On the Need to Explicitly Manage Privacy Obligation Policies as Part of Good Data Handling Practices

Marco Casassa Mont
Hewlett-Packard Labs, Bristol, UK
marco.casassa-mont@hp.com

Abstract

Nowadays, people have to disclose their personal data to enterprises (and other organisations) in order to access web services and engage in business interactions. This practice is not going to disappear in the foreseeable future. It is of paramount importance, in order for them to participate confidently in the digital world, that their personal data is managed according to their privacy preferences, privacy laws and best practices. It is not only a matter of privacy-aware access control. We argue that privacy obligations, dictating duties and expectations on how personal data should be handled, need to be explicitly managed – in a complementary way (i.e., not subordinated) to access control. They need to be explicitly represented in a suitable language, as part of a broader data handling context. Compatibility with current privacy-aware languages and frameworks must be preserved. The standardisation of this language is also important to enable interoperability during the exchange of personal data and associated policies. This position paper aims at creating awareness of the "privacy obligation" aspect, analyses the current situation, highlights related requirements and proposes ways to move forwards.

1. Position Statement

The purpose of this position paper is to make the case for the explicit management of privacy "obligation" policies [2] within enterprises (and other organisations), as part of good data handling practices. Privacy obligations describe privacy duties and expectations (defined by data subjects and administrators) on how personal data should be handled: they enable privacy-aware information lifecycle management. In this context, privacy obligations are complementary to access control policies and part of data handling policies. Current limitations, due to the subordination of obligation policies to access control policies, must be addressed. We believe that privacy obligation policies need to be explicitly managed, enforced and monitored - within and across organisational boundaries. A proper language (or a suitable extension of current languages) must be defined to represent them, in a broader context of privacy-aware data handling management. We also believe on the importance of standardising this language, to enable interoperability and an open exchange of privacy policies (across organisational boundaries) along with the associated personal data.
This position paper analyses the current situation, highlights related requirements and proposes ways to move forwards.

2. Setting the Context

Nowadays, people are asked to disclose (part of) their personal data in order to access web services and/or engage in business interactions. This information is required by enterprises (e.g., service providers, e-commerce sites, etc.) to enable their business processes and transactions. This trend is not going to disappear in the foreseeable future. Emerging technologies such as federated identity management and automated supply-chain solutions are further simplifying and automating the process of acquiring and exchanging personal data within and across organisational boundaries.

In this context, it is of paramount importance to ensure that personal data (once disclosed by data subjects) is collected, processed and transferred to third parties according to best data handling practices [2], in a way that is compliant with privacy preferences expressed by data subjects, privacy laws [1,2] and organisational privacy guidelines.

At the very core, privacy policies dictate criteria on how data should be collected, accessed, used, disclosed and retained. They define privacy rights, permissions and obligations. Current state-of-the art work, including W3C work, focuses primarily on privacy aware access control policies, their management and enforcement, see [3,4] for more details. Of course, this is very important in order to handle privacy rights and permissions. On the other hand, the "obligation" side of privacy policies is still under-emphasised, currently either subordinated to access control policies or not fully specified. In a comprehensive privacy management framework all aspects of privacy policies must be properly addressed – to enable adequate privacy-aware data handling management.

3. On the Role of Privacy Obligation Policies

Privacy obligations are policies dictating constraints, duties and expectations to data receivers, in particular enterprises, on how personal data should be handled [3,4]. This includes data retention management, deletion of data, notifications, data transformations, etc. Obligations define, at the very base, the criteria that drive privacy-aware information lifecycle management: they are an integral part of enterprise privacy policies, along with data handling and access control policies.

Privacy obligations can be derived from privacy preferences defined by data subjects (e.g., choice of notifying a user when their data is accessed; choice of deleting users' data once the processing of their transactions is over, etc.) and/or be defined by privacy administrators, as part of their process of dealing with privacy laws/guidelines.

Privacy obligations are associated to personal data: they are a type of "sticky policies" to be managed and enforced also when data is disclosed across boundaries in a federated identity management/multi-party context. As such they must "stick to" data once data is disclosed to third parties and must be locally enforced.

To enable this scenario, obligations need to be explicitly represented, interpreted and enforced to ensure that personal data is managed in the expected way. Of course the management of privacy obligations must be compatible (and integrated) with current approaches to deal with data handling aspects (e.g., management of data purposes, enforcement of data subjects' consent, checking of data requestors' intent against stated purposes, etc.) and privacy-aware access control.

Current state-of-the-art privacy languages and related frameworks (e.g., EPAL, XACML, etc.) subordinate the management of obligation policies to the management of access control policies. We believe these approaches have limitations, given the nature of obligations policies. For example, an obligation dictating the deletion of data after a predefined period of time has to be fulfilled independently from the fact this data has ever been accessed. A language (and framework) that subordinates the triggering and enforcement of obligations purely based on access control events is not able to capture even this simple type of constraint.

A proper language is required to describe a broad variety of "events" (beyond access control, i.e., time-based events, context-based events, etc.) that might trigger obligations: this language must also allow for an explicit description of the “target” of an obligation (i.e., the personal data that is subject to the obligations) along with the actions to be carried on (e.g., deletion, notification, etc.), allowed exceptions and be extensible to future needs [3,4].

4. Requirements

A list of core requirements and needs to be addressed, in order to handle privacy obligations (as part of a comprehensive data handling process), follow:

1. Need for a language to explicitly represent privacy obligations;
2. Need to ensure that this language is integrated with – but not subordinated to – languages used to describe access control and data handling policies. Current privacy-aware languages (such as XACML) might need to be reviewed and extended in order to accommodate privacy obligation requirements;
3. Need to provide the right level of flexibility in the language to describe the target of an obligation, its triggering events, actions and exceptions, along with the capability to extend this language for future needs;
4. Need to describe the entities involved in the obligation policies with meaningful ontologies, whose semantic is shared with other privacy-aware policy languages;
5. Need to explicitly associate privacy obligations to personal data to enable its lifecycle management, both when data is locally stored by an organisation and when this data is transmitted to third parties. Obligations must be considered as an instance of sticky policies;
6. Need to address the problem of negotiation of obligation policies across organisational boundaries, effective stickiness of obligation policies to data and mechanisms to enable accountability of all the involved parties;
7. Need to define a framework for the explicit enforcement and monitoring of privacy obligations – driven by the specifications described by obligations;
8. Need for this framework to be integrated to – but not subordinated to – current frameworks used to deal with privacy-aware access control and data handling;
9. Need for this framework to be compatible with state-of-the-art identity management solutions and identity management standards (e.g. Liberty Alliance, WS-*, etc.) in order to be adopted by enterprises as part of their current identity management solutions;
10. Need for standards – at least at the language level - to enable interoperability among all the involved parties.

5. Proposal for Next Steps

As next steps, we propose to discuss in more details (during the workshop and afterwards, in an appropriate W3C forum) the implications of managing privacy obligations on personal data along with their requirements. We recommend this should happen in the context of a broader discussion on privacy-aware data handling and access control policies.

As a starting point, we suggest to consider the work done in the context of the EU PRIME project [5], in particular how privacy obligations have been represented and managed in this project, how they have been associated to data and integrated within data handling policies and how this has been done in synergy with privacy-aware access control. This is a significant example and we believe it is worth to share the results with the audience – in order to open a debate.

Our immediate goal, to be achieved during this workshop, is to explore the level of interest and/or support of participants for one or more of the following aspects:

1. Analysing and designing an "integrated" language (potentially by extending and/or leveraging existing ones) to address various aspects of privacy policies, inclusive of privacy obligations, data handling and access control policies;
2. Analysing and designing a reference model for a framework that supports the management and enforcement of these policies;
3. Exploring the standardisation of such language and framework to enable interoperability, in particular in a context of federated identity management where data is disclosed along with associated policies (sticky policies);
4. Exploring alternative views and approaches to the obligation management problem and getting feedback on requirements and actual needs.

6. Conclusions

This position paper highlighted the importance of managing privacy obligations in enterprises, as part of enterprises' privacy-aware data handling practices.

We made the case for the importance of explicitly representing, enforcing and monitoring privacy obligations, instead of subordinating these elements to access control aspects, as it happens in current works (e.g. EPAL, XACML, etc.).

We believe there is a need for a language and a framework to represent and manage privacy obligations integrated with (but not subordinated to) privacy-aware access control and data handling policies along with their frameworks.

Standardisation is key to enable interoperability across organisational boundaries.

This W3C workshop is a good opportunity to open a discussion on this topic, allow the audience to express their views and decide about the next steps.

7. References

[1] Laurant, C.: Privacy International: Privacy and Human Rights 2004: an International Survey of Privacy Laws and Developments, Electronic Privacy Information Center (EPIC), Privacy International. http://www.privacyinternational.org/survey/phr2004/, 2004

[2] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.", http://www1.oecd.org/publications/e-book/9302011E.PDF, 1980

[3] Casassa Mont, M.: Dealing with Privacy Obligations: Important Aspects and Technical Approaches, TrustBus 2004, 2004

[4] Casassa Mont, M.: A System to Handle Privacy Obligations in Enterprsies, HPL-2005-180, http://www.hpl.hp.com/techreports/2005/HPL-2005-180.html, 2005

[5] PRIME Project: Privacy and Identity Management for Europe, European RTD Integrated Project under the FP6/IST Programme, http://www.prime-project.eu/, 2006