Comments of ARMA International
Information Privacy and Innovation in the Internet Economy
[Docket No. 100402174–0175–01]
RIN 0660–XA12

Submitted electronically (as a PDF document) to: privacy-noi-2010@ntia.doc.gov by fmoore@smithbucklin.com for Bob.Tillman@armaintl.org.

Subject line: "PRIVACY NOTICE OF INQUIRY DOCKET NO 100402174-0175-01"

Date: June 7, 2010

INTRODUCTION AND SUMMARY

ARMA agrees with the importance of creating systems and regimes that will give consumers the confidence that their personal information is properly created, managed, used and disposed of relative to engaging in Internet commerce –

> Consumers have expressed concern regarding new or unexpected uses of their personal information by online applications. Since Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained. At the same time, companies need **clear policies**[1] that enable the continued development of new business models and the free flow of data across state and international borders in support of domestic and global trade. Our challenge is to align flexibility for innovators along with privacy protection.

ARMA commends the Department[2] in its search for policies that will –

---

[1] ARMA has long held that safeguarding records, information and data depends not only on effective and emerging tools, but also on flexible, principles-based recordkeeping programs – articulated as policies and procedures that are endorsed across an enterprise and supported by an organization's senior leadership.

[2] Office of the Secretary, U.S. Department of Commerce; National Telecommunications and Information Administration, U.S. Department of Commerce; International Trade Administration, U.S. Department of

1. Enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy

2. Enhance the public confidence necessary for full citizen participation with the Internet

3. Uphold fundamental democratic values essential to the functioning of a free market and a free society.

We also look forward to the progress of the Task Force[3] and its ability to identify and evaluate privacy challenges[4].

Of particular interest to ARMA is the observation –

> In addition to the growth of online commerce, the Internet, the World Wide Web, and associated information systems have lead to an unprecedented growth in productivity over the last decade. More businesses are using the Internet to provide **electronic records** to customers and trading partners, and enterprises are shifting to a digital back office and greener business environment. Although this has spurred additional green innovation, the fact that increasingly **more data is being stored electronically and aggregated** creates new challenges in the privacy arena.
>
> Sustaining the growth of digital commerce and U.S. commerce generally will require continued innovation in **how information is used**

Commerce; and National Institute of Standards and Technology, U.S. Department of Commerce.

[3] Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education and political and cultural life, the Department has made it a top priority to ensure that the Internet remains open for innovation. The Department has created an Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment.

[4] Responses to this Notice will assist the Task Force in preparing its report on Privacy and Innovation in the Information Economy. The purpose of this report will be to identify and evaluate privacy policy challenges, and to analyze various approaches to meet those challenges.

and shared[5] across the Internet. Commerce today depends on online communication and the transmission of significant amounts of data. Key to the current inquiry, the Department believes this development places **data protection**[6] in a new light.

With these comments, ARMA respectfully recommends the use of *generally accepted recordkeeping principles* for addressing concerns relating to the use and protection of records and files of all formats, which will contain personal information required in commerce today. Internet commerce will present its own challenges relative to tools (technology) that should be employed, but ARMA believes that more effective protections are achieved by combining appropriate tools with enterprise-wide policies and procedures that speak to the management of records and information.[7] The information collected from consumers and maintained, used, and disposed of by various business models are records, however stored, and should be covered by appropriate

---

[5] How information is used and shared is better characterized as an organization's recordkeeping policies and procedures (program), and as such, would speak to the creation, retention, and disposition, including destruction as and when appropriate, of records of information.

[6] Effective data protection will include an enterprise-wide program of policies and procedures that speak to the life cycle management of information sought to be protected. ARMA believes that the most innovative approach to data management (and therefore protection) is through a flexible application of generally accepted recordkeeping principles. A principles-based approach to data management will allow organizations to tailor programs to their sectors, business models, and types of records and information required. Generally accepted recordkeeping principles also speak to 1) transparency of an organization's recordkeeping program – documenting the disposition of information in an understandable manner, and 2) accountability through the support of senior management and adoption of policies and procedures to guide personnel and ensure program auditability.

[7] From the perspective of ensuring appropriate management of personal information, it should be unnecessary to distinguish between online commerce and other forms of commerce where the sellers of goods or services also collect information from clients, consumers, patients or others with relationships with vendors and providers.

recordkeeping policies, informed by generally accepted recordkeeping principles, and supported by appropriate technology.[8]

The *generally accepted recordkeeping principles* speak to accountability, transparency, and compliance by the enterprise and integrity, protection, availability, retention and disposition of records and information. These principles create a foundation for an appropriate and effective recordkeeping program that speaks to enterprise-wide commitments and life cycle management of records and information – and their flexibility provide appropriate and effective application to protecting personal information associated with Internet commerce and in the possession and custody of Internet businesses. With these principles –

1. The enterprise would establish a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

2. The recordkeeping program would be constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate manner and the appropriate or required time, and such disposition is documented.

GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES

ARMA believes that eight *generally accepted recordkeeping principles* can provide effective and objective guidance for the development of clear policies relative to managing records and information, including personal information that is part of Internet commerce.

---

[8] Furthermore, it should be noted that information collected on-line for purposes of enhancing Internet commerce, or supporting business models or consumer needs via the Internet, should be viewed as records, whether more accurately described as record series, files of records or classes of records.

Organizations have historically been challenged to establish appropriate and effective recordkeeping regimes, intended to promote records and information management that meets vital business needs, supports contractual obligations, and ensures compliance with statutory and regulatory obligations. Too often, by organizations and by those with oversight responsibilities over regulated entities, records and information management has been defined solely by regulatory requirements (e.g. safeguarding and disposal responsibilities as recognized by the Federal Trade Commission for non-financial institutions). However, protecting personal information from inappropriate or criminal use requires an enterprise-wide approach more comprehensive than simply complying with statutory and regulatory recordkeeping regimes (often referred to as "document retention").

ARMA believes that recordkeeping requirements can and should be tailored to any organization that possesses and controls personal information. This makes it more likely that organizations will voluntarily develop and engage meaningful recordkeeping, and it also provides guidance to others looking to organizations to demonstrate the stewardship over records and information reasonably expected of them[9].

Relative to this inquiry, ARMA further believes that a principles-based standard will position organizations to more likely mitigate known and unknown risks and creates a reasonable standard for purposes of determining compliance with any statutory or regulatory requirements.

As such, the policies and procedures that should be expected of these organizations are made most effective, with objectivity and reasonable levels of investment, by being based on the *generally accepted recordkeeping principles* set forth below – recognizing at the very least that no one size or format of any operational policies and procedures will fit all similarly situated entities.

For these reasons, ARMA recommends, as the foundation of any expectations that may be created regarding clear policies for managing personal information, that the Task Force look to these *generally accepted recordkeeping principles* –

---

[9] We note the expectations of customers and consumers that their personal information be appropriately safeguarded. As such, the most effective safeguards are those that are made systemic to the entire organization through known policies and procedures.

Accountability – An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.

Essential to this principle are the following program elements:

1. The records manager is an officer of the organization and is responsible for the tactical operation of the ongoing program on an organization-wide basis.
2. The records manager is actively engaged in strategic information and record management initiatives with other officers of the organization.
3. Senior management is aware of the program.
4. The organization has defined specific goals related to accountability.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The records manager is a senior officer responsible for all tactical and strategic aspects of the program.
2. A stakeholder committee representing all functional areas and chaired by the records manager meets on a periodic basis to review disposition policy and other records management-related issues.
3. Records management activities are fully sponsored by a senior executive.

Transparency – The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

Essential to this principle are the following program elements:

1. Transparency in recordkeeping is taken seriously and information is readily and systematically available when needed.
2. There is a written policy regarding transparency.
3. Employees are educated on the importance of transparency and the specifics of the organization's commitment to transparency.
4. The organization has defined specific goals related to transparency.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Exceeds the essential elements above in the following ways:
    a. Transparency is an essential part of the corporate culture and is emphasized in training.
    b. The organization monitors compliance on a regular basis.

Compliance – A recordkeeping program shall be constructed to comply with the applicable laws and other binding authorities, as well as the organization's policies.

Essential to this principle are the following program elements:

1. The organization has identified all relevant compliance laws and regulations.
2. Record creation and capture are systematically carried out in accordance with records management principles.
3. The organization has a strong code of business conduct which is integrated into its overall information governance structure and recordkeeping policies.
4. Compliance and the records that demonstrate it are highly valued and measurable.
5. The hold process is integrated into the organization's information management and discovery processes for the "most critical" systems.
6. The organization has defined specific goals related to compliance.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The organization has implemented systems to capture and protect records.
2. Records are linked with the metadata used to demonstrate and measure compliance.
3. Employees are trained appropriately and audits are conducted regularly.
4. Records of the audits and training are available for review.
5. Lack of compliance is remedied through implementation of defined corrective actions.
6. The hold process is well-managed with defined roles and a repeatable process that is integrated into the organization's information management and discovery processes.

Integrity – A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.

Essential to this principle are the following program elements:

1. The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes.
2. Appropriate data elements to demonstrate compliance with the policy are captured.
3. The organization has defined specific goals related to integrity.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. There is a clear definition of metadata requirements for all systems, business applications, and paper records that are needed to ensure the authenticity of records.
2. Metadata requirements include security and signature requirements and chain of custody as needed to demonstrate authenticity.
3. The metadata definition process is an integral part of the records management practice in the organization.

Protection – A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.

Essential to this principle are the following program elements:

1. The organization has a formal written policy for protecting records and centralized access controls.
2. Confidentiality and privacy are well defined.
3. The importance of chain of custody is defined, when appropriate.
4. Training for employees is available.
5. Records and information audits are only conducted in regulated areas of the business. Audits in other areas may be conducted, but are left to the discretion of each function area.
6. The organization has defined specific goals related to record protection.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The organization has implemented systems that provide for the protection of the information.
2. Employee training is formalized and well documented.

3. Auditing of compliance and protection is conducted on a regular basis.

Availability – An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Essential to this principle are the following program elements:

1. There is a standard for where and how official records and information are stored, protected, and made available.
2. Record retrieval mechanisms are consistent and contribute to timely records retrieval.
3. Most of the time, it is easy to determine where to find the authentic and final version of any record.
4. Legal discovery is a well defined and systematic business process.
5. The organization has defined specific goals related to availability.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. There are clearly defined policies regarding storage of records and information.
2. There are clear guidelines and an inventory that identifies and defines the systems and their information assets. Records and information are consistently and readily available when needed.
3. Appropriate systems and controls are in place for legal discovery. Automation is adopted to facilitate the implementation of the hold process.

Retention – An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.

Essential to this principle are the following program elements:

1. A formal retention schedule that is tied to rules and regulations is consistently applied throughout the organization.
2. The organization's employees are knowledgeable about the retention schedule and they understand their personal responsibilities for records retention.
3. The organization has defined specific goals related to retention.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Employees understand how to classify records appropriately.
2. Retention training is in place. Retention schedules are reviewed on a regular basis, and there is a process to adjust retention schedules as needed.
3. Records retention is a major corporate concern.

Disposition – An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.

Essential to this principle are the following program elements:

1. Official procedures for records disposition and transfer are developed.
2. Official policy and procedures for suspending disposition have been developed.
3. Policies and procedures exist and they are standardized across the organization.
4. Individual departments have devised alternative procedures to suit their particular business needs.
5. The organization has defined specific goals related to disposition.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Disposition procedures are understood by all and are consistently applied across the enterprise.
2. The process for suspending disposition due to legal holds is defined, understood, and used consistently across the organization.
3. Electronic information is expunged, not just deleted, in accordance with retention policies.

RESPONSE TO NOTICE OF INQUIRY QUESTIONS

ARMA respectfully submits its comments to the questions raised by the Department and restated below, focusing our observations and recommendations on the role that programs, policies, and procedures relative to records and information management can play in effectively creating transparent and auditable regimes intended to safeguard personal information.

The U.S. Privacy Framework Going Forward

The Department raises the question whether the traditional "notice and choice" approach to consumer protection may be outdated, especially in the context of information-intensive, highly interactive, Web-based services:

Does the existing privacy framework provide sufficient guidance to the private sector to enable organizations to satisfy these laws and regulations?

ARMA has long believed that "notice and choice" does not on its own evidence appropriate data management or demonstrate necessary or appropriate safeguards of personal information.[10] Notice can be considered a statement of intention by an organization without demonstrated regimes or mechanisms in place to ensure, document, or audit compliance. Choice is rendered meaningless if personal information is required for the provision of specific goods and services.

Are there modifications to U.S. privacy laws, regulations and self-regulatory systems that would better support innovation, fundamental privacy principles and evolving consumer expectations? If so, what areas require increased attention, either in the form of new laws, regulations or self-regulatory practices?

The various regimes established by statute or regulation that speak to protecting the personal information lack 1) a comprehensive approach to the management of information and 2) a clear statement of core principles upon which a management regime should be built. ARMA believes that any program established to protect personal information should be applied across the entire enterprise and thereby deeply imbedded in the business model and mission of the organization. Rather than simply speaking to specific information by establishing retention schedules or requiring safeguarding regimes, ARMA believes that the integrity and management of information is most effectively and efficiently achieved by an enterprise-wide commitment to processes and procedures that ensure –

The enterprise establishes a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and

---

[10] See Final Model Privacy Form Under the Gramm-Leach-Bliley Act: A Small Entity Compliance Guide issued by the Security and Exchange Commission at http://www.sec.gov/divisions/marketreg/tmcompliance/modelprivacyform-secg.htm.

guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

The recordkeeping program is constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate manner and the appropriate or required time, and such disposition is documented.

What is the state of efforts to develop a self-regulatory privacy framework? Are there certain minimum or default requirements that should be incorporated either into self regulation or to law?

ARMA believes that the *generally accepted recordkeeping principles* provide the foundation for voluntary, sound business practices relative to managing records and information, as well as for any recordkeeping and information management requirements established through statute or regulation. A principles-based approach allows the necessary flexibility to ensure a recordkeeping program is appropriate to the organization and meets the needs and expectations of regulators, enforcement agencies, and the general public.

What is the proper goal of privacy laws and regulations: Should the focus on commercial data privacy policy be on satisfying subjective consumer expectations or is it also necessary to enact objective privacy principles?

ARMA supports the concept of principles-based privacy and recordkeeping programs. Various iterations of fair information practices have been promoted over the years[11], and these stand as sound guidance for policy

[11] For a currently posted articulation of fair information practices by the FTC, see http://www.ftc.gov/reports/privacy3/fairinfo.shtm. However, it should be noted that this iteration relies on both notice and consent. See the testimony of Robert Pitofsky, Chairman of the Federal Trade Commission (May 25, 2000) on the same: http://www.ftc.gov/os/2000/05/testimonyprivacy.htm.

makers and business leaders[12]. ARMA believes that safeguarding and disposal requirements, as well as fair information practices, are incorporated, appropriately, in the recognized generally accepted recordkeeping principles. Treated in isolation, safeguarding, disposal or other attempts to address protection, are at risk of being less effective, less efficient, and easily marginalized in enterprises whose business models rely so intensely on information sharing and consumers' willingness to add their personally identifiable information to the records and files of Internet businesses. These privacy principles are incorporated in and enhanced by an enterprise-wide recordkeeping program, which speaks not only to privacy principles (protection of personal information), but also to senior management engagement, transparency, auditability, and appropriate life cycle management.

Sectoral Privacy Laws and Federal Guidelines

The various sectoral privacy laws and regulations[13] have emerged in the absence of a more comprehensive approach to the stewardship of records and

---

[12] ARMA believes that a principles-based approach, focusing on outcomes relative to records and information, is applicable to both public and private sector entities. See *Memorandum Number: 2008-01* (December 29, 2008) for 8 Fair Information Practice Principles endorsed by the Department of Homeland Security pursuant to the Privacy Act of 1974: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[13] As defined by this Notice: "The U.S. privacy framework is composed of sectoral laws combined with constitutional, statutory, regulatory and common law protections, in addition to industry self-regulation. Sectoral laws govern the handling of personal data considered most sensitive. For instance, the Communications Act includes privacy protections that telecommunication providers and cable operators must follow when handling the personal information of subscribers. The Health Insurance Portability and Accountability Act (HIPAA) stipulates how "covered" health care entities can use and disclose data. The Fair Credit Reporting Act (FCRA) governs how consumer reporting agencies share personal information. The Gramm-Leach-Bliley Act (GLBA) covers certain data held by financial institutions. The Children's Online Privacy Protection Act (COPPA) protects information collected online about children under 13. In addition to these sectoral laws, the Federal Trade Commission Act (FTC Act) provides the FTC authority to combat "unfair or deceptive" business practices. The FTC also provides guidance for businesses regarding privacy and security practices. These laws and guidelines affect U.S. economic activity by controlling how organizations

information that are either required by regulators or enforcement agencies, or are created through the business imperative or other mission critical aspects of an organization.

How does the current sectoral approach to privacy regulation affect consumer experiences, business practices or the development of new business models?

ARMA believes that this sectoral approach represents a well intended effort to address the privacy expectations of society; however, the effect of this approach has been to create silos in the management of records and information throughout an organization that result in inefficiencies, break downs in effective auditing and compliance measures, and ignores the practical fact that records and information are not used in isolation to other functional or business activities within most organizations today.

How does the sectoral approach affect individual privacy expectations?

This sectoral approach unintentionally results is unnecessary confusion for most individuals. Individuals are faced with notices at their various health care provider offices, such as doctors, dentists, other specialists, as well as providers such as hospitals. Individuals also receive these notices from various financial institutions, and increasingly online as a part of Internet commerce. It is unlikely that most individuals could articulate what these notices say or what obligations if any they impose on the persons or entities giving notice.

More importantly, however, these sectoral requirements have failed to demonstrate to the general public that a set of core principles exist that are applicable to any personal information an individual is required or expected to divulge in the course of seeking goods or services in today's economy.

What practices and principles do these sectoral approaches have in common, how do they differ?

Continuing the theme of our comments above, ARMA believes that these sectoral approaches have in common the fact that they are the result of public policy reactions, drawn as narrowly as possible around the records and

---

can use data to develop new products and services or improve existing ones. The laws and guidelines differentiate between categories of data (e.g., health care, financial and other), and they differentiate between data subjects (e.g., children and others)."

information in question, and that these approaches impose a silo-styled set of requirements for purposes of compliance.

Are there alternatives or supplements to the sectoral approach that should be considered?

As suggested above, ARMA believes that a principles-based approach to enterprise-wide management of records and information would result in efficiencies for the organizations required to comply with these sectoral approaches, establish a common set of expectations between these organizations and their regulators and any enforcement agencies with jurisdiction over their activities, and inform consumers of the core principles that every organization will employ in the management of their personal information.

What can be done to make the current framework more conducive to business development while ensuring effective privacy protections?

As noted above, a principles-based approach to managing records and information creates efficiencies for organizations, both in the consolidation of managing information across its various functions, but also in the consistencies created between regulatory requirements and best practices in the absence of statutory or regulatory mandates. A single set of principles, acknowledged by public policy and public expectations, enhances the ability of organizations, regulators, enforcement agencies, customers, consumers and business partners to understand and dialogue on common ground.

New Privacy-Enhancing Technologies and Information Management Processes

The Department points to researchers at universities, think tanks, international organizations and company laboratories that are developing privacy-enhancing technologies and business methods to implement company privacy policies and user preferences and to increase company accountability.

In particular, the Department asks: **What steps can be taken to assure that privacy-enhancing business processes are robust, complied with and regularly updated?**

ARMA believes that an application of generally accepted recordkeeping principles would uniquely motivate innovate business processes, consistent with the recognition that sector, size, complexity, and offerings will influence

the actual policies and procedures employed to appropriately manage records and information.

The Role for Government/Commerce Department

The Department notes that "surveys continue to indicate that consumers are concerned or confused about what happens to their personal information online," and asks for input on how to help address barriers to increased innovation and consumer trust in the information economy.

How can the Commerce Department help address issues raised by this Notice of Inquiry?

As discussed above, and consistent throughout these comments, ARMA believes that the sectoral approach to protecting personal information has created confusion for the general public and has left regulators with little assurance that records and information are accurate, that the recordkeeping practices of the subject organization is transparent and auditable, or that the expectation that personal information be appropriately managed has become an enterprise-wide value proposition.

ARMA urges the Department to consider the role of *generally accepted recordkeeping principles* in establishing clear policies for internal management, clear ground rules for regulators and enforcement agencies, and clear expectations for consumers.

CONCLUSION

With these comments, ARMA respectfully recommends the use of *generally accepted recordkeeping principles* for addressing concerns relating to the use and protection of records and files of all formats, which will contain personal information required in commerce today. Internet commerce will present its own challenges relative to tools (technology) that should be employed, but ARMA believes that more effective protections are achieved by combining appropriate tools with enterprise-wide policies and procedures that speak to the management of records and information of all types and for all purposes. Principles for the management of personal information does not require distinguishing between online commerce and other forms of commerce where the sellers of goods or services also collect information from clients, consumers, patients or others with relationships with vendors and providers.

The information collected from consumers and maintained, used, and disposed of by various business models are records, however stored, and

should be covered by appropriate recordkeeping policies, informed by generally accepted recordkeeping principles, and supported by appropriate technology. It should be noted that information collected on-line for purposes of enhancing Internet commerce, or supporting business models or consumer needs via the Internet, should be viewed as records, whether more accurately described as record series, files of records or classes of records.

ARMA supports the concept of principles-based privacy and recordkeeping programs. ARMA believes that safeguarding and disposal requirements are incorporated, appropriately, in an organization's recordkeeping program. Treated in isolation, safeguarding, disposal or other attempts to address protection, are at risk of being less effective, less efficient, and easily marginalized in enterprises whose business models rely so intensely on information sharing and consumers' willingness to add their personally identifiable information to the records and files of Internet businesses. Privacy principles are incorporated in and enhanced by an enterprise-wide recordkeeping program, which speaks not only to privacy principles (protection of personal information), but also to senior management engagement, transparency, auditability, and appropriate life cycle management.

These principles create a foundation for an appropriate and effective recordkeeping program that speaks to enterprise-wide commitments and life cycle management of records and information – and their flexibility provide appropriate and effective application to protecting personal information associated with Internet commerce and in the possession and custody of Internet businesses. With these principles –

The enterprise would establish a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

The recordkeeping program would be constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate

manner and the appropriate or required time, and such disposition is documented.

Respectfully submitted,
ARMA INTERNATIONAL