OECD High Level Meeting, Paris, 28-29 June 2011

Remarks by John Sabo

On behalf of CA Technologies and representing the OASIS standards organization and the Internet Technical Advisory Committee, it is an honor to have the opportunity to discuss data privacy in an open Internet and to propose a path forward to achieve greater privacy protections and online trust.

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 inter-connected 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, devices, location, time, data flows among systems, applications and data stores. 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 no longer static. The policies governing PI, whether derived from laws, regulations or individual user preferences, now must interact in a web as complex as the data itself. And so data and policy have merged in a way never experienced before the advent of the Internet.

A further reality is that the expectations of individuals- their personal policies and requirements so to speak - about how their personal information should be collected, communicated, used and protected are not at all uniform and are extremely context-dependent. These issues are compounded as businesses and governments rapidly deploy cloud computing services to achieve significant cost and economic benefits.

These realities - and the absence of globally 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 lengthy time periods and across multiple systems and applications, and that can enable large-scale trusted systems having predictable behaviors and meaningful risk management controls.

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 privacy policies 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 increased understanding and deeper collaboration among policy communities and technology communities.

I believe that a path is available to support this vital collaborative model. That path is through the increased use of international standards development organizations and consortia. We see this happening more often today. For example, ISO/IEC is developing three major privacy standards. In OASIS, the Cross-Enterprise Security and Privacy Authorization standard supports the exchange of privacy policies, consent directives, and authorizations among healthcare organizations; the Open Reputation Management System Committee, is developing reputation mechanisms for Internet-based based communities and for validating the trustworthiness of online services; and the Privacy Management Reference Model Committee, which I co-chair, is developing a standard to enable operational privacy management in complex online systems and infrastructures.

These standards committees and others have actively engaged governments to ensure that public policies are considered in the privacy standards development process. And we are seeing similar outreach from governments in public policy initiatives - in the EU consultation supporting the revision of the data protection directive and the outreach by the United States government as part of its National Strategy for Trusted Identities in Cyberspace.

In closing, I believe that the policy entropy and lack of Internet-scale, interoperable data privacy standards can be addressed. But progress will require greater collaboration among academic, industry, government and individual experts using the well-established structures and processes present in recognized standards organizations such as ISO/IEC, ITU-T, OASIS, IETF, W3C, ETSI and other bodies.

This will help bring a measure of order to the policy and technology entropy we see today in online privacy. It will make possible standards-based, interoperable implementations that support policy-configurable and context-sensitive privacy management on the Internet and make possible technical systems that can help manage policy conflicts. 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.

However, a key factor to ensure success of this collaborative model will be the active support of governments, including 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 and to actively support the development of badly-needed data privacy standards and their wide adoption.

Thank you for your kind attention.