

A decorative graphic on the left side of the page, consisting of several overlapping, semi-transparent, curved shapes in shades of gray and blue, creating a layered, abstract effect.

Privacy for Pragmatists A Privacy Practitioner's Guide to Sustainable Compliance

August 2005

Table of Contents

Executive Summary	3
How Sun's Experience Can Help Guide Your Privacy Initiatives.....	3
Defining Practice Guidelines for Protecting Data Privacy.....	3
Obtaining Informed Consent	4
What have we learned?.....	4
What remains to be done?.....	4
Intended Use of Personal Data	5
What have we learned?.....	5
What remains to be done?.....	5
Collecting Only Necessary Data	6
What have we learned?.....	6
What remains to be done?.....	6
Securing Personal Data	7
What have we learned?.....	7
What remains to be done?.....	7
Access Accountability	8
What have we learned?.....	8
What remains to be done?.....	8
Third Party Access to Personal Data	9
What have we learned?.....	9
What remains to be done?.....	9
Retention of Personal Information	10
What have we learned?.....	10
What remains to be done?.....	10
Conclusion	11
Profiting from Pragmatic Privacy.....	11

Executive Summary

How Sun's Experience Can Help Guide Your Privacy Initiatives

Data privacy lapses are front-page news, and regulators are responding. As a result, C-level executives with fiduciary responsibility are carefully reviewing their organizational processes and physical and IT infrastructures to update and prioritize privacy-related activities. The goal is ultimately to better manage vulnerability to security and data privacy threats.

Sun is no exception. As a public company operating internationally, Sun is subject to the Sarbanes-Oxley Act of 2002, the European Union Data Protection Directive, and California Senate Bill 1386, to name just a few regulations governing data privacy and integrity. As in many multi-national businesses, the Sun Privacy Office's time these days is spent developing and communicating strategies both to manage these compliance issues and to provide critical information to the appropriate people at the appropriate time.

The following are some basic technology-independent practice guidelines, grounded in privacy fundamentals, that we believe can help ensure that decisions are made for the right reasons and that appropriately protected data can continue to flow.

Defining Practice Guidelines for Protecting Data Privacy

As a network-centric organization, Sun has always made data integrity and availability protections essential components of its products, architectures, and business relationships. With this basic privacy-friendly architecture in place, we have defined the following guidelines to align traditional practice with the ever-expanding overlay of regulatory policy and privacy sensitivities.

1. Informed consent will be obtained from users before collecting personal information or using data in a new or unexpected fashion.
2. Personal data will only be used for the purpose for which it was intended. Sun's policies will be enforced on a global basis even when local laws are less stringent.
3. Only data that is necessary for a justifiable business use will be collected. Scope of the permission and consent for use of personal information must be understood by any person, system, or organization to which the personal information is transferred or by which it is managed.
4. Personal data will be kept secure to prevent unauthorized access and use. Security will be equally maintained for both live and archived data throughout its life cycle.
5. Persons with access to or management responsibilities for personal data will be trained and accountable for executing on Sun's data privacy policies.
6. Third parties with access to personal data will be required to abide by Sun's policies and appropriate terms and conditions for protecting that data.
7. Retention of personal information will be within a limited timeframe and will include a plan for data destruction.

Let's look at each of these areas more closely.

Chapter 1

Informed consent will be obtained from users before collecting personal information or using data in a new or unexpected fashion.

We are acutely aware of the need to carefully manage and protect information that's collected from customers online. Sun, working cooperatively with legal, IT, marketing, and security teams, has developed a consistent and effective data management policy and privacy agreement to govern e-marketing operations. We have assured ourselves through extensive testing that the policy is readable and backed up with internal guidelines and procedures. These guidelines and procedures have created a common language for e-marketers wanting to leverage the Internet as a tool and for consumers wishing to engage with Sun. We have made the policy easily accessible by posting the link prominently on our web properties and displaying it whenever data capture is requested. In addition, behind the scenes, we provide an easy mechanism for customers to update their information or just ask questions. Managers of programs that collect and manage personally identifiable information (PII) are held accountable for using in-house training tools and leveraging international Sun data privacy communities of experts to get the job done right.

What have we learned?

The people building the data capture systems at Sun believe in respecting data privacy. By working with them in joint efforts such as the Sun Privacy Council, Sun's Privacy Office has been able to help ensure that they do the right thing — and that they do it consistently and uniformly, with less of the variation, review, and risk associated with customized efforts. As Sun has developed new connected customer services and other new technologies that may impact our privacy profile, the privacy team has been a core member of the planning and design processes, to help design in the controls from the beginning.

In short, privacy becomes a passion to those who understand the simplicity, accuracy, and efficacy of managing data to a high level of excellence. This commitment to doing the right thing results in better compliance and a lower risk profile for the corporation.

What remains to be done?

Customer, partner, and employee data are rich business assets to be appropriately valued and defended. Sun's challenge now is the responsible stewardship of that data throughout its life cycle. We're working on tracking the respective processes from collection to active management and appropriate use to destruction, and making those processes more visible, more automated, and more reliable. Scale matters when it comes to best practices, particularly when those in research labs, on product teams and even in marketing may not have traditionally viewed data protection as a key part of their success.

Chapter 2

Personal data will only be used for the purpose for which it was intended. Sun's policies will be enforced on a global basis even when local laws are less stringent.

Before data is collected, to preserve information value to the enterprise and keep privacy promises to the owners of that information, there must be a process in place that correctly identifies personal data and links it to systems based on who needs it and why. Active management of access is crucial because authentication of an authorized user is only part of the story. Consider the many roles filled by an individual who may have access to personal data: an employee may also be a manager, a consumer, a content creator and a fiduciary officer—and may need to view and share different types of information in each of these roles. To help ensure that this happens in a way that's consistent with Sun's practice guidelines, Sun applies a combination of education and technology at capture points and at use points.

What have we learned?

The cost of being open, secure, and compliant need not be prohibitive. Creating globally available information systems that rely on Internet and web services standards makes it possible to improve both capabilities and efficiencies. For example, a Sun employee uses a secure web portal that is customized to different roles and linked into the role-based access controls in Sun's directory system. The directory is updated dynamically through links to HR systems that can turn on and off specific privileges. By tapping into the identity infrastructure to manage roles and access privileges companywide, Sun is able to streamline individual access (reducing the number of passwords that users have to remember, for example) and, at the same time, reduce the cost and increase the consistency of user administration.

People and processes work in tandem with the technology infrastructure to fill gaps where automation and technologies leave off or where in-person judgment provides better service to the data owner who has entrusted information to our care. Training never stops. A partnership with legal teams that have global expertise, coupled with education regarding the products and services that are core to our business, help define process and create the metrics that make us successful.

What remains to be done?

Constant consideration about how to simplify processes so that they apply as broadly as possible across regulations is key to ongoing synergy between legal requirements, business and policy needs, and IT capabilities.

With a few notable exceptions, the vast majority of the requirements of these regulations—about 80%—are the same. Many seemingly new requirements in one geography or line of business are already part of an existing requirement from another place or area of focus, and most of them draw from established data hygiene and data governance practices. Local requirements are better supported by flexible systems that allow segmentation and separation where necessary and integrate separate systems where required through standards-based channels such as web portals. Global delivery of a strong infrastructure that can be broadly applied will make it possible to meet the needs of new regulations with a minimum of disruption and expense.

Chapter 3

Only data that is necessary for a justifiable business use will be collected. Scope of the permission and consent for use of personal information must be understood by any person, system, or organization to which the personal information is transferred or by which it is managed.

When it comes to data capture, one business group's definition of "justifiable" may not match another's. That's why it's important to keep an open line of communication through which different parties can come to agreement about what's justifiable. Clear and conspicuous notice regarding the purpose for which data is managed is key to compliance, especially in light of requirements that govern trans-border transfers for data and security assurances.

What have we learned?

Awareness about how we actually use data assets before we collect them has positive benefits far beyond those of privacy enablement. Transparency to customers and employees, for one, is a big part of an organization's ability to satisfy that data owner.

Privacy Impact Assessments (PIAs) and similar risk assessment tools give a common set of questions for systems owners and users to answer to determine the nature of data collected and managed, where this activity will take place (from the perspective of the data center as well as the system or human accessing data), the type and effectiveness of proposed security tools and procedures employed, and more. Once we define the asset to be protected, we understand what the enterprise risk profile will be and we can clearly articulate what the expected RODA (return on data asset) should be before personal data is collected.

What remains to be done?

Across all the organizations that collect, manage, and use personal data, risk assessment and a common set of understood business justifications must be normalized and turned into standards. Auditing to understand where the people-processes-tools system is successful and where it needs improvement is an important but often manual and costly undertaking.

Great progress has been made to audit workflows and identity management systems. New tools and standards with an emphasis on interoperability among heterogeneous systems continue to provide automated insight to personal information from the time a user authenticates himself or herself into a system to the time that that data is permanently deleted (or effectively deleted by encrypting the data and throwing away its key).

Chapter 4

Personal data will be kept secure to prevent unauthorized access and use. Security will be equally maintained for both live and archived data throughout its life cycle.

Historically, security has included a focus on secrecy and intrusion prevention. Data privacy sensitivity means implementing finer-grained controls over systems and data access, often to prevent “authorized” users from gaining access to data that is inappropriate for that person's function or need to know. Today, fortunately, there exists a good deal of technology for systems and application level protection of personal information (such as role-based authentication and access management tools, layered defenses, real-time access controls, encryption, and more), as well as a solid understanding of how to deploy it.

What have we learned?

The more integrated security functions are with processes, people, and tools, the easier it is to build, maintain, and improve the security infrastructure. This is increasingly becoming the norm as more security- and privacy-enhancing features are built into mainstream products, like portal access and operating environments, and as security is elevated in organizational stature and visibility. Maintaining an open relationship with the CISO and other key data stewards within the organization is one of the best ways to ensure that the Privacy Office stays on top of new privacy threats and effectively supports privacy of data.

What remains to be done?

Secure archival of data across the life cycle of use is critical. Security processes designed for systems now need to be extended to services and the life cycle of information use. Think of security services and identity services running on a utility computing grid: the CPU and storage systems are fairly straightforward to manage. But how do you ensure that privacy policies are respected and maintained in a virtual world that cannot be physically identified?

Sun faced part of this challenge when we deployed improved authentication and access controls for highly distributed and mobile workforces. Doing so involved authenticating the identities of people authorized for access, factoring in their location and level of trust (home system vs. Internet kiosk, for example), displaying appropriate data, auditing their access, and streamlining the processes associated with managing access. Such an endeavor can be particularly challenging when dealing with systems outside the organization, through outsourcing or supply chain integration (see Chapter 6).

Chapter 5

Persons with access to or management responsibilities for personal data will be trained and accountable for executing on Sun's data privacy policies.

As important as automation has become, it will never eliminate the role of people in enforcing privacy policies. Sun has done a tremendous amount of training around this issue, from mandatory in-person training for financial teams worldwide, to live and web-based legal training for marketing personnel who capture and handle personally identifiable information (PII). Part of the training is educating users on what PII is and how to capture, control, and archive it reliably and retrievably.

What have we learned?

By instituting training processes that have senior management support, Sun is in a better position to handle evolving policy requirements. And users become accustomed to thinking about privacy issues as part of their day-to-day activities. As noted above, where data strategy is often first viewed as yet another compliance necessity, understanding and use of personal data in a privacy-enhancing fashion is likely to breed better and more efficient use of data and a passion for a job well done.

What remains to be done?

As people change roles and leave behind responsibilities, they also leave behind databases, programs, and systems that contain personal information for which we remain fiduciaries. Sun is constantly exploring new ways to document and manage data to ensure we follow through on privacy obligations and to maintain the value of data assets. We are also inventing new ways to associate policies and documentation to allow more automated and consistent destruction where appropriate.

Chapter 6

Third parties with access to personal data will be required to abide by Sun's policies and appropriate terms and conditions for protecting that data.

Outsourcing of IT, HR, and manufacturing has made third parties a vital part of Sun's business model. The company manages these relationships through the centralized definition and administration of consistent policies. In this effort, Sun has relied extensively on its own experience in defining security processes, architectures, and user roles and separation of duties, extending those definitions and authentication practices to third parties. However, business partners have their own compliance procedures and processes along with regulatory and legislative requirements that they must adhere to—further complicating each compliance scenario. Sun works closely with third parties to coordinate policies and processes.

What have we learned?

Anonymizing data is a valuable tool when working with third parties. If identifying information is eliminated, information can be shared freely without jeopardizing privacy. For example, Sun has now outsourced much of its employee benefits and management. To test the implications of privacy, the company chose a small project that wasn't mission-critical and worked with one partner to federate systems. Together, the two companies designed a strategy for sharing information and technologies, looking for ways to automate protections and manage risk. This upfront planning helped enable ongoing interoperability and consistent policy enforcement, creating an environment that minimized the potential for risk while enhancing the opportunity for collaboration. The learning on data usage, process and relationship documentation, and access to data in transit through the system has been enormously valuable as we define requirements for more business-critical outsourcing projects. (We've also helped our partner achieve a competitive edge.)

What remains to be done?

Sun is helping its partners adopt more standards to make it easier to integrate and sustain the company's privacy policies. Contracts are being negotiated to include the necessary standards-based infrastructure. This makes the true costs more apparent up front and helps Sun design in knowledge transfer time. The employee life cycle is also an important consideration in third-party relationships. Turnover is high at many outsourcing organizations, and it's important to ensure that data is locked and that access rights disappear immediately when the employee is terminated.

Chapter 7

Retention of personal information will be within a limited timeframe and will include a plan for data destruction.

In defining personal information to be captured, Sun also defines a timeframe for retaining that data. However, the time has to be linked to the roles and rules for that data. Employee data is retained for the employment period plus x years. Opt-in prospect data is retained until the prospect opts out or has been inactive for a specified period of time.

What have we learned?

Having the right tools and technologies to support corporate policies assists in automation, auditing, and compliance with both internal policies and privacy regulations. By designing practices into business processes, Sun improves the overall protection profile, as well as reducing the cost and effort for the employees and auditors.

What remains to be done?

There are still some tough questions to answer around the issue of data retention and destruction. For example, what is the appropriate retention limit for customer data—especially as legal case experience redefines best practice monthly? What about evidence retrieval for litigation responses? Variation across regulations and geographies sometimes means that questions like these have more than one right answer—and the policies change as consumer knowledge and fear increase. These open areas are where we as a community need to invest time to educate and drive governmental policy in ways we can actually support with processes and systems.

Conclusion

Profiting from Pragmatic Privacy

Sun's practice guidelines are important because they help improve Sun's business capabilities. By considering privacy compliance requirements earlier rather than later, it's possible to minimize disruption and deliver on the CPO's primary job responsibility: enabling access to business information. Having good control of information allows you to share appropriate data with appropriate parties on time and securely.

Privacy isn't about closing doors. It's about controlling how and when and for whom they are opened. This control generates power and trust in the systems, and it inspires the confidence to rely on them. This assurance is increasingly critical to carrying out the ongoing responsibility of protecting the privacy of personally identifiable information.

