Enabling Privacy, Data Protection and User Trust: the Convergence of Privacy Policies and Data and Technical Standards Development [Contributed by John Sabo, CA Technologies, on behalf of OASIS]

- **Data and information** are what the open Internet exists to deliver. They form the core of economic development, societal transformation, innovation, consumer value and global dialogue.

- **And so personal information and personally-identifiable information are no longer confined and stove-piped** – they are **integral to value-added and essential online services, a trend which will only accelerate** in Internet-dependent electronic health information systems, smart grid infrastructures, federated identity management systems, new consumer applications, and networked devices - the Internet of Things.

- **Entirely new forms of personal information are also generated as a by-product of Internet connectivity** and the convergence of individual identities, location, time, devices, data flows among systems, applications and data stores in addition to **the real-time interaction of individuals with Internet-connected systems** continually creates new aggregations of personal information, new inferences about individuals, and **new privacy risks.**

- The global connectivity of the Internet also means that **the policies which define the rights and responsibilities associated with the collection, use, communication, and destruction of PI are likewise no longer isolated and stove-piped.** The policies governing PI, whether derived from laws, regulations or individual user preferences, now interact in a web as complex as the data itself. And so d**ata and policy have merged** in a way never experienced before the advent of the Internet.

- Another reality is that the **expectations of individuals about how their personal information should be collected, communicated, used and protected are not uniform and are very context-dependent.**

- **These issues are compounded as businesses and governments rapidly deploy cloud computing services to achieve significant cost and economic benefits**. Cloud computing by definition **transcends the old model of a singular data processing center** and physical location, upon which most of today's data protection principles, practices, laws and regulations were originally developed.

- These realities - and the **absence of harmonized data privacy laws**, regulations and policies that align with today's Internet-connected world - mean that we face a condition in which **policy entropy – disorder - compromises our ability to design and deliver Internet-scale technologies that can**

- **support the context-driven, privacy expectations of consumers and citizens over time and across multiple systems and applications, and**
- **support trusted systems having predictable behaviors** and **measurable assurance** that will satisfy governments' interests in citizen privacy.

- **Therefore, our challenge is not fundamentally about technology.** Industry has demonstrated that IT systems, software and Internet technologies are capable of managing complex rule sets, data flows and contextual policy conditions.

- **Our challenge is to understand the nexus between policy and technology and to harness that understanding** to design and implement interoperable, trusted, operational privacy systems that can **work at Internet scale.** To accomplish this, we **need deeper collaboration between the policy community and the technology community.**

- **We believe that a path is available to bring some order to this disordered environment** and to support this vital collaborative model. That path is through **the use of international standards development organizations and consortia.** We are already seeing this happen.

- **For example**, **ISO/IEC is developing a privacy framework** (ISO/IEC 29100), **a privacy reference architecture** (ISO/IEC 29101)**, and a privacy capability assessment framework** (ISO/IEC 29190**).**

- In the **OASIS standards organization** a number of **technical committees** are focusing on work that **will contribute to a more privacy-manageable and trusted online environment. A few examples:**

  - **The Cross-Enterprise Security and Privacy Authorization (XSPA) Committee**, through which privacy policies, consent directives, and authorizations within/between healthcare organizations can be exchanged
  - **The Open Reputation Management System Committee,** developing reputation mechanisms for Internet-based based communities, and for validating the trustworthiness of web sites, blogs, events, products, companies
  - **The Privacy Management Reference Model Committee** to serve as a template for developing operational solutions to Internet privacy management and address lifecycle and cloud computing privacy

- These standards committee have made strong efforts to include outreach to government leaders and policymakers to ensure that governmental requirements are considered in the standards development process. But **the policy entropy mentioned earlier requires much greater coordination and interaction among policymakers and the technical community. We are seeing examples of that in major government initiatives -** in the EU consultation supporting the revision of the data protection directive and the outreach to industry by the United States government as part of its National Strategy for Trusted Identities in Cyberspace.

- **In closing, progress in managing operational privacy and security risks at Internet scale is achievable, but only**
    - **through** much greater collaboration among **academic, industry, government and individual experts who focus on data protection and data privacy and who understand the convergence of data privacy policies, technologies and standards**
    - **through the coordinated use of recognized standards organizations** such as ISO/IEC, ITU-T, OASIS, IETF and others, **to develop both technical and "framework level" management standards and promote their widespread adoption by all stakeholders.**
- **This will help bring a measure of order to the policy and technology entropy we see today around online privacy and enable standards-based, interoperable implementations that support policy-configurable and context-sensitive privacy management** on the Internet.
- **The institutional structures are in place to make this happen today.** If we use them effectively, we can provide a foundation for **metrics-driven compliance** and **self-regulation, instill consumer and user trust**, and earn the **confidence of governments**, business, and other institutions that **Internet privacy risks are manageable**.
- A key factor in our success will be the **active support of governments, including international institutions such as the OECD,** to foster the greater use of recognized standards organizations as vehicles to advance the sound integration of privacy policy interests with the realities of technology, innovation and the Internet.