

# Regulatory Compliance

*Distributing paper documents electronically in an age of increased regulatory requirements*



Data Protection Act



Health Insurance Portability and Accountability Act (HIPAA)



Gramm-Leach-Bliley Act



Privacy and Electronic Communication Regulations



Freedom of Information Act



Sarbanes-Oxley Act

## Purchasing a scanning solution

By electing to deploy a scanning solution, you exhibit the foresight to recognize the unique return on investment an integrated scanning solution can offer your enterprise. You understand that the office copier has emerged as a networked device with many functions: copy, print, fax, and scan. The benefits of scanning are not as obvious as copy, print, and fax, but can have the greatest impact on productivity by enabling you to integrate paper into your digital enterprise applications. Not only will your company realize an immediate increase in productivity but, you will also directly, positively impact your bottom line.

Today, there are many scanning solutions to choose from. Before you make your final decision, it is critical to consider the Total Cost of Ownership (TCO) of the products you are evaluating. This white paper was designed to help you select the right copier-based scanning solution for your business. By reading this document you will be able to assess the appropriate product requirements for your environment, determine acquisition costs, and understand what ongoing expenses you will bear after installing the product.

# Contents

Introduction:	
The Case for Electronic Document Distribution	2
The Changing Business Environment	3
Using Technology To Meet the Compliance Challenge	5
Records Management	6
E-mailing	7
Faxing	8
Activity Tracking	9
Questions to Ask When Considering a Scanning Solution	10
Personal Privacy and Protection of Confidential Information	11
Transmitting Information Electronically	13
Tracking of Disclosures	14
Purging of Temporary Files	15
Information Availability	16
Making Paper Document Available Electronically	17
Handling Requests for Information	18
Summary	18

# Introduction:

## The Case for Electronic Document Distribution

Electronic distribution and storage of paper documents offers enormous opportunities for cost savings, productivity improvements, and increased business effectiveness. Here are just a few examples:

- > Deliver original-quality documents immediately and at virtually no cost using your existing network infrastructure, instead of sending them by fax or overnight mail.
- > Scan incoming paper documents into your existing electronic workflows, eliminating costly delays and ensuring accuracy.
- > Convert existing paper records into digital files and store them in computerized databases for fast, easy retrieval from any location.
- > Back up your scanned documents to offsite data storage facilities to ensure business continuance in the event of a disaster.

Given these and the many other compelling reasons for switching to electronic document distribution and storage, it's not surprising that most businesses have either already adopted or are considering adopting a document scanning solution of some form.

All major copier vendors now offer some form of electronic distribution technology, all promising ease-of-use, rapid return on investment, and integration with existing enterprise applications.

# The Changing Business Environment

While this transformation in the way organizations handle paper has been taking place, changes in the business environment have forced companies and public agencies worldwide to examine and modify their business processes, particularly those related to information management:

> A slew of high profile corporate accounting scandals (Enron, Arthur Andersen, WorldCom, etc.) have resulted in calls for greater corporate oversight and demands for executive accountability. Businesses today must be extra vigilant in ensuring that all business-related transactions and communications are documented and retained for subsequent examination.



> The exponential growth in the acquisition and storage of personal information by governments and businesses, as well as an increasing number of cases of identity theft, has led to heightened concerns for personal privacy by consumer advocacy groups and individuals, particularly when information is transmitted across the Internet. Organizations handling confidential or personal information must take proactive measures to ensure information is safeguarded and is not disclosed to unauthorized persons.



> Increased expectations for openness and accountability have ushered in a new era of transparency in governments around the world. Agencies must respond rapidly to citizen requests for records relating to public health, environmental hazards, consumer product safety, government spending, taxes, and foreign policy, to name just a few. By making information available over the Internet, requestors can conduct their own searches, and providers can eliminate the laborious and expensive process of locating and retrieving information often stored in dusty basements or inconvenient paper archives.



These new standards and expectations have brought about a tidal wave of new laws and regulations in Europe, the United States, and worldwide, designed to protect consumers and investors, and empower individual citizens. A sampling of recent legislation is shown in the table below.

Law/Regulation	Country	Requirements
Sarbanes-Oxley Act	United States (including overseas subsidiaries of US companies)	Requires public companies to retain all documentation related to financial reports, audits, business transactions, and meetings for a period of five years in such a way that documents can be recovered quickly.
SEC Exchange Act 13-a-15(f)	United States	Requires companies to “provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles.”
Gramm-Leach-Bliley Act	United States	Requires financial institutions to ensure the security of customers’ private information.
Privacy and Electronic Communications Regulations	European Union (EU)	Protects the right to privacy with respect to the processing of personal information in the telecommunications sector.
Health Insurance Portability and Accountability Act	United States	Protects individuals’ personal health information from unauthorized access. Requires appropriate administrative and technical safeguards, including data encryption, to ensure the privacy of patient health information.
Data Protection Act	UK and other European Union (EU) nations	Provides individuals with access to any records containing their own personal information, and establishes mechanisms to ensure that personal information is accurate, relevant, and subject to appropriate security.
Personal Information Protection and Electronic Documents Act	Canada	Requires consent before disclosing personal information and measures to ensure that personal information is subject to appropriate security
California Senate Bill 1386	United States	Requires disclosure of any security breach in which unencrypted personal information might have been acquired by an unauthorized person and due diligence in protecting customer information from unauthorized access. Applies to any company doing business in the state of California.
Freedom of Information Act	Enacted in various forms by governments worldwide	Gives individuals the right to request information from government agencies and obligates those agencies to deliver information promptly. It is intended to promote openness and accountability, and facilitate better public access to government information. Advanced integration into backend applications

Overwhelming in their range and complexity, these laws nonetheless boil down to three key information management issues:

- > **Records Management:** The need to document all business transactions and retain records
- > **Privacy protection:** The need to protect confidential personal information

> **Information availability:** The need to make information available to the general public and respond quickly to requests from individuals

The remainder of this paper examines the benefits and potential pitfalls of electronic document distribution in this challenging regulatory environment.

# Using technology to meet the compliance challenge

Against this backdrop of technological and regulatory change, organizations cannot afford to simply continue “business as usual.” All organizations, large and small, must examine their existing business processes and look for ways to improve their effectiveness while ensuring regulatory compliance. Some may require only minor changes in administrative procedures, while others may require major overhauls in the way they operate.

A carefully considered electronic document distribution and storage policy can go a long way to increasing competitiveness while helping with regulatory compliance. On the other hand, a poorly considered policy can expose an organization to a minefield of potential problems:

- > Important steps in the business transaction cycle may be left undocumented if audit trails are not maintained
- > Confidential information once kept under lock and key may become visible to unauthorized individuals
- > A mountain of paper may be transformed into a sea of unstructured electronic files, making it impossible to locate the information you need

It is vital, therefore, that organizations move cautiously when implementing an electronic document distribution and storage solution. Of the many solutions available today, most fall short in one or more of these areas, making it critical to ask the right questions before making any purchasing decision.

# Records Management

Records Management governs the creation, availability, retention, and ultimate destruction of documents relating to business activities and transactions. These records, or “information assets,” which may include orders, receipts, financial statements, policy statements, legal disclosures, and so on, are vital to the organization’s existence - loss of these records could seriously compromise the company’s ability to function or could put the company at risk of violating the law. Many companies have run into problems because they failed to retain information about business transactions, or because they purposely altered or destroyed such documents. Records Management, then, is the control and maintenance of these various assets over the course of their lifecycle.

Records Management does not mean keeping everything forever. In fact, there are many good reasons not to keep everything beyond its required retention period, including:

- > The costs of storage and maintenance, especially if older information must be migrated to newer storage media to ensure continued access
- > The additional time and expense involved in retrieving the information you want from a larger volume of data
- > Possible exposure to litigation based on outdated documents
- > The potential illegality of holding personal information longer than necessary

The retention period for documents will vary depending on factors such as:

- > The nature of the communication
- > Regulations that govern such records in a particular industry, country, or state
- > Internal policies regarding the retention of documents

In all cases, though, the employer is responsible for ensuring that employees are aware of the company’s document retention policy and understand how to comply with the requirements. Numerous court cases involving employees who have not followed company procedures have exonerated the employee and held the employer liable for failing to provide appropriate guidelines or training.

In the post-Enron/Sarbanes-Oxley era, a wider definition of records management has emerged – one that places emphasis not only on traditional business documents, but also on the peripheral supporting communications, including e-mails, instant messages, voicemails, and other exchanges, regardless of media. Such communications are admissible as evidence in most courts of law and may be subject to the same rules of document retention. When questions about transactions or business practices arise, organizations must be able to retrieve all relevant information within a reasonable timeframe.

# E-mailing

The “scan and mail” systems offered by copier vendors today make it very easy to send electronic copies of paper documents, including important business documents, to customers, vendors, business partners, regulatory agencies, etc. Given the importance of records management, it is vital to track and manage these communications.

Unfortunately, tracking these e-mail communications is not possible with many of the scanning solutions available today. Most of these systems require the use of an SMTP relay for the delivery of e-mail. As its name suggests, SMTP (Simple Mail Transfer Protocol) provides a “simple” way to deliver e-mail messages over the Internet. In fact, its simplicity and lack of any built in authentication makes it a perfect mechanism for spammers and virus spreaders, who can broadcast literally thousands of untraceable messages a second using fictitious sender names. Its simplicity also means there is generally no record of outgoing communications.

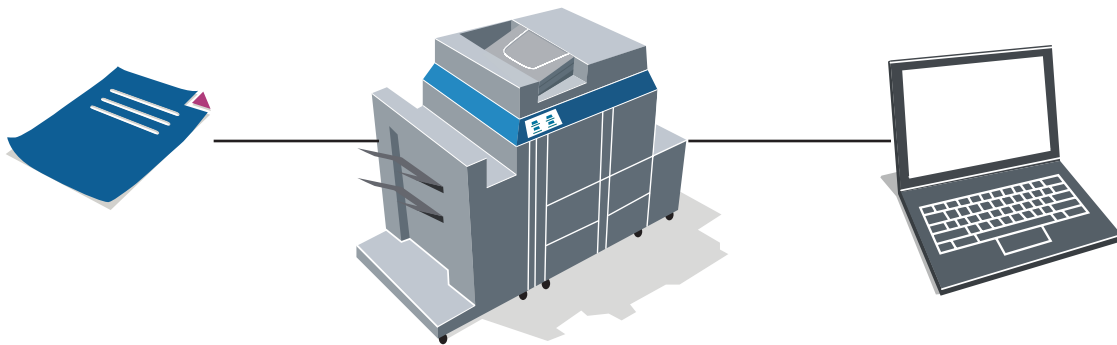
You can configure any PC with an Internet connection as an SMTP relay. All that is required is some SMTP server software, like Microsoft IIS (included with most versions of Windows) or any of the free SMTP applications available on the Internet. To demonstrate just how simple SMTP actually is, here is an SMTP message you can create using any text editor:

From: [cfo@mycompany.com](mailto:cfo@mycompany.com)  
To: [cfo@yourcompany.com](mailto:cfo@yourcompany.com)  
Subject: Asset transfer authorization  
I have authorized the transfer of \$100,000 to your holding account. A copy of the wire transfer authorization is attached.

You then place this file in your SMTP server’s “pickup” directory and the message is delivered to the recipient - no authentication, no tracking, no encryption, no confirmation of delivery, or receipt.

Remarkably, this is exactly how most copier-based scan and mail systems work - the copier prompts the user to enter the sender and recipient information, formats the message as shown above, attaches the scanned document, and delivers it to the SMTP server's "pickup" directory, where it gets processed and sent out over the Internet. Clearly, such systems expose organizations to untold risks.

The solution is to select a scanning system that integrates directly with your company's corporate e-mail system and delivers documents as if they were sent from the user's desktop. To do this requires an e-mail client that supports authentication and integrates with your mail server at the API level. This way the transaction is captured and retained along with all of the organization's other e-mail communications using whatever e-mail archiving solution has been selected.

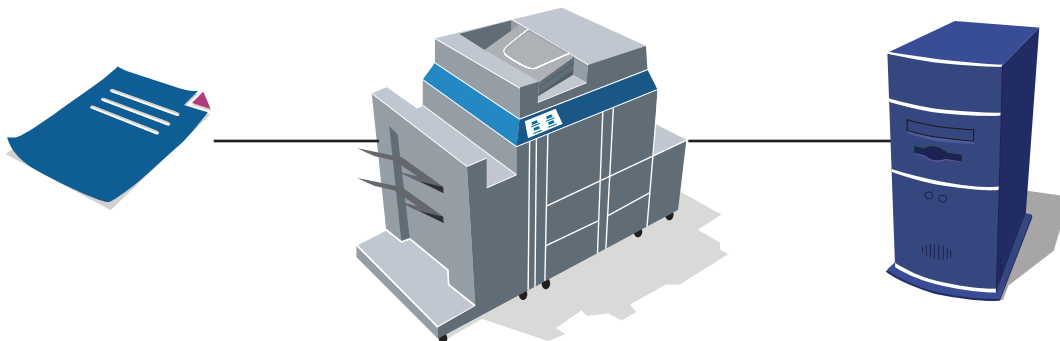


Find a scanning solution that sends paper documents via e-mail safely and securely using your existing e-mail system. It should be as easy as scanning a piece of paper at your digital copier, entering your recipients' e-mail address, and clicking send. Options for 128-bit encryption and user authentication make solutions even more secure.

## Faxing

There are similar problems with the faxing capabilities of many copier-based scanning solutions. Many of these systems provide faxing capabilities that are no more sophisticated than a standalone fax machine, with no record of outgoing faxes that can be retained as part of the company's records management policy. Look for a

scanning solution that offers integration with most network fax servers, including Captaris RightFax and Microsoft Exchange or Lotus Notes-based systems. These server-based systems maintain a record of all outgoing faxes, including what was sent, who sent it, when it was sent, and to who, making it easy to track or audit fax-based communications.



Look for a scanning solution that offers integration with most network fax servers, such as Captaris RightFax.

# Activity Tracking

Another useful feature provided by some copier-based scanning solutions is the ability to capture a record of scanning activities. The purpose behind this is two-fold:

- > To bill costs back to a department or an account (“cost recovery”)
- > To maintain a log of outgoing communications for audit purposes

While cost recovery is not a compliance issue, the ability to record information about document-related activities is. To create a useful audit trail, a system must capture at least the following information:

- > What was scanned
- > Who scanned it
- > When was it scanned
- > How it was sent (e-mail, fax, network file transfer, etc.)
- > Who it was sent to

Many systems lack even the most basic activity logging capabilities, while others simply log the number of pages scanned, with perhaps the ability to capture a billing or department code. Look for a solution that offers comprehensive activity logging that captures basic information about the sender and recipient, and lets the system administrator configure custom fields to capture information about the document being sent.

## Questions to ask when considering a scanning solution

- > Does your system ensure that all outgoing scanned e-mail can be traced back to the individual who sent it?
- > Does your system save a copy of all outgoing scanned e-mail on the central mail server?
- > Can Microsoft Outlook users view a copy of scanned documents they e-mailed from the copier by clicking "Sent Items" in Outlook?
- > Can your system maintain a record of outgoing faxes?
- > What tracking and audit trail capabilities does the system offer?
- > Is your system easy enough to use that my staff can comply with our document retention policy without affecting overall productivity?

# Personal privacy and protection of confidential information

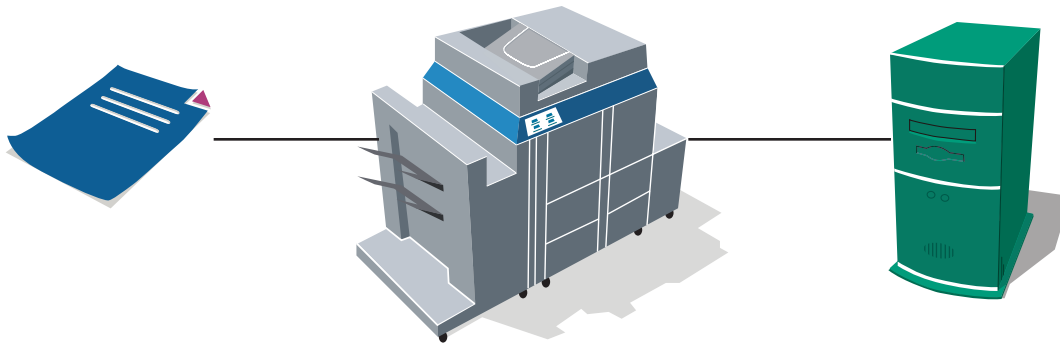
Widespread use of the Internet for communication has led to increased concern about the security of personal information, primarily personal financial and health information. Most countries have enacted laws to protect personal information from unauthorized access. Typically this involves limiting access to records and reducing the chances of information being intercepted as it is transmitted between locations.

## Limiting access to records

Traditional paper-based records are typically stored in file cabinets or document storage boxes. When the information in those records is confidential, physical safeguards must ensure that only authorized personnel have access.

When confidential information is stored electronically, similar safeguards must be implemented to ensure information privacy. Typically, companies employ document management systems to store such information, and assign security restrictions to limit the level of access based on the user's security profile.

For any organization that has invested in an electronic document management system, scanning becomes an obvious way to integrate paper-based documents with the company's other information assets. Imaging solutions that scan and file large volumes of incoming paper and file them electronically have been available for many years, but these solutions are expensive and complex to implement, so they are usually limited to specialized vertical markets. Frequently, the volume of documents handled by an office does not justify such a specialized solution, or the paper-based information varies in content and format so it must be handled on a piece-by-piece basis. In these cases, a copier-based scanning solution that integrates with your backend document management system for "ad-hoc" scanning provides an appropriate solution.



Look for a scanning solution that offers native integration with document management systems such as Interwoven, OpenText, and EMC Documentum.

Several copier vendors now offer integration with various document management systems, but most simply deliver the scanned image file, plus perhaps some associated metadata describing the document, into a network folder, where it is processed by a release script and deposited into the backend system.

For organizations handling confidential or personal information, such a simplistic solution cannot meet the requirements of limited access and secure handling. What is needed is a solution that supports authentication at the scanning device and allows the authenticated user to deliver the scanned document directly into a specific target folder that he or she is authorized to access. This way the existing security restrictions applied by the document management system to files in that folder ensure that only authorized users can access the data.

Look for a solution that offers direct integration with several major document management systems directly from the copier. While the precise implementation varies depending on the backend system, users typically log on using their existing system credentials, select the target folder from a list of folders the user is authorized to access, enter the required metadata, and store the document. A built-in OCR engine can optionally create a text version of the image to support full text searching during the document retrieval process. Only with this level of integration can organizations handle personal information in a way that ensures confidentiality.

# Transmitting information electronically

Although most people know that standard Internet e-mail is inherently insecure, an astonishing amount of confidential and personal information is transmitted every day over the Internet. Due to the sheer volume of Internet traffic, the likelihood of this information being intercepted and used surreptitiously is very small, but the possibility exists nonetheless. And regardless of the likelihood, privacy laws may require organizations to eliminate such a possibility or face stiff penalties.

In order to safely transmit information over a public network like the Internet, the information must first be encrypted. This means that any organization planning to send confidential information should make sure any scanning solution they consider includes an encryption capability. Most solutions do not encrypt scanned documents, making them virtually useless in any organization that plans to transmit personal information electronically.

It is important the solution you choose includes 128-bit document encryption that lets you securely encrypt confidential or personal information and deliver it by e-mail or network file transfer. When configured, the sender enters an encryption password at the scanning device. This password is used to generate the encryption key which is used to encrypt the scanned image file, making it unreadable to any unauthorized person who may intercept the document. Upon opening the file, the authorized recipient enters the password to reverse the encryption algorithm and read the document.

# Tracking of disclosures

When transferring personal information over a public network, organizations may be required to retain records of all information disclosures. For example, the Health Insurance Portability and Accountability Act in the United States requires health providers to retain records documenting situations where personal information was released to a third party. Patients have a legal right to request this information, and organizations must be able to demonstrate satisfactorily that personal information was disclosed only on a “need to know” basis.

The tracking of disclosures can be done by enforcing administrative procedures that the handlers of personal information must follow. In busy offices, however, and under the pressure of time constraints, it becomes easy to “forget” what may seem like a burdensome detail. Best, then, is to make the tracking of disclosures an integral part of the document transfer process.

Few of the copier-based scanning solutions available today make it possible to track personal information disclosures. Most simply prompt the sender for the recipient’s address and deliver the scanned document image via SMTP, providing no record of the transaction (see “E-mailing” on page 7). Look for a solution that provides tracking at two levels:

- > Direct integration with Microsoft Exchange and Lotus Notes mail servers ensures that a copy of the transaction is stored on the central e-mail server
- > Activity tracking with custom fields ensures that a record of the transaction is entered into the transaction log file  
(see “Activity tracking” on page 9)

Together, these two mechanisms help organizations comply with disclosure tracking requirements with minimal additional effort.

# Purging of temporary files

Whenever documents are scanned, the scanning system creates temporary image files during the process. When confidential data is involved, it is important to make sure temporary files are not left on the device's hard drive - doing so could make this data vulnerable to theft or to access by unauthorized individuals.

The way these temporary files are handled varies from vendor to vendor, but some solutions simply leave the files on the system's hard drive or remove them using standard (and easily reversible) file deletion functions. Choose a solution that provides secure deletion of temporary files by overwriting the disk locations with multiple layers of random characters. This ensures that the data is properly purged and cannot be retrieved using data recovery tools.

## Questions to ask when considering a scanning solution:

- > Does your system support scanning documents directly into my document management system from the copier?
- > Can your system save documents to my document management system in a way that ensures that only authorized individuals can access the information?
- > Can your system encrypt personal information before sending it by e-mail?
- > How does your system help document disclosures of personal information?
- > Does your system ensure that temporary files containing confidential or personal information are purged from the system's hard drive after use?

# Information availability

The third major information management compliance issue of particular relevance to electronic document distribution focuses on the availability of public information. While businesses have an obvious economic incentive to make information about products and services available to the general public, the same is not necessarily true of government agencies. It is only recently that governments have enacted laws requiring public agencies to make information available to their constituents.

One of the first implementations was the United States' Freedom of Information Act (FOIA). Although the concept of openness and transparency in government has existed since the drafting of the US Constitution, it is only recently that citizens' rights were formalized under law. Under the FOIA, you can get information about how an agency operates, actions it has taken, how it spends its money, and what information it has collected. Although FOIA predates the Internet, it is still relevant because it specifies the type of information that must be available, exclusions, rules for compliance, appeals processes, etc., rather than specifying access mechanisms or technologies. It has, however, lost some practical significance today because of its formal and time consuming operation - while written requests and 10 day waiting periods were once acceptable, the Internet has transformed people's ideas about access to information. FOIA remains, though, an important legal minimum standard for accessing public information.

More recent "freedom of information" acts, like the UK's version, specifically require public authorities to adopt and maintain publication schemes - guides to the type of information that the authority publishes, the format in which the information is available, and fees for access, if applicable. The UK's act was created as part of the government's "e-Government" program, which aims to make all public services accessible via the Internet, so much of the language is geared towards the use of technology as an enabler. As a result of a large advertising campaign by the government, the public has become well informed about their rights of access to information, so public agencies have been preparing for an anticipated deluge of requests.

# Making paper documents available electronically

Much government archive information has already been converted from paper records to online databases. For example, the National Security Archive (NSA), an independent research institute located at George Washington University in Washington, DC, collects and publishes declassified documents acquired under the Freedom of Information Act. The NSA uses production scanning and workflow systems along with computerized indexing technology to make the massive amount of material on international affairs already released by the US government accessible to researchers and the public.

Although it would be a mistake to think that copier-based scanning solutions can handle massive undertakings such as the NSA, they are nonetheless well suited to scanning and archiving small to moderate volumes of documents on an ongoing basis (“ad hoc scanning”). By selecting a scanning solution that integrates with an existing document management system, agencies can efficiently store paper-based documents along with other electronic files, making them instantly available to those with appropriate access.

Many of the copier-based solutions that offer document management system integration, however, lack key features, such as support for full text searching or metadata entry at the time of storage. Without these features, a scanning solution that was supposed to facilitate document retrieval may do exactly the opposite, if the end result is a folder of unstructured image files that must be searched manually for relevant content. What is needed, then, is a system that makes indexing an integral part of the scanning process, ensuring that documents are entered according to the filing specifications laid down by the archive administrator.

A few companies offer direct integration with major document management systems directly from the copier and provide support for PDF, full text searching, and metadata entry, making them well suited for information that is available for download via the Internet. Additionally, some solutions offer integration with document management systems to simplify the document indexing task by prompting the user to enter all required fields and providing “pick lists” of choices where appropriate. Depending on the application, the image file can be stored directly in the system or diverted to an electronic workflow system for approval before it is actually filed.

# Handling requests for information

Most “freedom of information” acts specify how an individual must submit a request and how long the agency has to comply with the request. In the United States, for example, requests are submitted in writing and the agency must respond to the initial request within 10 days. The agency then has an additional 10 days to provide the information requested. The agency is permitted to charge appropriate fees to cover retrieval and duplication costs.

Regardless of the details of specific acts, it is undoubtedly true that the more information an agency provides voluntarily, the less work they will have to do later handling specific requests. By making information available over the Internet, agencies can minimize the number of requests, or respond to requests by directing the requestor to their Web site. For information that is not necessarily appropriate for public access via the Internet, agencies that store records electronically can minimize or eliminate the time and costs to retrieve, photocopy, re-file, and mail the requested documents.

As requests by e-mail or via online request forms become more common, agencies can save themselves additional time and expense by returning the requested information electronically. Many of the costs associated with providing information are due to copying and mailing expenses, both of which can be eliminated using e-mail.

## Questions to ask when considering a scanning solution:

- > Does your system allow me to scan paper documents directly into my document management system?
- > What image formats does your system support and are these formats viewable using standard Web browser software?
- > Can your system convert document images into fully searchable text?
- > Can I add metadata describing the document's content so it can be retrieved easily?

## Summary

This document has outlined the many benefits of electronic document distribution and highlighted the important compliance issues to consider when selecting a scanning solution. There are scanning solutions that offer all of these benefits and more. You can build your own personalized solution, with integration into “home grown” document management systems and native integration to existing e-mail systems, to suit the needs of your own company.

**eCopy, Inc. (Headquarters)**

One Oracle Drive  
Nashua, NH 03062  
USA  
tel: +1.603.881.4450  
fax: +1.603.881.4399  
www.ecopy.com  
info@ecopy.com

**eCopy Japan**

eCopy KK  
Beniya Bldg. 4F  
4-3 Kojimachi  
Chiyoda-ku  
Tokyo 102-0083  
Tel: +81 3 5215 7511  
Fax: +81 3 5215 7515  
japan@ecopy.com  
www.ecopy.com/japan

**eCopy Europe**

1 Chalfont Park  
Amersam Road  
Gerrards Cross  
Buckinghamshire SL9 0GA  
UNITED KINGDOM  
tel: +44 (0)1753 895 000  
fax: +44 (0)1753 895 001  
europe@ecopy.com  
www.ecopy.com/europe

**eCopy Asia Pacific**

Level 21  
201 Miller Street  
North Sydney  
NSW 2060 AUSTRALIA  
Tel: +61.2.9909.0938  
Fax: +61.2.9025.3777  
asiapacific@ecopy.com  
www.ecopy.com/asiapacific

© 2007 eCopy, Inc.

The eCopy logo, eCopyFax, the Simplify logo, the MailRoom logo, eCopy ShareScan, eCopy ShareScan OP, eCopy ScanStation, eCopy ScanStation OP, eCopy Desktop, eCopy Quick Connect, eCopy Xpert Compression, UniDoc, SpeedFax, and SpeedPrint are trademarks of eCopy, Inc. ShareScan, Simplify, and MailRoom are registered trademarks of eCopy, Inc. All other terms and products are trademarks or registered trademarks of their respective owners and are hereby acknowledged.