Outsourcing personal data processing to the cloud

Chris Mitchell
25th January 2013

1 Introduction

Use of the cloud for a wide variety of data processing purposes is undoubtedly a major growth area, with many potential advantages for users in terms of reduced costs and simple and quick access to processing resources. However, problems potentially arise when cloud services are used to process personal data or, more precisely, *Personally Identifiable Information* (*PII*). In particular, whilst the data processing is outsourced, the legal obligations with respect to PII protection remain with the client of the cloud service. That is, the user of cloud services will have to ensure that the cloud service respects the legal obligations associated with the storage, management and processing of the PII which it submits for processing.

Since it is hard to imagine an organisation that does not hold a certain amount of PII, e.g. relating to its employees, this is likely to be a potential obstacle to almost any organisation wishing to outsource its data processing to the cloud. To ensure that it is not in breach of its legal obligations, an organisation will need to determine which cloud service providers will process PII appropriately.

One possible solution to this problem would be an auditable standard for cloud service providers which process PII. An auditor could verify whether a cloud provider meets the requirements of the standard and, if satisfied, it could issue a compliance certificate. This certificate could then be used both as a marketing tool for the cloud provider and as a simple way for a client to verify that a provider will meet their legal and regulatory obligations with respect to PII processing. Indeed, audited compliance to such a standard could be written into the contract for cloud service provision agreed between the cloud client and service provider.

The main focus of this article is an emerging international standard, ISO/IEC 27018 [7], which is intended to become just such a standard. As such, it is hoped that ISO/IEC 27018 will solve a key problem for the cloud industry.

2 Meeting a business need

We next explore in a little more detail the need for such a standard. We first introduce some terminology. PII can be formally defined as any information that (a) can be used to identify the *PII principal* to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal. As implied above, a *PII principal* (or *data subject* in some jurisdictions) is simply the person to whom the PII relates.

We are concerned here with the needs of organisations acting as *PII controllers*. A *PII controller* (or *data controller* in some jurisdictions) is a person who, either alone or jointly or in common with

other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed. We suppose that a PII controller wishes to use a public cloud service provider, acting as a *PII processor*, to process its PII (note that, in line with the scope of ISO/IEC 27018, we do not address issues relating to *private* cloud services). A PII processor is any entity that processes PII on behalf of and in accordance with the instructions of a PII controller. We refer also to a *cloud PII processor*, meaning a public cloud service provider acting as a PII processor.

The relationships between the key roles involved in PII management and use are shown in Figure 1.

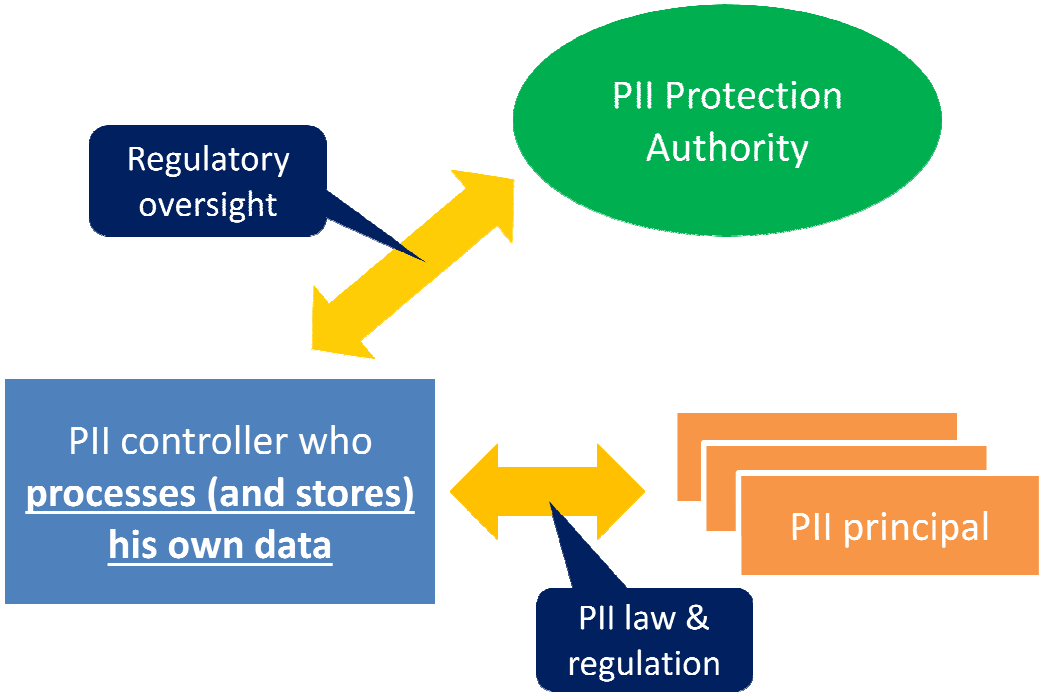

Figure 1: PII – context of management and use

As briefly discussed above, developing the industry opportunity provided by the cloud needs both customer and regulatory authority confidence that PII will be processed in the cloud in ways that do not breach laws or regulations applying to the PII controller. To maximise the market opportunities, such confidence needs be developed as speedily as possible.

The goal of the work described here is to create a system for cloud PII processor governance, and for demonstrating conformance using certification. Moreover, this system should ideally integrate with processes already used by today's cloud infrastructure, based on existing PII processing obligations, to encourage rapid and wide adoption. The system should be capable of being developed in future releases to move towards improved cloud privacy as cloud infrastructure and privacy requirements develop.

3 PII processing in the cloud

If the PII controller uses a cloud service to process PII, then the PII controller retains its legal and regulatory obligations relating to the gathering and processing of PII. The precise nature of these obligations will, of course, depend on the jurisdiction within which the PII controller operates. The

relationship of the PII processor to a public cloud service provider acting as a PII processor is shown in Figure 2.

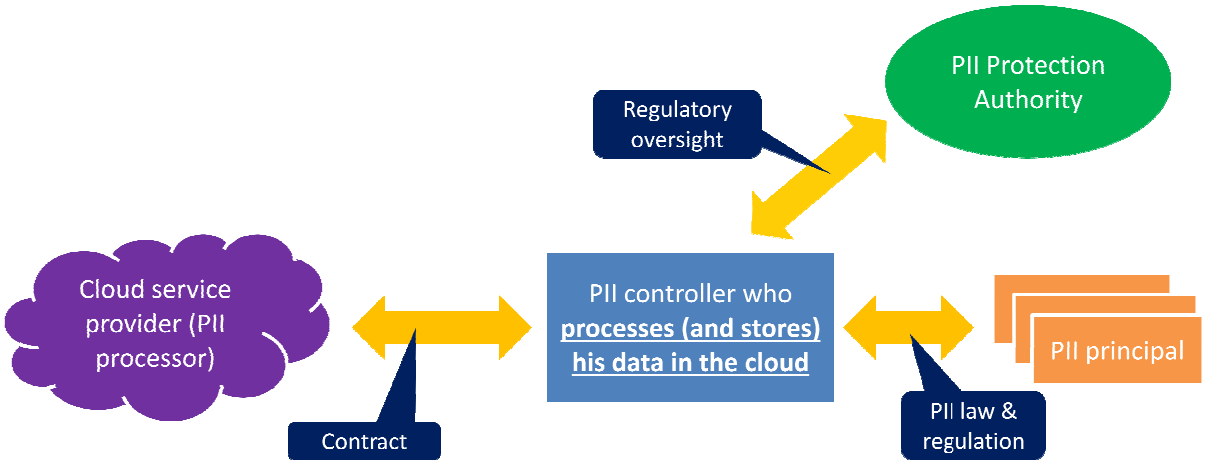

Figure 2: Relationship of PII controller to cloud PII processor

The PII controller therefore needs to ensure that the public cloud service provider will meet the PII controller's obligations when processing PII. This can be achieved in two main ways.

1. The PII controller can ensure that the contract it establishes with the PII processor enshrines all the principles necessary to ensure that the PII processor's obligations are met.
2. The PII controller can verify that the PII processor behaves in appropriate ways through compliance auditing.

It is intended that ISO/IEC 27018 can assist with both of these steps. The PII controller can cite ISO/IEC 27018 in its contract, and can verify that the PII processor has been audited against the principles specified in the standard, thereby allowing the PII controller to select a well-governed PII processor.

4 The ISO/IEC 27018 approach

The cloud provider market already understands, invests in, and extensively implements, audited certification to ISO/IEC 27001 (*information security management system requirements*) [2], using the information security controls catalogue in ISO/IEC 27002 [3]. Moreover, the notion of ISO/IEC 27001 certification, with its origins in BSI 7799 parts 1 and 2, is now very well-established internationally, and is therefore something that will be familiar to many potential users of cloud services.

As a result, it has been decided to build on the existing ISO/IEC 27001 security management system. That is, cloud provider PII protection certification will be achieved using the existing ISO/IEC 27001 processes. ISO/IEC 27018 will act as a supplement to ISO/IEC 27002, containing (a) additional cloud PII processing-specific implementation guidance for existing ISO/IEC 27002 controls, and (b) additional cloud PII processing-specific controls; using the ISO/IEC terminology, ISO/IEC 27018 will be structured as a sector-specific standard to cover PII protection for a cloud PII processor. The additional controls in ISO/IEC 27018 will be used in conjunction with the ISO/IEC 27002 controls as the basis for certification of a cloud PII processor.

This approach is designed to provide a practical and pragmatic base to start the process of creating confidence that the cloud industry deals appropriately with the PII that it processes. At the same time, the public cloud industry will have clear guidance about what it needs to achieve to meet the legal and regulatory concerns of its clients.

It is hoped that the ISO/IEC 27018 approach will be attractive to existing cloud providers and will scale well. It also seems reasonable to believe that it will provide an economically viable means of developing an incremental accreditation and certification process, which can be continuously improved once it is in place.

5 Scope of ISO/IEC 27018

The scope of ISO/IEC 27018, as explained above, is a relatively narrow one. That is, it is restricted to those controls of relevance to a *public* cloud service provider acting as a *PII processor*. This scope is show diagrammatically as 'Scope 1' in Figure 3. In particular it excludes privacy concerns which may arise if a cloud service provider also acts as a PII controller. In fact, 'Scope 2' shown in Figure 3 is a potentially considerably larger scope, which it is intended will be addressed by a different standard that is currently at an earlier stage of development. Indeed, this latter standard is currently being balloted as a possible new work item, and will only proceed if the ballot result is positive.

ISO/IEC 27018 can be seen as implementing the privacy principles of ISO/IEC 29100 (the *privacy framework*) [4] as applied to a PII processor (but not as applying only to a PII controller). In the second Working Draft of ISO/IEC 27018, all additional controls have been classified according to these privacy principles.

The scope of ISO/IEC 27018 is summarised in Figure 3.

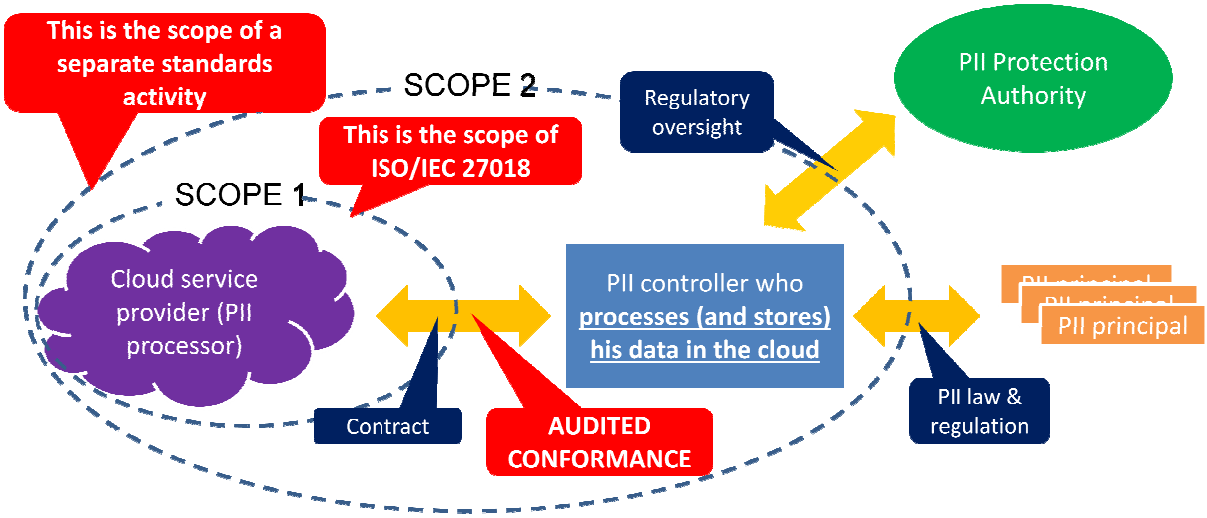

Figure 3: Scope of ISO/IEC 27018

Within SC27/WG5 we believe that ISO/IEC 27018 is a key element to start the cloud industry moving down the path of privacy conformance.

6 Origins of ISO/IEC 27018 protection controls

Prior to producing the first draft of ISO/IEC 27018, an extensive analysis was performed of existing law relevant to third party processing of PII. The main result of this analysis was a set of 70 controls, which were documented in the original proposal for a new work item [5]. Only those not already covered by the existing set of controls in ISO/IEC 27002 were included in the first Working Draft of ISO/IEC 27018 [6].

Subsequently, the European Union published an important review of cloud computing privacy issues [1]. These were carefully analysed, along with other published opinions, and used to derive a number of additional controls which were included in the current (second) Working Draft of ISO/IEC 27018 [7].

The origins of the controls in the current Working Draft of ISO/IEC 27018 is summarised in Figure 4.

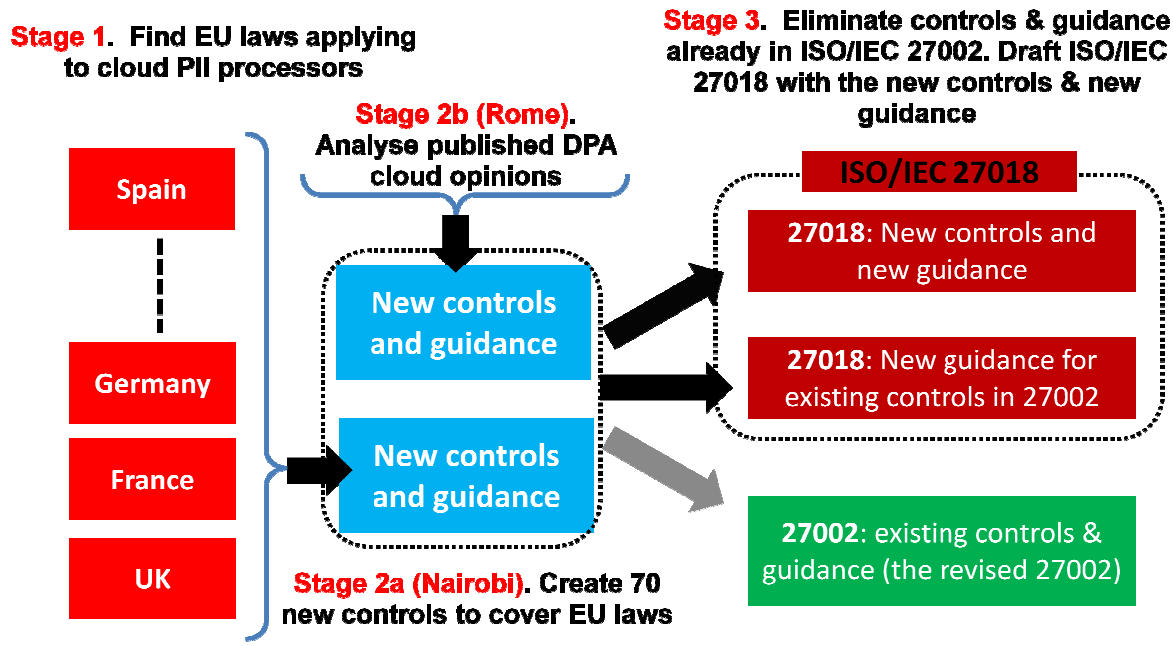

Figure 4: Origin of ISO/IEC 27018 controls and guidance

7 The development of ISO/IEC 27018

ISO/IEC 27018 is being developed within SC 27 (*Security techniques*) of ISO/IEC JTC1/SC 27, concerned with *Information technology*. Within SC 27, the development of the standard is being performed within Working Group 5 (WG 5), concerned with *Privacy and identity management*.

Work officially started on ISO/IEC 27018 with the successful conclusion of a new work item ballot in February 2012. A preliminary Working Draft was circulated in March 2012, and this was discussed at the Stockholm meeting of SC 27 in May 2012. A first official Working Draft [6] was circulated in June 2013, and discussed at the Rome meeting of SC 27 in October 2013. Following lively discussions in Rome, a second Working Draft [7] was circulated in December 2012, which is due to be discussed at the Sophia Antipolis meeting of SC 27 in April 2013.

To participate in the development of ISO/IEC 27018 please consider joining the work on SC 27/WG 5, via your national standards body. As the editor of ISO/IEC 27018 I am always happy to provide information and answer questions – please contact me at me@chrismitchell.net.

8 Acknowledgements

I would like to thank John Phillips for not only providing all the figures in this article, but also helping greatly with the structure and text. I am further indebted to Microsoft for their generous support during the development of ISO/IEC 27018. Finally, I must thank all the experts in SC 27/WG 5, whose valuable comments and suggestions have helped shape the current draft of ISO/IEC 27018.

9 Bibliography

[1] European Union, Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, adopted July 2012.

[2] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*, 2nd edition (to be published).

[3] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*, 2nd edition (to be published).

[4] ISO/IEC 29100, *Information technology — Security techniques — Privacy Framework*, 2011.

[5] ISO/IEC JTC1/SC27 N10550, *Proposal for a new work item on Code of practice for data protection controls for public cloud computing services*, November 2011.

[6] ISO/IEC JTC1/SC27 N11253, *1st WD 27018, Information technology – Security techniques - Code of practice for data protection controls for public cloud computing services*, June 2012.

[7] ISO/IEC JTC1/SC27 N11742, 2nd WD 27018, *Information technology — Security techniques — Code of practice for data protection controls for public cloud computing services*, December 2012.