

## CS1/06-0166 2<sup>nd</sup> IBM Contribution on NWI for A Privacy Reference Architecture Scheme

The following text was provided by Bob Blakley, IBM's Chief Scientist for Security and Privacy.

*Privacy protection has much more to do with preventing incorrect uses of information by authorized users of that information than it does with data protection or access control, and even this falls short of a complete privacy solution. Technology to automate even this process is still immature.*

*Speaking as past general chair of the IEEE workshop on Security and Privacy referenced in the NSA note, I believe that no one in IEEE is confused about the difference between security and privacy - and the fact that both words appear in the workshop title (and the magazine title) separated by an "and" is a good indication that the community considers these to be separate problems (though of course related in some ways).*

*SOME "privacy technologies are based in part on long standing IA technologies" - but other privacy technologies are NOT so structured, and tools designed to meet traditional security goals are NOT by themselves adequate to provide the privacy protection required by individuals in the modern world.*

*Building a privacy reference architecture on a security reference architecture is EXACTLY the sort of mistake IBM wants to avoid, and this is part of the reason for our original comments.*

\*\*\*\*\*

Also attached below is an informal paper that presents additional privacy discussion points and privacy resources:

**Disclaimer: This informal paper presents a set discussion points on the topic of privacy. The author<sup>i</sup> is not commenting on specific government policies with respect to policy.**

A definition: *Privacy: The right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.*<sup>ii</sup>

Note that this is not necessarily the consensus view across the world.

Privacy requires effective information security, including assurance, "CIA," etc. However, effective information security does *not* guarantee an expected level of privacy.

The OECD Privacy Principles<sup>iii</sup> express the concepts that underpin most privacy legislation and fair practices around the world. These principles are:

⊗ purpose specification,

- ⌘ collection limitation,
- ⌘ use limitation,
- ⌘ accountability,
- ⌘ security safeguards,
- ⌘ openness,
- ⌘ individual participation (including consent), and
- ⌘ data quality.

Note that the FTC<sup>iv</sup> is closely, but not completely, aligned with the OECD principles.

The challenge is to build an environment where an individual's concern for privacy can be respected and protected while allowing information to flow and organizations that depend on information to operate effectively.

Privacy is not new, but new technologies and technology-driven social changes, especially e-business and e-government, heighten concerns and redefine the issue. More organizations have CPOs than CSOs because privacy affects millions of people (e.g., customers and voters). A high degree of public attention is focused on enterprises that collect PII. Therefore, organizations must respond in a public way. Note that while the most recent FBI/CSI survey showed year-to-year improvements, and discounting the more sensationalist media coverage, the recent set of data breaches has raised awareness in individuals that all manner of PII about them has been collected, and they don't know what "ownership" control they have over its collection, use, etc. Note also that there are a set of information security and assurance underpinnings that can mitigate some breaches (e.g., encrypted files, disks and tapes), but that more is required to guard against malicious operations and insider threats.

The following are examples of how privacy issues can arise:

- ⌘ A business wants to increase its sales, using information collected from past sales, without eroding its customers' trust and loyalty. As the world moves to data-centric computing, abuse of collected PII (direct and inferred) must be prevented.
- ⌘ PII leaks, allowing PII to move outside of defined domains/use policies. This could include inappropriate movement of PII from an organization to one of its partners, or an inadvertent posting of PII to a public website.

An organization reduces the risk of privacy breaches by a 5-part privacy management process:

1. *Define* the privacy policy, then create a link between the human-readable policy and machine-readable policies. Note that an organization's privacy policy is increasingly likely to be governed, at least in part, by legislation or regulation. In the United States, there are now multiple data breach laws across the states. In an increasingly global environment, organizations

must comply with national laws and regulations that may be difficult to reconcile.

2. *Deploy* the privacy policy, associating the policy with specific privacy-sensitive resources.
3. *Record* user acknowledgment/consent to the privacy policy and choices, attaching a “sticky policy” to data.
4. *Monitor/enforce* data access according to the consented privacy policy. Track consent on a per-user, and sometimes on a per-data instance.
5. Create *audit* reports, including the reason associated with a data access.

There are differences between classical authorization (access control) and privacy management. When considering privacy management:

- ⌘ The data owner (e.g., PII subject) is equally important to the data user. Traditional access control factors in only the data user, e.g., credentials, groups, entitlements, roles, etc. Privacy management also considers the data owner, e.g., choices (opt-in to sales messages), attributes (age, legal residence), and other factors (time of day, etc.).
- ⌘ The business purpose must be considered – e.g., a shipping clerk accesses a customer's address for the purpose of order fulfillment, but the clerk does not need to access the customer's credit card information. Traditional access control authorizes “actions” or “operations” such as create, read, update and delete. Privacy management authorizes “actions for a business purpose” such as:
  - read for the purpose of fulfilling an order,
  - write for purpose of registering political party affiliation, and
  - delete for purpose of removing from preferred physician list.
- ⌘ Privacy policy is a relationship. Traditional access control attaches “policy” to a protected object, e.g., an ACL. Privacy management is an agreement between the data collector and the data owner (usual the PII subject). This agreement:
  - Must be recorded on a per-data owner basis.
  - Ethics of privacy management require that the agreement is immutable.
  - “Sticky Policy” is attached to data instances.
- ⌘ Data Usage must be traced to consent. In traditional access control, logging the access is enough. In privacy management all actions on PII must be justified in in terms of consented policy.
- ⌘ Obligations may be incurred. In traditional access control, decisions are atomic, e.g., permit|deny. In privacy management, decisions sometimes start other processes, e.g.,

- The IRS can access your financial history for audit purposes, but the data owner must be notified.
- The ACME Research Corp can access a person's genome information, but only if the data subject opts in and Acme Research pays the data owner \$100 a year.
- A minor's e-mail address may be collected, but only if parental consent is obtained in 30 days, otherwise it must be deleted.
- ⊗ Sometimes just monitoring (versus enforcing) is sufficient. In traditional access control, all accesses that aren't conformant to policy must be denied. In privacy management, sometimes it's good enough to just record the non-compliance.

Finally, for another view of why privacy is important, please read Bruce Schneier's 19 May 2006 essay on "The Value of Privacy" at [http://www.schneier.com/blog/archives/2006/05/the\\_value\\_of\\_pr.html](http://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html).

Additional resources:

- ⌘ <https://www.privacyassociation.org/> – IAPP (International Association of Privacy Professionals) – note that IBM Corporation is a Platinum Member.
- ⌘ <http://www.bbbonline.org/UnderstandingPrivacy/PMRC/pms.asp> – BBB's “Privacy Made Simple” web site. Note that IBM Corporation is a sponsor of BBBOnline.
- ⌘ <http://www.privacyinternational.org/> – Privacy International.
- ⌘ <http://www.privacyfoundation.org/> – Privacy Foundation.
- ⌘ <http://www.privacyexchange.org/> – Privacy Exchange.
- ⌘ <http://www.truste.org/> – TRUSTe program – note that IBM Corporation is a member.
- ⌘ <http://www.privacyalliance.org/> – Online Privacy Alliance.
- ⌘ <http://www.cdt.org/> – Center for Democracy & Technology.
- ⌘ <http://www.consumer.gov/> – FirstGov for Consumers.

Acknowledgments:

- ⌘ Calvin Powers, Governance, Risk and Compliance Solutions, IBM Corporation.
- ⌘ George Robert Blakley III, Chief Scientist, Security & Privacy, IBM Corporation.

---

i David K. Hemsath, dhemsath@us.ibm.com

ii Dr. Alan Westin, *Privacy and Freedom*, 1967

iii [http://www.oecd.org/department/0,2688,en\\_2649\\_34255\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/department/0,2688,en_2649_34255_1_1_1_1_1,00.html)

iv <http://www.ftc.gov/privacy/>