Defining Consent and Revocation Policies

Ioannis Agrafiotis, Sadie Creese,
Michael Goldsmith, Nick Papanikolaou
International Digital Laboratory
University of Warwick
Coventry, UK
E-mail: {I.Agrafiotis, S.Creese,
M.H.Goldsmith, N.Papanikolaou}@warwick.ac.uk

Marco Casassa Mont, Siani Pearson
Systems Security Lab
HP Labs
Bristol, UK
E-mail: {marco.casassa-mont, siani.pearson}@hp.com

Abstract— **In this paper we present the notion of a *consent and revocation policy*, as it has been defined within the context of the EnCoRe project. A consent and revocation policy is different to a privacy policy in that it defines not enterprise practices with regards to personal data, but more specifically, for each item of personal data held by an enterprise, what consent preferences a user may express and to what degree, and in what ways he or she can revoke their personal data. This builds on earlier work on defining the different forms of revocation for personal data, and on formal models of consent and revocation processes.**

Keywords - privacy policies, policy hierarchy, policy refinement, conceptual model

I. INTRODUCTION

Alan Westin has advanced a view of privacy as control over one's personal information [1]. In this view, an individual has privacy if he or she can exercise control over the use and flow of such data in society. Actual control over personal data shared by individuals today, especially over the Internet, is significantly lacking even though there exist laws and regulations in which such control is enshrined as a basic right. We take the view that control over personal data in our modern society amounts to two things: (a) having at one's disposal technical means of giving and withdrawing consent for specific uses of personal data by any party interested in that data, and (b) having mechanisms that enforce such consent or non-consent in every instance of data use. Implementing suitable mechanisms of *revocation* for personal data poses particular challenges (where revocation is understood most generally as a change of consent, namely, a partial or complete withdrawal of consent), both technological and legal, which have yet to be fully met.

All modern enterprises rely, in various ways, on collection and processing of personal data about their customers. However, a recent rise in identity theft and other related crimes has made people increasingly aware of the perils of sharing personal data, and enterprises are now required to develop and disclose detailed privacy policies. While privacy policies mostly describe an enterprise's personal data handling practices, there is no commonly accepted way of stating clearly to customers whether (and which) mechanisms for granting and revoking consent for personal data are provided. In other words, what is desirable is a description of exactly which *controls* an enterprise provides to its customers. In this paper we call such a description a *consent and revocation policy*.

There is good reason for consent and revocation policies to be expressed in a machine-readable form, in a manner analogous to website privacy policies [4, 5], for then enforcement can be fully automated; our aim here is not to define the syntax of such policies, rather their structure and general characteristics. The development of enforcement mechanisms for consent and revocation is the object of the EnCoRe project [2, 3].

In particular, EnCoRe is exploring and providing deliverables about how to handle consent and revocation policies in three key areas affecting people: enterprise data management, biobanks and assisted living.

Consent and revocation appear in many different forms, and the relationship between the two concepts is rather subtle. For instance, they are not symmetric: it is possible for an individual to revoke personal data for which consent has not been given (in Section III we will refer to this as *consentless revocation*). Consent itself is not a simple yes/no ("store this data" or "do not store this data"), but has many subtly different gradations, depending on the type of data it refers to.

In Section II we provide an overview of how consent and revocation, along with related policies, are perceived by the main stakeholders i.e. organisations, data subjects (end-users) and the regulators. In Section III we define the notion of a consent variable, which is an attempt to quantify consent in terms of its constituent parts, while in Section IV we review the different forms of revocation, as identified in earlier work [6]. These elements come together in Section V, where we define consent and revocation policies. The final section describes future work and concludes.

II. How Consent and Revocation are Perceived by Different Stakeholders

This section provides an informal overview of how the concepts of consent and revocation (and related policies) are perceived and dealt with by the key stakeholders, notably organisations, data subjects and regulators. The remaining part of the paper will then primarily focus on the data subjects' perspective.

Conceptually there are several layers of abstraction of policies, ranging from human readable high-level policies to semi-formal representations (which are actionable by humans while also being translatable into operational policies), to machine-readable policies that are not usually intended to be exposed to users.

This also applies to consent and revocation policies, which specifically deal with the handling of personal and confidential data based on privacy preferences and constraints driven by data subjects and legislation.

Different stakeholders have different priorities and views of consent and revocation, as described below.

A. Organisations

Organisations have a pragmatic view about consent and revocation. Incorporating these processes into their business practices requires effort and investment, esp. to provide necessary enforcement mechanisms; also potential liabilities, in case of failures, are introduced.

Because of this, it is common practice that these policies are represented in the form of opt-in or opt-out choices for end users – as these are simple to handle and not requiring complex enforcement mechanisms.

In addition, consent and revocation policies are just a small part of the overall set of policies organisations need to take into account, for example business policies, security policies, compliance policies, etc.

Current legislation enables organisations, in some circumstances, to bypass the need to obtain consent (and revocation) from end-users, based on "fair usage".

Of course organisations need to take into account the trade-off between carrying on with the current minimalistic data management practice and the increasing interest and willingness of end-users to obtain control over their data.

The EnCoRe project is exploring how to ease the pain in dealing with consent and revocation management and the enforcement of related policies hence hoping to shift organisational behaviour towards a more privacy-friendly approach

B. Data Subjects (End-Users)

From the point of view of a data subject, or end-user, if an enterprise provides consent and revocation controls, it increases that user's *choice* regarding how his or her personal

data is handled. We are interested here in the point of view of the end-user, and in Section V we argue that an enterprise can define its own consent and revocation policy, as a way of informing end-users of the choices available to them.

C. Regulators

Regulators have been very active in providing laws and legislation concerned with the management (collection, processing and disclosure) of personal data. Laws are usually abstract and primarily focus on the circumstances in which consent might be necessary. On the other hand the concept of revocation is fuzzy and not properly addressed.

As a consequence, policies that derive from these laws and legislation do not properly address these aspects and in particular meeting the expectations of the end-users

The work carried out in EnCoRe, described in this paper, aims at providing a detailed description of the concept of consent and revocation and how they can be pragmatically dealt with by technical means.

III. Forms of Consent and the Notion of a Consent Variable

With regard to his or her personal data, there are four principal things for which an enterprise or other data collector requires the consent of an end-user:

- **collection** of data,
- **processing** of data,
- **sharing** of data.

Collection of data refers to the initial process by which data is acquired and stored on the enterprise's information system. Processing includes any access of the data that has been collected and is characterised by a *stated purpose* (e.g. research, marketing, aggregation to derive average customer habits). Data may be shared – internally and externally (e.g. to third parties) so that it can be processed, often elsewhere than the site of data collection.

Thus, consent may be defined as a wish for a datum d to be collected, processed, shared, or any combination of the above. This definition is too coarse, however, for it does not account for subtleties such as these:

- It may be desired to restrict data collection so that it occurs only in one country, so that it is subject to that country's privacy legislation.
- It may be desired that consent lasts for only a fixed period of time.
- It may be desired to restrict processing of data so that it is used for only certain stated purposes.
- It may be desired that the data is shared with only particular parties, and to banish uses of the data by others.

Thus we claim that consent is parameterised by certain quantities referred to as *consent variables*. As examples we

consider: time t for which consent is granted, volume v of data for which consent is granted, the set S of allowed purposes (stated purposes for which consent is granted), the set Π of parties who may access the data.

Thus, consent is fully determined when there are specified:

- the **task** for which consent is given (collection, processing, sharing, or any combination thereof)
- for this task, the **values of the consent variables** of interest.

From this one can extract a mathematical definition of consent and develop a hierarchy of its different forms. Formal models of consent and the attendant logic are addressed in our other work [7].

IV. FORMS OF REVOCATION

Revocation corresponds to the withholding or withdrawal of consent. It is manifested in its simplest form as deletion of data, although there are many variations of revocation, as listed below (from [6]):

1. **No Revocation At All:** Personal data remains static, and once it has been disclosed, it is either physically impossible to revoke (how could ever revoke reputation) or prohibited for various reasons (e.g. law-enforcement, data from police's DNA database).

2. **Deletion:** Data are completely erased and cannot be retrieved or reconstituted in any way.

3. **Revocation of Permissions to Process Data:** Data subjects withdraw consent that would enable an enterprise to process or analyse their personal data for a specified purpose.

4. **Revocation of Permissions for Third Party Dissemination:** Data subjects withdraw consent that would enable an enterprise to disclose information to a third party.

5. **Cascading Revocation** is a variation on any of the above kinds of revocation, whereby the revocation is (recursively) passed on to any party to whom the data has been disclosed. Through this mechanism, data subjects are able to revoke data by only contacting the enterprise that they disclosed their data to originally.

6. **Consentless Revocation:** Personal data for whose storage and dissemination no consent has been explicitly given by the user, but which may need to be revoked. Again, any of the fundamental types of revocation may be invoked. The need to revoke consentless data emerges mainly when a breach in privacy has occurred. In the italics below we describe a characteristic example of consentless revocation.

7. **Delegated Revocation:** This is a kind of revocation which is exercised by a person other than the individual concerned, such as an inheritor or parent/guardian.

8. **Revocation of Identity (Anonymisation):** Data subjects may be happy for personal data to be held for certain purposes so long as it is not linkable back to them personally. Anonymisation may be regarded as a variant of revocation, in that data subjects request a change to data held so that it is no longer personally identifiable.

These forms of revocation should be available as actions that individuals can perform on personal data held about them by an enterprise.

V. DEFINING CONSENT AND REVOCATION POLICIES

Having considered the many different forms and variations of consent and revocation, we are in a position to define the notion of a consent and revocation policy, whose purpose is to enable an enterprise to inform customers of:

a) what consent is required of them for each data field, and
b) which revocation types are available to them should they wish to exercise control over their personal data.

Thus, a consent and revocation policy is defined over a set of data $D = \{\delta_i\}$ as a set of tuples

$$\{\forall i: (c_i, p_i, d_i, R_i)\}$$

where the c_i, p_i, d_i define together a value of consent (specifying collection, processing and dissemination rights respectively), and R_i is a set consisting of the names of allowed revocation types.

As an example, consider this policy over $D = \{\delta_1, \delta_2\}$:

$$\{ (c(30 \text{ days}), -, d(10 \text{ days}), \{2,3\}),$$
$$(-, p(10 \text{ days}), -, \{2\}) \}$$

What this policy specifies, assuming the only consent variable of interest is the time for which data is held, is that consent is required to enable the collection of δ_1 for 30 days and its dissemination for 10 days; furthermore, δ_1 can be revoked using revocation types 2 (deletion) and 3 (revocation of permissions to process data) (see Section III). The example policy also states that consent to process δ_2 for 10 days is required, and that deletion may be performed.

Note that the symbol $-$ is used when one of the c_i, p_i, d_i is omitted. Some further formalisation work is needed to make the definitions more rigorous, but we believe that the above presentation is sufficient for our purposes here.

An enterprise is likely to require stipulations on the minimum consent a customer can provide for each data field. In other words, rather than stating in a policy specific consent values that an enterprise needs from a customer, it may be desirable to specify a *range* of values. We regard this as a direction for further investigation.

Automatically enforcing such a policy involves obtaining specific consent from customers through some user interface, and implementing suitable controls corresponding to the revocation types in an enterprise's information system. Such work is being carried out within the EnCoRe project, in particular for case studies involving personal data held by one's employer, and for data held in biobanks.

VI. CONCLUSIONS AND FUTURE WORK

We have in this paper explained the significance of consent and revocation preferences for personal data, and introduced the notion of a consent and revocation policy. We have described in detail the different aspects of the notions of consent and revocation respectively, and explained how an enterprise can define policies that make clear what options are available to a customer in terms of controlling his or her personal data.

There is much further work to be done on consent and revocation policies, most notably refining the definition of the R_i, so that the revocation types include parameters analogous to consent variables. In practical terms, we expect to link consent and revocation policies to a real-world access control language, such as XACML, so that enforcement of consent and revocation can be done programmatically. There are also considerations to do with the internal consistency of such policies, such as preventing conflicts or incompatibilities between the consent requested and the revocation types made available.

We believe that it is essential to incorporate consent and revocation controls in enterprise information systems that handle personal data, and that the deployment of consent and revocation policies across such systems is a useful means of ensuring that the privacy preferences of individuals will be respected.

REFERENCES

[1] Alan Westin (1967). *Privacy and Freedom*. New York: Athenaeum.

[2] Marco Casassa Mont, Siani Pearson, Gina Kounga, Yun Shen, and Pete Bramhall (2009). *On the Management of Consent and Revocation in Enterprises: Setting the Context.* Technical Report HPL-2009-49, HP Labs, Bristol.

[3] EnCoRe. http://www.encore-project.info.

[4] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. M. Reagle, M. Schunter, D. A. Stampley, and R. Wenning (2006). *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification.* World Wide Web Consortium Note NOTEP3P11-20061113.

[5] OASIS eXtensible Access Control Markup Language (XACML). Standard available from http://www.oasisopen.org/.

[6] Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, and Nikolaos Papanikolaou (2009). *Reaching for Informed Revocation: Shutting Off the Tap on Personal Data*, Proceedings of Fifth International Summer School on Privacy and Identity Management for Life, Nice, France, 7th – 11th September 2009.

[7] Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, Nick Papanikolaou (2010). *The Logic of Consent and Revocation*. Submitted.