NYMITY

Toronto / Washington DC / Brussels
www.nymity.com

Privacy Interviews with Experts
July 2010

Michael Willett

Board Member and Chair
ISTPA

Privacy by Design: A Systems Architect, Engineer and Designer Tool

For years we have had principles and policies to guide our developers in integrating privacy into our systems and processes. Translating these principles and policies into a consistent application has been difficult for developers, both business and technical, especially when the demands of the lines of business teams for functionality and timeliness often overshadow the standard requirements, like privacy.

The International Security, Trust, and Privacy Alliance (ISTPA) has developed a Privacy Management Reference Model (PMRM) that is ready to be tested as one such tool. The PMRM will serve as the basis for a new OASIS Technical Committee (the PMRM TC), where the PMRM will be further refined and applied to a variety of Use Cases across business and governmental sectors.
John Sabo of CA Technologies and Michael Willett, a security and privacy consultant, are leading the effort to take the Privacy Management Reference Model to the next step in OASIS. They discuss the model and the goals to carry it forth in an open-source manner to become a standard tool to assist in the effort to architect privacy into systems and processes in a granular fashion.
Michael Willett, ISTPA Board Member and the ISTPA Technical Committee Chair provided the responses below to a number of questions from Nymity regarding the PMRM.

Nymity: Why are standard privacy methods and tools needed by architects, designers and implementers of systems and processes? Why are principles and policies not enough?

Willett: Privacy principles and practices (such as notice, consent, collection limitation, etc) and policies provide the verbal description for the privacy requirements that apply in a given context (Use Case). But, these verbal statements provide little or no clue as to how a system designer should build these requirements into a privacy management system. Privacy requirements tend to be non-operational. What is needed is a complete set of privacy services that can be implemented into systems and invoked on command. The system designer would then need to map a given set of privacy requirements into the operational services. Privacy principles and practices typically describe the desired OUTCOME, but not the HOW. The PMRM provides the HOW.

Nymity: Do such standard security methods and tools exist? If so, why has it been so difficult to develop privacy parallels?

Willett: Security is a technically mature discipline. Algorithms and operational implementations have been around for security for some time. Maturity models exist for security, which underscores the 'maturity' of the subject. Standards, up through international standards, for operational security mechanisms and tools exist and offer complete coverage of security requirements. Not so for privacy. Privacy requirements are not as well-defined and certainly not as codified as for security.
Privacy has remained largely in the policy domain, with legislation, best practices, and principles defining the requirements for privacy.

Since privacy deals with the life-cycle management of personal information (PI), privacy management goes well beyond standard security controls; eg, even after gaining access to PI, privacy deals with what can be done with the PI. Work on the PMRM should help to move privacy management from the policy domain to operations.

Nymity: When technology changes exponentially, how have security methods and tools adapted to assist developers? What adaptation criteria will be important for privacy methods and tools?

Willett: Elaborate and complete security taxonomies that exist that show the higher-level security services (like confidentiality, integrity, access control, and authentication/authorization) broken into multiple choices at the 'mechanism' level.

For example, under "confidentiality", there is encryption, which in turn has multiple choices for the specific algorithm (such as AES, PGP, public-key etc). The specific mechanisms evolve to satisfy stringent security and performance requirements, while the higher-level services remain stable. We expect the same evolution for privacy management: a set of complete privacy Services, implemented using an evolving set of privacy mechanisms.

Nymity: What is the ISTPA? What is the Privacy Management Reference Model? Why was it necessary to move away from the terminology in the various high level Privacy Principles and Guidelines found in the Fair Information Principles, the OECD Guidelines and APEC Privacy Framework?

Willett: The International Security, Trust, and Privacy Alliance (ISTPA) has been working toward an operational definition of privacy management, culminating in the Privacy Management Reference Model (PMRM). The recent analysis of legislative instruments conducted by the ISTPA, including those listed above (found on the web site: www.istpa.org), demonstrated that the language used to express privacy policy, principles, and practices is far from standardized. Even the simple-sounding requirement for Notice has many different meanings, depending on context and jurisdiction.

The ISTPA decided not to attempt to standardize the privacy requirements language (such debates about meaning go on forever!), but rather to take any set of privacy requirements and map those requirements into a well-defined set of privacy Services. Remember: policies, practices, and principles are requirements for OUTCOME (and represent the sometimes ambiguous "voice of the customer"), whereas the PMRM Services define the HOW.

Nymity: What are the next steps in the development of the Privacy Management Reference Model?

WIllett: The formal steps to create the PMRM Technical Committee in OASIS are underway and should be completed by 8 September, 2010. The ISTPA has donated the PMRM to that new Technical Committee. The first orders of business will be to vet the PMRM in the larger OASIS audience and to seek Use Cases from several 'vertical' industries and associations.

Nymity: What privacy risks is the Privacy Management Reference Model intended to mitigate? What controls is it intended to put in place?

Willett: The operational definition of privacy is: the assured, proper, and consistent collection, processing, sharing, transmission, minimization, use, retention, and disposition of Personal Information (PI) throughout its life cycle, consistent with information protection principles, policy requirements, regulations, and the preferences of the individual.

The 10 operational Services of the PMRM have been derived by examining this definition in lengthy detail. "Risks" result from potential violations of any tenet of the definition; e.g, improper actions, inconsistent with individual preferences etc. The 'controls' result from implementing the appropriate functions under each selected Service.

Nymity: What will be the open source method and organization for testing, improving and implementing the Privacy Management Reference Model? What privacy issues will be used in the testing and methodology development? When will the exercise begin?

Willett: The ISTPA specifically selected OASIS for its openness and broad reach to form a Technical Committee to carry on the work of the ISTPA. The OASIS work is open to the public and any entity can join in order to actively participate in any Technical Committee. The output of the PMRM Technical Committee will be royalty-free to any user. The exercise begins in earnest when the PMRM Technical Committee is formed: 8 September, 2010. The PMRM Technical Committee will need to choose a methodology for formally presenting and analyzing Use Cases.

Nymity: How can companies participate?

Willett: Any company can join OASIS and sign up for the PMRM Technical Committee, when it is formed.

Nymity: Who would be good candidates from companies to participate? The CPO or the CPO staff? The IT systems developers? The CISO or the CISO Staff? The business developers?

Willett: Anyone charged with implementing a privacy management system or a privacy policy will benefit from working on the PMRM Technical Committee. More broadly, anyone who handles personal information will also benefit.

Nymity: In conclusion, what have we not addressed and what additional advice do you have for those that have not yet been able to implement tools to successfully guide their development staff in integrating privacy into their designs? What other practical considerations are there?

Willett: Follow the evolution of the PMRM in the Technical Committee, especially the Use Cases as drawn from a variety of settings and with varied privacy requirements. The Use Cases will reveal any nuances behind the PMRM and will in turn lead to a practical 'implementer's guide to privacy management'.