

Answer to the European Commission public consultation on the early challenges regarding the "Internet of Things"

Please indicate your preference (use a X):

- I agree that this document is made public
 I want this document **not to** be made public

If you reply on your own behalf, please indicate:

- Name:
- Telephone:
- Email:
- Country of residence:

If you are replying on behalf of an organisation, please indicate:

- The organisation's name: [CA Inc.](#)
- The type of organisation:
 - private company
 - government/public body/international organisation
 - academic/research institution
 - non governmental organisation
 - other:
- Your organisation details
 - o location: [One CA Plaza, Islandia, NY 11749, USA](#)
 - o size: [13,500 employees; 4.3 billion US\\$ in revenue](#)
 - o scope of activities (max 3 sentences): [CA \(NASDAQ: CA\) is the world's leading independent IT management software company. With CA's Enterprise IT Management \(EITM\) vision and expertise, organizations can more effectively govern, manage and secure IT to optimize business performance and sustain competitive advantage.](#)
 - o website: [ca.com](#)
- Contact person: [Carlo Cecchi](#)
- Contact person' telephone: [+39 02 90464222](#)
- Contact person's email: [carlo.cecchi@ca.com](#)

About CA Inc.

CA is one of the world's largest IT management software providers. Our software and expertise unify and simplify complex IT environments—in a secure way—across the enterprise for greater business results.

We call this Enterprise IT Management (EITM)—our clear vision for the future of IT. It's how you can manage systems, networks, security, storage, applications and databases securely and dynamically. You can build on your IT investments, rather than replacing them, and do it at your own pace.

Our software developers create and deliver IT management software that keeps our vision real. And we've taken our decades of experience solving complicated IT problems and developed practical paths for you to get from where you are today to where you want to be.

Founded in 1976, CA today is a global company with headquarters in the United States and 150 offices in more than 45 countries. We serve more than 99% of Fortune 1000® companies, as well as government entities, educational institutions and thousands of other companies in diverse industries worldwide. We are driving our next level of growth through our four-part strategy of product development, leveraging partners, global expansion and strategic acquisitions—all with the goal of helping you realize the full power of IT to drive your business.

In addition:

- We have approximately 13,500 employees worldwide.
- CA is a publicly traded company. We're financially strong and growing with more than \$2 billion in cash as of March 31, 2008 and reporting a revenue of 4.3 billion US\$ for fiscal year 2008, ending March 31, 2008.
- We have 5,900 engineers globally who design and support CA software, and we spend more than \$500 million annually to develop solutions that enable customers to better manage their IT.
- Our product development staff is global, with locations in Australia, China, the Czech Republic, Germany, India, Israel, Japan, the United Kingdom and the United States.
- To keep CA on top of major technological advances and to ensure our products continue to work well with those of other vendors, we are active in most major standards organizations and take the lead in many, including: Eclipse, SNIA, OASIS, The Open Group, CMDBF, W3C, DMTF, and ISTPA, to name a few.
- Many of our professionals are certified across key standards, including ITIL®, PMI, CISPP, and have built knowledge and expertise in key vertical markets, such as financial services, government, telecommunications, insurance, healthcare, manufacturing and retail.
- CA was the first major software company to earn the International Organization for Standardization's (ISO) 9001:2000 Global Certification.
- CA Greenability is how we act on our ability to make a positive difference in our environment.
- We are committed to improving the quality of life in communities where our employees live and work. We do this by supporting organizations, programs and initiatives that enhance the lives and wellbeing of others.

More information is available at: ca.com

The Internet of Things: Urgency in Understanding the Data Privacy Infrastructure

*By John T. Sabo, CISSP
Director, Global Government Relations
CA, Inc.*

This paper is a response to the call for public consultation in preparation of a Communication from the European Commission which will propose a policy approach addressing the whole range of political and technological issues related to the move from RFID and sensing technologies to the Internet of Things. While it appears from the staff paper that the Communication may have a broad focus (including architectures, control of critical infrastructures, emerging applications, security, privacy and data protection, spectrum management, regulations and standards, and socio-economic aspects), this paper proposes an initial and very heavy focus on data privacy policy and privacy infrastructure issues, particularly as they relate to the networked interoperability of systems and devices.

This focus is suggested in the Commission staff working paper, "Early Challenges regarding the "Internet of Things," which states that "...the productivity and efficiency improvements rendered possible by this Internet of Things and the services it will convey will definitely contribute to improvements in European living standards. So citizens and society will benefit. But there are also important policy issues, especially in the areas of privacy and data protection."

In fact privacy and data protection issues are already reaching a critical state in the current environment of interconnected networks, systems and applications where the flow of personal information has emerged as a default path for consumer, business and government service and applications. We have already begun tasting the benefits and the risks of a rapidly growing, immeasurably complex integration of technology and the societal fabric. Its components will be embedded in networked electronic health systems, industrial control systems, transportation, food production, financial and government and public safety systems, as well as consumer applications. The Internet of Things will only increase this complexity.

Security and privacy risks today require immediate attention by organizations attempting to understand, assess and manage the risks of a global infrastructure in which physical devices and physical instrumentality are increasingly networked, addressable, interactive, linkable to identity, and therefore of special concern as a personal privacy and public policy matter. In addition to the specific risks associated with the use of RFID for electronic passports and other governmental identity systems, or as incidental identifiers when RFID tags are used for tracking objects associated with individuals, there are other technologies (such as road-use tags, satellite-based automobile communications, medical device applications, and obviously mobile telephones and communicators) already in use which raise serious questions about our ability to assess and manage *today's* privacy and security and privacy risks – well before we have migrated to the Internet of Things envisioned in the call for public consultation.

We must not fail to take action. We must begin the hard work of understanding the structural demands of data privacy in the context of networked systems, applications, users and devices. Following this, we must devise a methodology to assess and categorize risks associated with the *use* of classes of devices in the growing networked environment and then to take action to develop a structured approach to security and privacy policy governance, management, and technical controls. High level support for managing such controls is available in the governance, risk and compliance discipline, which has emerged in the technical risk management community. Such a structured approach will enable policymakers and

implementing organizations to apply a baseline set of practices and tools to new risks which are likely to emerge in the Internet of Things. Many standards and solution mechanisms are now available, but can be molded to specifically address risks inherent in the Internet of Things.

A useful starting point to address these issues is therefore much more than an understanding of particular policy challenges and risk characteristics of specific networked devices (such as RFID or nanotechnology medical device implants). Today an equally useful and perhaps more urgent focus is to understand the broader policy and technical, architectural structures needed to manage privacy across interconnected systems, networks, governance structures and applications. These receive inadequate attention today and will be increasingly critical in the emerging world of ubiquitous networked devices.

Recent work undertaken by the International Security Trust and Privacy Alliance (ISTPA – see www.istpa.org) points to such an approach. The ISTPA, recognized that contemporary data privacy laws and principles/practices required an operational, policy-configurable technical framework or reference model. Version 1.1 of the ISTPA Privacy Framework was published in May 2002. It reflected extensive consultation with international data protection commissioners and privacy practitioners, as well as much refinement and testing. Whereas privacy requirements (typically expressed as fair information practices or privacy principles) provide little insight into how to actually implement them, the ISTPA Privacy Framework was developed to aid in the design and implementation of operational privacy management systems, many of which span policy and jurisdictional boundaries and used interconnected networks and applications. The vetting of the Framework confirmed that its 10 privacy Services represented a robust set of operational functions capable of supporting any set of privacy requirements.

An operational privacy framework is needed because the data and information privacy discipline, unlike the information security discipline, has had inadequate technical and operational infrastructure attention from both the IT policy and practitioner communities. Data privacy is often seen as only a policy issue, and few models are available to guide development of operational privacy architectures and systems. Additionally, data privacy is also often conflated with security. For example, in recent years data breach has often been treated as synonymous with data privacy, but data breach risk represents only one small part of overall data privacy risk. In the context of the consultation's focus on the Internet of Things, the approach taken by ISTPA in developing a policy-neutral technical framework can be very useful.

Since the ISTPA Privacy Framework was released, however, the state of privacy and data protection has changed substantially, as has privacy risk, through increased cross-border data flows, networked information processing, use of federated systems, application outsourcing, and experience with increased privacy breaches – as well as the growth of networked physical devices having personal privacy implications.

To address these changes, the ISTPA undertook studies and in-depth exercises aimed at examining the Framework and considering necessary revisions. As a starting point and with the understanding that privacy requirements come in many forms (practices, principles, legislation, regulations, and policies), the ISTPA completed a major study to determine if were possible to examine the dizzying array of privacy laws, principles and regulations and derive a workable, composite set of privacy requirements that could lead to improved technical and process engineering approaches to privacy management. The Framework would then be tested against those requirements and revised as necessary. As an example of the ISTPA's findings, the study's authors learned that common terms may often be used (notice, consent, individual access, etc), but that there is no uniform taxonomy or vocabulary. Obviously that is a barrier to developing enabling architectures and standards.

The ISTPA "Analysis of Privacy Principles: An Operational Study," published in May 2007, assessed twelve representative international privacy instruments (law, regulations, major statements of privacy principles), and extracted a working set of core privacy requirements. These requirements were then grouped together to create a composite set which in turn was used to inform further analysis of the ISTPA Privacy Framework. As a result of this analysis, the ISTPA determined that the services which compose the ISTPA Privacy Framework do comprise a robust and comprehensive set of privacy management functionality, but that changes to the Framework were needed. Consequently, the ISTPA is now completing a revision of the Framework document and initiated a number of activities to update the Framework content, improve its presentation of material, remove extraneous and outdated references, and incorporate additional structure to make the Framework more usable.

Ten ISTPA Privacy Framework Services - Audit, Certification, Control, Enforcement, Interaction, Negotiation, Validation, Access, Agent and Usage, as well as data security, incorporate subsidiary functions, any subset of which can be invoked in a particular privacy management scenario or use case. As part of the revision, the ISTPA is developing a new canonical format for the services and functions, designed to enhance the clarity and utility of the Services and provide a better foundation for automation and machine implementation of the underlying functions, as well as support modeling and simulation studies.

In summary, developing a useful approach to the challenges inherent in the emerging Internet of Things means more than examining narrow device-related issues. It means taking seriously the data privacy management, governance and risk issues associated with the underlying policy and technical infrastructure supporting such devices. The work completed by the ISTPA can and should be a model and starting point for examining these infrastructure-related issues.

There are immediate opportunities to begin this work. As an example, the Technical Management Board of the International Organization for Standardization (ISO) has requested that a task force provide expert opinion and advice on whether and how to address data privacy from the standards perspective. Although there is debate in the international standards community about the appropriateness of an ISO privacy standard, there are other options for pursuing such work, including industry standards organizations such as OASIS, or special chartered studies or industry-supported research projects.

Whatever the method or methods used, a focus on the technical and process-related infrastructure issues pioneered by the ISTPA in its "Analysis of Privacy Principles" and its "Privacy Framework v1.1" and ongoing revision can be extremely valuable as normative documents and as methodologies for addressing the infrastructure challenges we are facing now and which will escalate as we move more fully toward an Internet of Things.

About the author:

*John T. Sabo, CISSP
Director, Global Government Relations
CA, Inc.*

John Sabo is Director, Global Government Relations for CA, Inc., providing expertise in the use of security and privacy technologies in trusted infrastructures.

Mr. Sabo is an appointed member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. He is a past member of the Information Security and Privacy Advisory Board (ISPAB), a federal advisory committee managed by the National Institute of Standards and Technology. He also serves as a board member and President of the non-profit International Security Trust and Privacy Alliance (ISTPA), which has published a privacy services framework.

Mr. Sabo is very active in industry-focused information security initiatives. He is a board member and Immediate Past President of the Information Technology-Information Sharing and Analysis Center (IT-ISAC); member of the IT-Sector Coordinating Council, where he also serves on the Executive Committee; and Chair of the ISAC Council, which addresses cross-sector information sharing issues impacting national critical sectors. Mr. Sabo also serves as a member of the IDtrust Member Section Steering Committee, established by the OASIS standards organization, and focusing on identity and trusted infrastructure technologies, policies, and practices.

Before working in the private sector, Mr. Sabo was Director of the U.S. Social Security Administration's Electronic Services Staff and recognized as a leader in the development of e-government services. He is an invited speaker at international security and privacy conferences, has authored journal articles, and contributes to technical studies on security, privacy and trust issues. He holds degrees from King's College (Pennsylvania) and the University of Notre Dame, and is a Certified Information Systems Security Professional (CISSP).