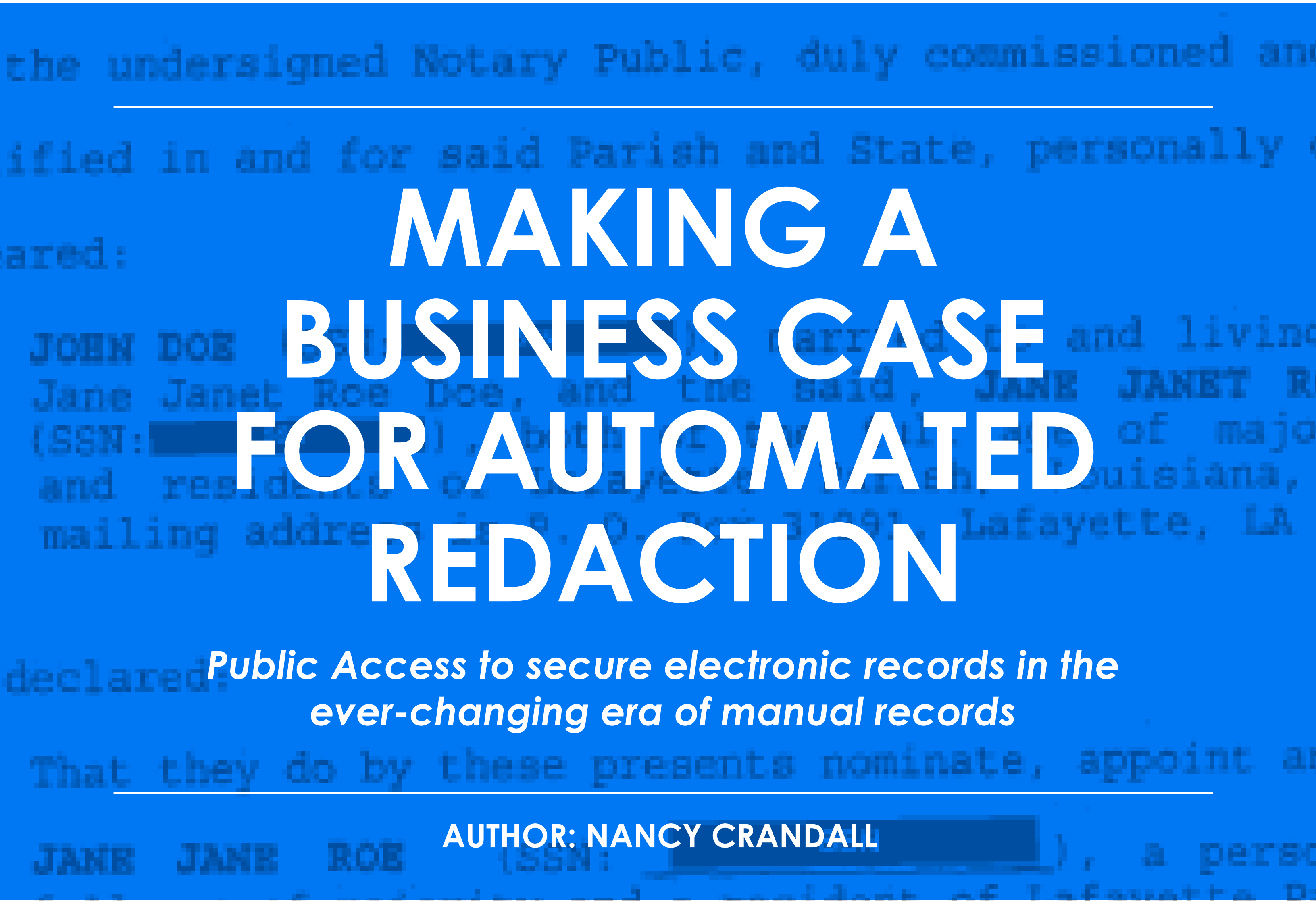

MAKING A BUSINESS CASE FOR AUTOMATED REDACTION

Public Access to secure electronic records in the ever-changing era of manual records

AUTHOR: NANCY CRANDALL

extract

EXTRACTSYSTEMS.COM

PUBLIC ACCESS IN THE ERA OF MANUAL RECORDS

There are many persuasive reasons for government agencies to make electronic public records accessible remotely. Access to public information is, after all, one of the cornerstones of transparency in government and excellence in customer service. Public demand for remote access to electronic public records is another driving force. Many of the same records that are now available electronically have been publicly available for years, with the limitation that if one was interested enough in the information, they would also be willing to travel to the courthouse or other government facility to search for and review public records. This approach inherently limited access to public information.

PUBLIC ACCESS TO TODAY'S ELECTRONIC RECORDS

The introduction and expansion of technology in government, such as case and records management systems, document imaging and electronic filing, has contributed to increased availability of electronic public records. Access to much of this information is becoming more broadly available to the public and other agencies remotely through websites, public portals or subscription services. The electronic era of public records makes information regarding court cases, land records and vital statistics accessible and searchable anywhere, at any time.

Making public records available electronically benefits agencies and consumers alike by limiting in-person requests for information and services and reducing foot traffic and wait times at public service counters. This, in turn, allows scarce government resources to be reallocated to other activities. It is a prime example of how technology can help government operate more efficiently "doing more with less," while also meeting customer demands for convenient and expanded access to information and services. However, for as many benefits as electronic systems and documents provide, new challenges also arise.

> "...111,000 government or military records were reported as breached within the first 22 days of 2013"

ABOUT THE AUTHOR

NANCY CRANDALL

Nancy Crandall is the principal of Justice Connections LLC, a court management consulting company. Ms. Crandall has nearly 30 years of experience in courts and criminal justice. She has held a variety of court management positions including: Court Administrator, Assistant Judicial District Administrator, Business Architect for a statewide case management system implementation and Manager as well as Deputy Director of the Court Services Division for the Minnesota Administrative Office of the Courts (AOC). Consulting services and expertise includes project and change management, project leadership, program management, technology implementation support and business process reengineering services.

forbrukeren
skal ha opplysning
avgifter og leveringskostnader
ikke
levering eller annen oppfyllelse av avtale
AV ANGRERETT

PROTECTING SENSITIVE DATA IN PUBLIC DOCUMENTS

Making electronic data available remotely or online requires up-to-date policies to protect sensitive data that may be contained in otherwise public records.

Types of sensitive data that might typically be found in many documents include:

- *Social Security Number*
- *Date of birth*
- *Financial account information*
- *Victim names and addresses*
- *Driver license numbers*
- *Names of minor children*

A variety of methods may be in place within government agencies today to protect sensitive data from being inadvertently displayed in publicly accessible electronic systems.

A few common methods include:

- *Rules and other policies that make it the responsibility of the filer to redact or otherwise ensure the absence of sensitive information in documents*
- *Requirement that the filer use only partial fields (such as last four digits of SSN) in pleadings or other documents submitted for filing*
- *Document classification approaches that restrict access to documents containing sensitive data fields*
- *Manual redaction of sensitive data*
- *Automated redaction tools*

Making the investment in technology to improve customer service and reduce labor costs comes with the responsibility to protect sensitive data in electronic documents and data stored in public systems. A single pronged approach using any one of the methods above is simply not enough. The prevalence and perils of identity theft is driving additional data security legislation at federal and local levels to protect sensitive information in electronic records across industries. Unfortunately, unintended release of private data does happen. There is a public expectation that government agencies meet an even higher standard than other industries in the protection of personal data. This article explores some key considerations and benefits of incorporating automated document redaction into an electronic document management business model.

IDENTITY THEFT ON THE RISE

It will come as no surprise to most that crimes involving the theft and misuse of personal data identity are on the rise. How much of this problem can be attributed to the breach of sensitive data in electronic government records and automated systems? It is difficult to say for sure, however the Identity Theft Resource Center1 states in an online report that more than 111,000 government or military records were reported as breached within the first 22 days of 2013 alone! 2 (Data Breaches, 2013).

> *ACCORDING TO JAVELIN STRATEGY AND RESEARCH STATISTICS;*
>
> *“IDENTITY FRAUD INCREASED BY 13% IN 2011. MORE THAN 11.6 MILLION ADULTS BECAME VICTIMS OF IDENTITY FRAUD IN THE UNITED STATES……. ”*
>
> *(VAN DYKE, & MONAHAN, 2012).*

The most egregious incidents of public data breaches are well covered by the media and tracked by a variety of groups and organizations. Still, an untold number of additional incidents impacting a single individual, for example, are also at risk for occurring. Remote and electronic access to public data systems has presented challenges in the protection of sensitive data for a number of years across public sector agencies. The introduction of electronic documents in those systems promises to increase these challenges.

An article in the Washington Post entitled "Online Records May Aid ID Theft" (Brubaker, 2008) illustrates with specific examples, the incidence of public exposure of sensitive information in some public sector record systems. This article highlights specific instances of complete Social Security Numbers found on hundreds of imaged and paper public records including land deeds, death certificates, traffic tickets, creditor filings and other electronic documents, as well as records related to civil and criminal court cases. All were found upon spot checking of records. From a business perspective the problem is a complex one, further complicated by timing and the sheer volume of records.

Monitoring the volumes of newly filed electronic documents submitted through electronic filing portals or new paper submissions scanned by staff for the presence of sensitive data is one part of the equation. Many older records have been scanned and exist in public systems. These documents were originally filed prior to newer laws and regulations restricting the inclusion of sensitive data in public documents. Social Security numbers are a prime example. Custodians of these records must go back to find and manually redact sensitive data that may be contained in these documents, while also manually monitoring the ever increasing volume of newly filed electronic documents. It is a daunting task.

The good news is that sophisticated and reliable software solutions for automated redaction of sensitive and protected data are available in the marketplace today. These tools help make the responsibility to protect sensitive data more manageable, while bringing into better balance the risks associated with making public data and documents electronically accessible with the benefits provided to public sector agencies and their constituency.

THE GOOD NEWS IS THAT SOPHISTICATED AND RELIABLE SOFTWARE SOLUTIONS FOR AUTOMATED REDACTION OF SENSITIVE AND PROTECTED DATA ARE AVAILABLE IN THE MARKETPLACE TODAY.

1Identity Theft Resource Center® (ITRC) is a nonprofit organization dedicated exclusively to the understanding of identity theft and related issues. The ITRC provides victim and consumer support as well as public education. The ITRC also advises governmental agencies, legislators, law enforcement, and businesses about the evolving and growing problem of identity theft.

2A breach is defined as an event in which an individual's name plus Social Security Number (SSN),driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format.

REDACTION SOLUTION

"Redaction" refers to the permanent removal of personal or sensitive information from documents. With automated redaction, electronic images are processed through Optical Character Recognition (OCR) software to convert them into a digital format. These digital formats are then "searchable" using rules-based logic driven by clues, pattern recognition, spatial location and algorithms designed to locate sensitive information in a variety of documents. If sensitive information is found within the document, the software will assign a "confidence level" based on how well the data found matches the pre-determined rules, pattern and clues. An image found to contain sensitive data may be automatically redacted (as in the case of a high confidence level result) or electronically routed for human verification for specific or all confidence level results, based on user preferences. The identified redaction zone is then "burnedin" to a copy of the image making it suitable for public view.

Redaction software that provides a high degree of flexibility, allowing customers to define customized rules, confidence levels and preferred actions based on specific business needs, provides the most precise and accurate results. Products with a proven ability to interface seamlessly with case management and records management systems already in place are an important consideration in terms of upfront costs and interoperability needs. Automated features that effectively process historical documents housed within large repositories, as well handling newly filed documents, are essential requirements when evaluating a product solution against business needs.

BENEFITS

As mentioned, one or more methods to protect sensitive data in publicly accessible electronic systems may be incorporated into document processing practices in courts and public agencies. Automated redaction software and tools enhance those methods already in place by further minimizing exposure and narrowing gaps that may exist. This results in greater assurance that sensitive data is not accessible to those not authorized to view it.

PROTECTING YOUR INVESTMENT

A decision by public sector agencies to invest in technology is often predicated on these basic objectives: improve the quality of information, increase access to publicly available information and services, and improve operational efficiency.

Similar to other security measures in place to protect data network and infrastructure, automated redaction can be viewed as a protective measure for the documents and data stored within public systems. It is difficult to quantify a loss that never occurs as a result of protective measures in place. Yet taking additional measures to minimize opportunities for errors that can occur within large, complex, remotely accessible systems, is time and money well spent. When you consider the "what if" scenarios experienced by some public agencies due to the release of private data, thinking in terms of "cost avoidance" is a sensible strategy.

STAFF EFFICIENCIES

Like other business ventures, anticipating the return on your technology investment is something that is often carefully calculated, communicated and monitored. The introduction of e-filing and electronic document management are technology initiatives well aligned to meet the stated business objectives. However, staff time savings (a metric in calculating ROI) can quickly erode if too many manual and time consuming tasks must be incorporated into new business processes.

Manual redaction is one example of a time consuming task that can have a significant impact when quantifying cost and time savings resulting from e-filing and electronic document management efforts.

Add in the realities of staff reductions, turnover, training and cross-training needs related to manual redaction efforts, and you can see where efficiencies are quickly reduced and risks increased, making automated software redaction a cost effective alternative.

QUALITY ASSURANCE

When receiving electronic documents for filing, it is important to evaluate the quality of work being processed in a new manner. In this context, quality relates directly to the skills and experience of staff responsible for this work and the tools available to them. The e-filing portal or review queue that serves as the point of entry for the filing of electronic documents should be viewed as your virtual service counter. As such, what kinds of skill and experience should staff performing these duties possess and what tools do they need to perform high quality work? Electronic document management is much more than simple data entry tasks and the movement of electronic documents. It typically requires that important decisions and determinations be made upon receipt of a filing. These decisions can include review of key acceptance criteria to determine whether the filing can be accepted, verification of case type and/or document type designation selected by the electronic filer and document classification determinations, as well as the review of documents for sensitive information and redaction.

All of these things occur during the initial review process and influence the quality of what goes into the system and what is ultimately available for public view. This makes the initial acceptance and filing of an electronic document critically important. It requires a high level of staff skill and experience, as well as sophisticated tools. Automated redaction software is one such tool.

The same quality considerations can be applied to current back scanning efforts or previously scanned documents. Older documents may contain types of sensitive data in multiple places that are no longer allowed in present day filings. When scanning older documents, a heightened awareness that sensitive data may be present in multiple places and a method to quickly locate it is essential. In the case of inactive or closed files especially, the people reviewing them (post scanning) are most likely to be members of the public rather than internal staff members. Not an ideal way to learn that something was missed!

By detecting and addressing sensitive data before the document is ever made viewable to the public, automated redaction can greatly improve and streamline the process of reviewing both existing paper documents as they are scanned into systems, as well as new electronic documents submitted for filing. For previously scanned documents already in systems, automated redaction can be a valuable tool to quickly and accurately review volumes of stored documents for the presence of sensitive data. This can all be done in seconds and with higher quality and more reliable results than manual redaction processes, where time constraints and distractions often lead to human error.

AUTOMATED REDACTION CAN GREATLY IMPROVE AND STREAMLINE THE PROCESS OF REVIEWING BOTH EXISTING PAPER DOCUMENTS AS THEY ARE SCANNED INTO SYSTEMS, AS WELL AS NEW ELECTRONIC DOCUMENTS SUBMITTED FOR FILING.

WHY AUTOMATED DOCUMENT REDACTION, WHY NOW?

Given the advantages of automated document redaction as discussed above, one may begin to wonder why an agency would not incorporate this technology tool into e-filing and electronic document management processes. Reasons and obstacles vary. Leaders immersed in e-filing and document management technology implementations may think of automated redaction as an "add on" feature that can wait, or as project "scope creep" that could threaten timelines. They may question whether a change-weary user community can endure another change in business processes. Other barriers to implementing automated document redaction include factors such as cost and skepticism regarding the reliability of automated redaction technology.

All of these barriers, while perhaps valid, are not insurmountable when compared to the benefits that can be provided. First, although automated redaction can be successfully implemented at any time, doing so in conjunction with an e-filing and electronic document management initiative is ideal. Compared to other typical integration efforts, automated document redaction software implementation is generally not considered resource intensive from a technical or business perspective.

Most redaction software solutions can integrate rather seamlessly with existing modern case or records management systems. The configuration of customized rules can be very manageable, depending on the product and with the help of an experienced product vendor. Next, from a business perspective, it is an understatement to say that e-filing and document management initiatives already require a major redesign of business practices. Introducing automated redaction upfront can actually eliminate extra manual steps, saving time and minimizing confusion.

Taking a proactive rather than reactive approach to protecting sensitive electronic data and documents can make for a convincing and compelling request for funding. One does not have to look far for examples of unintended breach of sensitive data in publicly accessible systems, and the high cost associated with making "whole again" those who were negatively impacted. Operational efficiency and quality considerations provide justification for funding to introduce automated redaction when transitioning to e-filing or electronic document management.

Finally, the quality of the automated redaction solution you choose can make a significant difference in how quickly confidence in the software is secured, workflow streamlined and accurate results achieved. When software automatically detects a high percentage of sensitive content without human intervention and the automated results are consistently confirmed by the redaction verification staff as accurate, organizations gain confidence in applying technology to what was once a very manual process. The degree of automation for the redaction workflow can be controlled at a pace and comfort level determined by the agency.

MOST REDACTION SOFTWARE SOLUTIONS CAN INTEGRATE RATHER SEAMLESSLY WITH EXISTING MODERN CASE OR RECORDS MANAGEMENT SYSTEMS.

WORKS CITED DATA BREACHES. (2013, JANUARY 29). RETRIEVED JANUARY 29, 2013, FROM IDENTITY THEFT RESOURCE CENTER: HTTP://WWW.IDTHEFTCENTER.ORG BRUBAKER, B. (2008, JANUARY 2).

WASHINGTONPOST.COM. RETRIEVED FROM THE WASHINGTON POST: WWW.WASHINGTONPOST.COM/WP-DYN/CONTENT/ARTICLE/2008/01/01/ AR2008010102334_P VAN DYKE, , J., & MONAHAN, M. (2012, FEBRUARY).

OVERVIEW: 2012 IDENTITY FRAUD REPORT: SOCIAL MEDIA AND MOBILE FORMING THE NEW FRAUD FRONTIER. RETRIEVED JANUARY 30, 2013, FROM JAVELINE STRATEGY AND RESEARCH: HTTPS://WWW.JAVELINSTRATEGY.COM/ BROCHURE/239

FOR MORE INFORMATION, REQUEST A DEMO;

INFO.EXTRACTSYSTEMS.COM/DEMO-AUTOMATED-REDACTION