



# **PRIVACY IN THE PARTICIPATION AGE**

White Paper  
May 2006

## Table of Contents

Entering the Participation Age . . . . .	1
Success in Participation Age Will Depend on Trust and Communities . . . . .	1
The Importance of Privacy to Trust and Community . . . . .	1
The Nature of the Network Has Changed. . . . .	2
Characteristics of the Participation Age . . . . .	3
Privacy as a Foundation for Trust and Community . . . . .	4
Turning Policy Into Practice — Integrating People, Processes, and Tools . . . . .	5
For More Information. . . . .	6

## **Entering the Participation Age**

The last twenty five years have been called the "Information Age" because information technology has had a big impact on our everyday lives and has fueled the growth of entire new industries through the commerce of information. Millions of people produce information, store it, and distribute it. And billions of people consume it in the same way we consume air, food, and water. However, the Information Age was one of passive consumers who essentially viewed the Internet as a database.

As technology has continued to advance, more open and ubiquitous access to information has begun to change the ways that people use technology. This is leading to the dawn of a new era that Sun calls the "Participation Age" — an age where participants aren't just acquiring information, but are also contributing to the information, refining it, and sharing it. More and more people are using technology to connect with each other to participate and to share work flows, to compete for jobs, to purchase goods and services, to learn and create.

Business models in the Information Age were protectionist and proprietary in nature with an emphasis on controlling the creation and distribution of information in an attempt to maintain competitive advantage. The Participation Age is the antithesis of that, bringing a focus on open access to information. It is through this open access that the pace of innovation is accelerating and new value is being created by communities of people. Networked human beings who share, interact and solve problems are generating meaningful content, connections, and relationships using the network as their medium of contact.

## **Success in Participation Age Will Depend on Trust and Communities**

Success in the Participation Age will rely on the Web and thriving communities to drive business growth. Businesses and the products and services they offer will evolve and develop based on community input. A critical success factor will be the quality and number of enthusiastic participants in a community. Communities are built around the shared value that is inherent in relationships between community members. They are also based on trust that the community will conduct itself in ways that are not harmful to its members. And because the value of the community is based on sharing, a community can become even more valuable as it grows in size. Consider, for example, an online auction that has a large community of buyers and sellers. As the community continues to grow, buyers can enjoy greater choice and competitive prices through more sellers. Likewise, sellers can find buyers more quickly through a larger community.

## **The Importance of Privacy to Trust and Community**

Because members must share in two way communications to participate, membership in these communities will grow only when there is trust in the business and the community. Trust is built when members feel safe in sharing because they expect their shared information to be used appropriately and not used against them in any way. One of the most important ways to build and maintain this trust is through consistent enforcement of effective privacy policies and practices. This paper reviews how the network has evolved along with the evolution from Information Age to the Participation Age and describes the impact this is having on security and privacy.

## The Nature of the Network Has Changed

Today's levels of collaboration and partnership are possible because the nature of the network has evolved to nearly eliminate boundaries. Barriers between in-house and external networks have gradually faded to enable open access as shown in Figure 1.

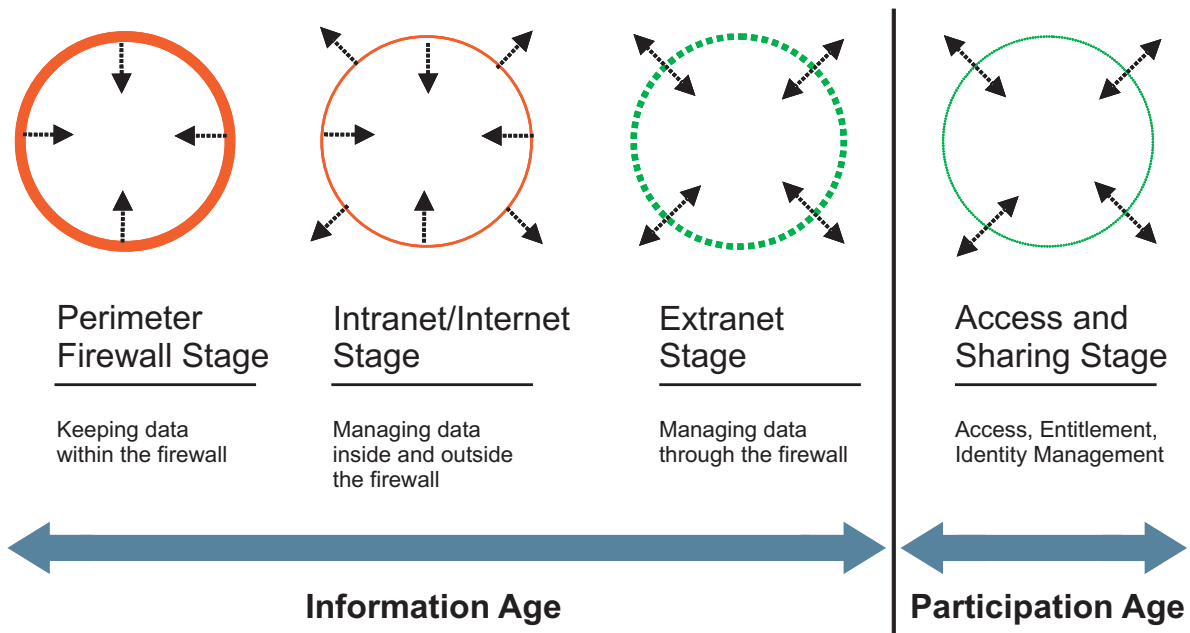


Figure 1. Barriers between in-house and external networks have gradually faded to enable open access

In the early days of network computing that we refer to as the “Perimeter Firewall Stage,” there were rigid perimeter boundaries to prevent information from flowing in or out. All data was contained inside of organization boundaries, so security and privacy issues were limited and were essentially defined by the perimeters of the secure environment.

The next stage involved an Intranet network that was still largely separate from the external world. Users could gain access to corporate data using a Web browser, but for the most part sharing of data was only available to users who were working inside the secure perimeter of their corporate network. There was some movement of data into and out of the organization via the Intranet/Internet, but it was carefully controlled by both perimeter control technologies and some contractual or fiduciary barriers. As a result, it was still possible to audit the flow of information into and out of the company because there were a limited number of transactions that crossed company boundaries.

As technology advanced, these perimeter controls gradually became more transparent and business models evolved accordingly to enable more fluid movement of information, eventually leading to the next stage of evolution, the “Extranet Stage.” In this stage, it became possible and necessary to share data across company boundaries. Security began to take a very different form in this stage. Traditional perimeter controls were not mature enough to truly enable a secure yet free flow of information. As a result, new security control technologies came into use. Identity management and access control technologies are now used to protect access to

information while enabling a greater flow of information in and out of the corporate network. The corporate network has essentially been extended to enable remote access by trusted parties.

As we move into the “Access and Sharing Stage” which is the dawn of the Participation Age, everything will be connected to the network with no practical boundaries (Figure 2). Greater access to information will enable value to be created through a trusted network of human beings who share, interact and solve problems. In this environment, organizations share targeted data, devices talk directly to other devices and Web services dynamically deliver information to users based on the context of each user’s situation as well as permissions attached to the data itself. For example, services can take into account a user’s geographic location and the type of device being utilized in order to deliver context-specific services that meet the user’s needs of the moment. Relationships are spontaneously created and destroyed, and data is deposited as needed throughout the network. These benefits are made possible when community members have trust in their community and in the security of the data that they send and receive.



*Figure 2. The Participation Age eliminates network boundaries, enabling large diverse communities*

### **Characteristics of the Participation Age**

To achieve the benefits of the Participation Age, security and privacy policies must be built into applications and data management schemes, and not defined by network boundaries. When designing and implementing these policies, systems developers must assume that users are not necessarily in a secure environment in the traditional sense. Users will be connecting to their corporate network from many venues such as through an unsecured wireless network in a public cafe. To support ubiquitous access while maintaining security, organizations are turning to enterprise identity management solutions which can simplify user authentication and access controls for the wide variety of applications and data that many organizations must cope with. Identity management offers automated provisioning of user profiles and role-based access controls to enhance efficiency and reduce the risk of errors in maintaining access rights.

In addition to identity management solutions, other IT technologies are evolving to combine policy with data in an automated fashion. For example, today's Web services and Service Oriented Architecture (SOA) environments can enable security and privacy access permissions and policies to be packaged right along with the information being delivered. Messages based on Simple Object Access Protocol (SOAP) and the eXtensible Markup Language (XML) document format can provide a means to embed policy information including how to decode message data. When these message formats are coupled with encryption technologies, policy information is contained in the message and travels with the message as it is passed between application services and users of those services on the network. The combination of identity management and these messaging and encryption tools can enable data access to be managed on a transaction basis. This provides a tremendous degree of flexibility because data protection schemes can then match the context of how each piece of data should be used.

Since security, privacy and usage policies travel with the data, there can be free flow of information into and out of an IT environment. Information flow is controlled by properly identifying recipients and verifying their access rights before enabling them to decrypt and view the data. Identity management solutions and encryption technologies have therefore become important tools in today's IT environments and access to information is identity-driven.

The free flow of information has enabled businesses to be more responsive to customer needs by building dynamic relationships that are based on the user's activity. For example, an online travel reservations site can build a user profile that includes personal information such as frequent flyer numbers and credit card payment information that can be reused for future reservations. That same company can also offer value added services such as automated calls to the user's cell phone to alert the user about flight status. Many users want an advanced warning if a flight is delayed, but will only provide their cell phone number because they trust that this is the only reason that number would be used. Users might also receive a suggestion to participate in a community of people that have similar travel interests and are willing to share travel tips. As mentioned earlier the value provided by such a community is based on the value of the shared information to each community member and the trust that the user can have access to this information without threatening their own privacy.

None of this would be possible if the user did not have trust in the privacy policies of the community. If the user believed that their address and credit card information might get into the wrong hands, there would be no relationship at all. For the travel company, the trusted community of travel customers is the primary asset of the business, without which the business could not survive. Similar communities of customers, partners, or suppliers are the lifeblood of today's business, regardless of industry. These types of communities depend on sharing and can thrive when there are clear rules of engagement and there is trust about how personal information will be used.

### **Privacy as a Foundation for Trust and Community**

Knowing that trust is vitally important to the success of online communities, organizations must make sure that users are fully informed and understand the organization's intentions for collecting and using personally identifiable information such as address, phone number, driver's license number before the information is used. One of the most effective ways of achieving this understanding is through "informed consent." Informed consent, in this context, is broader than a simple opt-in or opt-out process which can sometimes be misleading to a user if they don't understand the consequences or the context of how the data will be used or managed. Informed

consent requires full disclosure about not only the intent to collect private data, but also how it will be used or shared.

To realize the full value of community participation, organizations must operate on the basis of informed consent. Users should understand the context of how their personal information might be used and it should be explained in clear language. Before collecting personal information, organizations should disclose:

- Types of personal information to be collected
- What will be done with the information including how it will be used and whether it will be shared with any outside parties
- Where the data will be used, especially if it is crossing international borders
- How long the personal information will be maintained and how it will be discarded

This kind of disclosure gives users an opportunity to make an informed choice about whether they want to engage in a relationship on these terms or not. For example, if users fully understand that signing up for airline special offers requires giving a valid email address to receive the offers and that this email address will not be used for any other purposes, they can feel safe in giving out their email address. If on the other hand the airline were to have a policy of allowing partners to solicit to these users as well and this was not made clear when the user opted-in, then trust would be broken and the user would be much less likely to continue the relationship.

The two-way communication that is necessary for thriving communities requires trust in the owner of the community. Informed consent is the foundation for trust and a requirement for successful communities in the participation age. Conversely, abusing personal information can result in chaos and a breakdown of the online community.

*“Our research shows that 80% of our customers would walk away if we mishandled their personal information.”*

CPO, Royal Bank of Canada, 2003

*“When customers DO trust an online vendor, they are much more likely to share personal information. This information then enables the company to form a more intimate relationship with its customers.”*

Frederick F. Reichheld, *Loyalty Rules: How Today's Leaders Build Lasting Relationships*

## **Turning Policy Into Practice — Integrating People, Processes, and Tools**

Once committed to a privacy policy, the execution on that commitment requires a combined approach of educating people, defining and implementing the proper business processes, and taking advantage of the latest technologies and tools. The combination of these three ingredients is necessary to create value and facilitate trusted participation.

Technologies that help protect confidentiality, control access to data, and enforce enterprise data management policies are enablers for privacy, but don't address the decision making around how personal information will be used by the organization. Building trusted relationships with an online community also requires attention to people and process.

Privacy and other relevant policies must be integrated into an organizations business processes and systems and should become a company value that is ingrained throughout the organization. This requires a focus on training people that will have a role in creating, monitoring, and enforcing policy driven systems and commitments. An organization's most critical asset is its information and protecting this information requires true governance through privacy policies that have become part of the organizational and community culture. An informed organization has an inherent competitive advantage for sustainable growth. Companies that safeguard people's personal data will build trust and loyalty and will be able to offer more and better services to their online communities, enabling them to prosper.

The investment required to implement these policies across the organization is small compared to the value that can be generated from thriving communities.

#### **For More Information**

For more information on how Sun technology can help support privacy and governance policies and practices visit the Web links in Table 1 below or send email to [privacy@sun.com](mailto:privacy@sun.com).

*Table 1. Web Links for Additional Information*

<b>Web Site URL</b>	<b>Description</b>
<a href="http://sun.com/privacy/">sun.com/privacy/</a>	Sun online privacy policy
<a href="http://sun.com/security/">sun.com/security/</a>	Sun security solutions
<a href="http://sun.com/identity/">sun.com/identity/</a>	Sun identity management solutions

Copyright © 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.