

Solving the Problem of Data at Risk



Although all industries face governance, compliance, and issues of data security, for state and local governments the challenge is enormously greater. The proliferation and collection of data that state and local agencies collect is staggering and is increasing at a compound annual growth rate of 60%. As more and more services are provided on-line to drive down costs, the sheer volume of information to be maintained is growing exponentially. With over 253 million data breaches in both the public and private sector since 2005, state and local governments must proactively address privacy data protection issues to reduce risks and potential liabilities. Personally Identifiable Information (PII) includes a broad range of data assets defined by laws and standards such as HIPAA and Payment Card Industry (PCI) compliance and a variety of PII is routinely collected by agencies.

Privacy data needs to be managed, protected, and processed differently. With information residing in diverse repositories, individual computers, email systems, scanned content, forms, and fax systems, can an organization guarantee that they do not have potential privacy exposures? **PII discovery** addresses information assurance and risk management challenges regarding privacy information. The solution delivers the ability to identify organizational unique privacy information regardless of where it resides. Once identified, this information can be automatically routed to secure locations for proper administration. It's not about what you know exists, it's about what you don't know exists.

With privacy issues, there is no compromise.

The Issues

Personally Identifiable Information (PII) fundamentally deals with privacy. As state and local governments embrace electronic processes in order to reduce costs and improve services to citizens, new issues in the protection of data assets, risk management, and liability protection are becoming equally important. Managing risk as well as protecting the confidentiality of information assets is an on-going iterative process. It goes far beyond the responsible maintenance of privacy data but must also address the identification of unknown privacy exposures for the appropriate management of data assets. The challenges facing state and local government include:

- ⇒ Lack of tools to identify all possible privacy data exposures at the time of content creation and modification
- ⇒ Lack of end user compliance to segregate content from the network and ensure that uploaded privacy data is not available for general access and protected accordingly
- ⇒ Lack of governance to enforce the meta-tagging of documents based on content by end users
- ⇒ Stove pipe applications that prohibit the ability to identify privacy data from within the content
- ⇒ No standard process that addresses all aspects of data privacy that are unique to the agency
- ⇒ Inability to automatically identify PII and exposure risks in real time
- ⇒ Inability to ensure protected data assets are subject to portability and security controls



For The Record

- ⇒ Average cost of a data breach was \$6.3 million and ranges from \$225K to \$35 million
- ⇒ The average cost per exposed record is \$197 and ranges from \$90 - \$305 per record
- ⇒ Only 35% of all breaches involved the loss or theft of a computer or device
- ⇒ Overall 70% of all breaches were due to a mistake or malicious intent by an organization's own staff
- ⇒ 65% of citizens expressed little confidence that government can be trusted to maintain and protect records about them appropriately
- ⇒ 58% of state and local government employees were only slightly confident or not confident that their electronic information is accurate, trustworthy, and accessible

The Solution

PII discovery is a unique solution that helps organization's manage the risk associated with enterprise content residing in diverse repositories.

The innovative technology identifies content through advanced meta-tagging and automatic classification features. As content is created or ingested, PII is automatically identified and classified to a folder for security and review procedures.

PII discovery enables the organization to define PII according to their specific requirements and needs. Types of PII can include social security numbers, credit card numbers, date of birth, bank account numbers, passports, drivers licenses, or any unique organizational descriptors. Features include:

- ⇒ Automatic metadata tagging and classification of PII based upon its presence within content
- ⇒ Once tagged and classified the content can be managed in accordance with regulatory or government guidelines
- ⇒ PII from diverse repositories including:
 - ◆ eMail servers
 - ◆ Fax servers
 - ◆ Forms and scanned documents
 - ◆ Microsoft Office Applications
 - ◆ Websites
 - ◆ Servers and PC's
- ⇒ PII is automatically aggregated into a central location for review and disposition
- ⇒ Standard process that addresses all aspects of data privacy that are unique to the organization



The Benefits

PII discovery provides state and local government with the ability to continually and consistently identify unknown privacy data exposures automatically. Based on organizational procedures the PII is segregated from public access for appropriate management and disposition. Benefits to the organization include:

- ⇒ Automatic identification of PII mitigates risks associated with PII exposure
- ⇒ Standardizes and improves organizational processes associated with the identification and segregation of PII
- ⇒ Reduces organizational costs and effort in protecting and identifying PII
- ⇒ Reduces costs and risk exposure through automatic identification of PII from disparate content repositories
- ⇒ Eliminates risk associated with end user non-compliance issues
- ⇒ Reduces the portability and transmissibility of protected data assets
- ⇒ Improves protection of citizen's privacy information as well as homeland security or other sensitive

About Concept Searching

Concept Searching's suite of products deliver concept based search, automatic semantic metadata generation, automatic classification and taxonomy management. All technologies are fully SOA compliant and delivered as web parts and are easily deployed and managed. Based on Concept Searching's unique compound term processing, content is classified based on the conceptual meaning contained in the content enabling the retrieval of information using related concepts, compound terms, and multi-word fragments.