South African Journal of Philosophy*, 22(3):236–246, 2003.

[32] Vanja Seničar, Borka Jerman-Blažič, and Tomaž Klobučar. Privacy-enhancing technologies — approaches and development. *Computer Standards & Interfaces*, 25:147–158, 2003.

[33] David A Stamper. *Business Data Communications*. Benjamin/Cummings, fourth edition, 1994.

[34] Peter Swire and Lauren Steinfeld. Security and privacy after September 11: the health care example. In *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy*, pages 1–13. ACM Press, 2002.

[35] Tivoli Software. Enable your applications for privacy with IBM Tivoli Privacy Manager for e-business. Technical discussion, IBM, July 2002.

[36] World Health Organisation. The international statistical classification of diseases and related health problems, tenth revision (web page), 2002. `http://www.who.int/whosis/icd10/`.

M. S. Olivier, "Using organisational safeguards to make justifiable decisions when processing personal data," *South African Computer Journal*, **33**, 78–88, 2004.