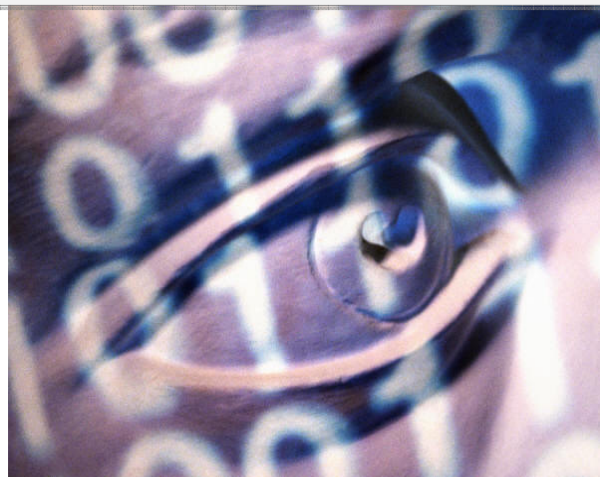


# Privacy, Public Access & Policymaking in State Redaction Practices:

Dealing with Sensitive Data in an Era of Open & Accessible Public Records



**Developed By**

National Association of Secretaries of State (NASS)

National Electronic Commerce Coordinating Council (eC3)

**Following a Symposium on August 14-15, 2007**

## SPECIAL THANKS TO THE SPONSORS

NASS & eC3 would like to recognize the following sponsors, whose support enabled our organizations to host the August 2007 redaction symposium in Maine that served as the basis for this white paper:



**AmCad**

[www.amcad.com](http://www.amcad.com)



**Appligent**

[www.appligent.com](http://www.appligent.com)



**Celcorp**

[www.celcorp.com](http://www.celcorp.com)



**Computing System Innovations (CSI)**

[www.csisoft.com](http://www.csisoft.com)



**Extract Systems**

[www.extractsystems.com](http://www.extractsystems.com)



**EDAC Systems**

[www.edacsystems.com](http://www.edacsystems.com)



**ImageSoft**

[www.imagesoftinc.com](http://www.imagesoftinc.com)



**Manatron** (Formerly Hart InterCivic Records Management Division)

[www.manatron.com](http://www.manatron.com)



**RapidRedact**

[www.rapidredact.com](http://www.rapidredact.com)

---

**PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES****TABLE OF CONTENTS**

Introduction & Background .....	2
Key Questions to Identify & Scope Problems .....	5
Issues: Balancing Security & Privacy with Accessibility .....	7
Technology: Choosing the Right Solutions .....	9
Policy Considerations: Asking the Right Questions .....	12
Next Steps: Integrating Approaches & Developing Standards.....	16
State Practices in UCC Redaction Policymaking .....	17
Appendix A: Glossary of Terms .....	22
Appendix B: IACA Survey of State Redaction Practices (Updated).....	23
Appendix C: About the NASS/ec3 Symposium .....	27
Organizers.....	27
Sponsors .....	28
Presenters .....	28
Participants .....	29
Appendix D: Additional Resources .....	30
Appendix E: Endnotes .....	32

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### INTRODUCTION

It's a familiar story in the Internet Age: personal information available online is stolen or exploited for commercial or criminal purposes—often with devastating consequences for the victim. This issue is an increasing concern for states that have public documents with signatures, Social Security numbers and birthdates—including deeds, mortgages, tax liens, court judgments, marriage licenses and voter registrations—accessible to anyone with a computer and an Internet connection.

While banks, political parties and other entities use the data for legitimate non-governmental purposes, unscrupulous users can do harm. In fact, the Federal Trade Commission recently reported that identity theft is the fastest growing crime in the U.S.<sup>1</sup> While the link between identity theft and government records is not well-documented, increased public concern about privacy protection—coupled with other factors that must be addressed when placing information online—require today's public officials to take a modern approach to state record-keeping.

From adopting new legislation to increasing penalties and updating record-keeping procedures, states are seeking new and innovative ways to protect citizens from identity thieves, stalkers and other threats. The most popular solution is *redaction*, which according to the International Association of Commercial Administrators (IACA), is defined as "*the act of striking out or otherwise removing from the public record or public view any sensitive, private, or confidential information not required by law and which is exempt by law from disclosure in a manner that does not distort the meaning of the record*".<sup>2</sup> In short, it is the process of removing sensitive data from the public portion of an official government record.

According to the National Conference of State Legislatures, thirty-five states considered bills in 2007 to restrict the use of Social Security numbers to identify individuals in government records, with about half of those involving some redaction provisions.<sup>3</sup>

In order to discuss the challenges that states are facing as they tackle the complexities of redaction, the National Association of Secretaries of State (NASS), in conjunction with the National Electronic Commerce Coordinating Council (eC3), held a two-day, invitation-only

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

symposium in Portland, Maine, on August 14-15, 2007. Participants included leading innovators in redaction and information management, including Secretaries of State, executives from state corporations divisions and Uniform Commercial Code (UCC) filings offices, state archivists, academics and private industry experts. Organizers chose the title, "Today's Three P's: Privacy, Public Access and Policymaking" to highlight the most central, but sometimes competing, issues that decision-makers must address.

To facilitate informed decision making, this white paper captures the key questions and considerations that emerged from the meeting. It does not attempt to make specific policy recommendations on the substance of what information should be public or what should be private. Instead, the symposium participants sought to provide policymakers with important background and context, as well as a framework for considering these issues.

Finally, this paper attempts to provide some modest guidance to policymakers and administrators when they have determined that there is a problem and a redaction policy is needed.

### **BACKGROUND**

The most basic question that policymakers must answer in pursuing a strategy for redaction is: What is the scope of the problem?

For starters, it requires identifying what constitutes "sensitive" information. Most states define this data in terms of "personally identifiable information" (PII), but even this is a broad term with no universally-established legal definition. In general, it can be applied to any personal identifier that the government uses or assigns to an individual, including:

- Social Security number
- Taxpayer identification numbers
- Bank or financial account numbers
- Driver's license number
- Signature
- Date of Birth (DOB)
- Address

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

As one symposium participant and state administrator stated:

If we are going to undertake the effort, then I think we have to be very concerned about what the standards are, what the intended outcome is supposed to be, who is going to be accountable... If the real solution is something other than going after Social Security numbers, then that would be a threshold question for me.<sup>4</sup>

At the same time, an executive who works for a company that provides redaction technology added that he is now hearing more from customers about handwritten signature images than Social Security numbers.<sup>5</sup> Another participant noted that it is possible to take five seemingly innocuous pieces of information and use them together to positively identify an individual, meaning that it is important to consider the uses of PII in both specific and broader contexts.

Once policymakers have identified the types of personally identifiable information that are to be redacted from the public record, it is necessary to determine the most practical, cost-effective strategy for removing that information. In light of the massive amounts of historical and current personal data that is available in state government databases—and more generally speaking, on the World Wide Web—leaders must narrow down the documents and timeframes that will be the focus of redaction efforts. In cases where government resources are limited, this process can be particularly challenging.

It is vitally important, too, that key stakeholders understand when government services and available data are *not* contributing to the erosion of privacy or personal security. As busy legislatures grapple with redaction laws, they are wise to avoid costly and ineffective blanket solutions that may not totally appease a worried public. Some information is widely available online, and embarking on an expensive redaction effort may not be the best solution.

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### KEY QUESTIONS TO IDENTIFY & SCOPE PROBLEMS

The following questions will help policymakers identify if there is a problem, as well as the scope of the problem, where one exists:

**Identity Security:** Is the information we are making available subjecting citizens to increased risk of victimization from identity theft? Leaders should carefully weigh the issues to determine if their data is contributing to the problem, specifically considering:

- Whether threats are real or perceived
- Whether the personal information that is available is being directly or indirectly obtained and used by identity thieves, and if so, how frequently/commonly
- Whether removing the information from government records sufficiently remedies the risk or threat to privacy or personal security

**Privacy:** Is the information we are making available subjecting citizens to unnecessary loss of privacy? Leaders should consider:

- Whether the information includes inadvertently collected data that alone, or combined with other data, is posing an increased risk to citizens
- Whether any deleterious effects on privacy are understood and outweighed by the benefits of collecting and making the information publicly available

**Personal Information:** If there is a problem, what pieces of personally identifiable information (PII) are causing the problem? Leaders should consider the following types of personally identifiable information:

- Social Security number (SSN)
- Tax identification numbers
- Driver's license numbers
- Date of Birth (DOB)
- Bank or financial account information
- Handwritten signatures

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

- Addresses
- Any other PII contained in documents, including name history

**Magnitude:** How many and what types of records contain the information? Leaders should consider:

- What is the extent of the data that is in the public custodian's possession?
- How many types of documents contain information to be redacted?
- How many images/documents containing this information are in the back-files?
- How many images/documents containing this information are processed in a week? A month? A year?
- How does presentation of the data (i.e. single record download versus batch download) alter the impact?

**Breadth:** Is the problematic information already out there, and publicly available, in areas beyond government control? Leaders should consider:

- What other government agencies control and make available records containing the same personal information?
- What, if anything, can government do to coordinate efforts with other policy makers and custodians who control access to such records?
- What other non-governmental, publicly accessible records contain the same information? How available are they via the Internet?
- Will removing the personal information from government documents conflict with open government (sunshine) laws?
- What are the short and long-term impacts on government services?
- How much data has been provided or sold to vendors that re-sell the data for legitimate business purposes, and what impact does redaction have on this data?



## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

### **ISSUES: BALANCING PRIVACY & SECURITY WITH ACCESSIBILITY**

The central problem facing many states and localities is the paradox created by the rise of the Internet: While making information easier and more accessible to the public, the increased access to public records presents a whole new set of challenges for citizens and government officials alike. The ideal goal is to create policies and practices that protect the public interest in privacy and security without compromising the spirit and letter of open government laws.

Today's searchable databases on secretary of state and other government Web sites offer anyone with a computer Internet connection the ability to instantaneously search for and download in minutes what used to take hours. Seasoned government clerks like to point out that public records used to languish in "practical obscurity," requiring those who wanted to view them to drive to the local records office and sift through endless stacks of files. In addition to being time-consuming, costly (photocopying fees were a major expense), and limited to the rigid nine to five government office-hour time structure, it was enormously challenging to aggregate public records data from different agencies without a lot of effort and expense. Web access to public documents sweeps away these traditional barriers.

On one hand, the Internet has made the work of government records-keepers less labor-intensive, providing greater ease in collecting and maintaining information. Copying and sharing public records in electronic format is also much easier and less expensive than in the past. On the other hand, there are other issues that can be troubling. For example, agencies may or may not be tracking who is accessing the information online or adequately protecting their Web site from hackers.

Privacy has emerged a hot-button issue in many states where documents with personal information are posted online. Although personal information can be found in many government filings, privacy advocates have generally focused their efforts on these sources of state records:

- Uniform Commercial Code (UCC) filings databases
- Property tax databases
- Voter-registration databases

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

- Multi-record sites, such as court records Web sites

Given the growing number of identity theft cases that are reported each year, millions of Americans are understandably concerned about their vulnerability to identity theft. In a recent Zogby poll, a majority of Americans said they worry about identity theft.<sup>6</sup> In fact, 91 percent said they worry about their identity being stolen.<sup>7</sup>

Compounding this anxiety is a whole industry of data brokers that mine government Web sites for information and sell what they collect, often with little oversight or regulation. Today's software programs allow for swift aggregation of vast amounts of public data—enormous databases can sometimes be scoured in minutes. Countless data brokers are marketing complete identities for \$14 to \$18, a drop from around \$90 dollars just a few years ago.<sup>8</sup> Social Security numbers are so readily available that they have become a commodity.<sup>9</sup>

When it comes to public records, state officials have already risen to the challenge of protecting the privacy and security of some of their most vulnerable citizens. Close to half of the states have adopted laws or programs that limit access to the personal information of domestic violence victims. The goal of these "Safe at Home" programs is to help those who have experienced abuse or stalking preserve their privacy and keep would-be aggressors from being able to locate or contact them. The state typically provides program participants with a post office box address that has no relation to their actual address. First-class mail and service of process can be sent to the post office box and then forwarded at no cost to the participant's real address. Furthermore, participants are able to use the substitute address when creating records with state or local government agencies.

Identity theft and stalking are serious crimes that deserve consideration when it comes to redacting information from public records. Government entities must be able to distinguish when the need to act in favor of the public interest for protecting privacy outweighs the need for providing access and transparency in government processes. Ultimately, however, some services and transactions require the exchange of personal information—and leaders will need to wade into the gray area to decide what limits, if any, should be put on those exchanges, and at what cost to services or transparency.

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### TECHNOLOGY: CHOOSING THE RIGHT SOLUTION

Commercial redaction providers have made revolutionary advances in the technologies they are bringing to market. Early software solutions relied exclusively on redacting specific zones of a document using a grid-like system. The latest, cutting-edge software now automatically locates and analyzes graphic images to decipher patterns, letters, words, numbers and more. These programs also allow redaction of specific words and numerical patterns (i.e. a string of nine digits, such as a Social Security number); and still others can target handwritten information and special fonts. Some software is also self-learning, meaning it has the ability to learn from past errors or omissions and to continually refine its own algorithms.

Generally speaking, three types of redaction methods are available:

- **Manual Redaction:** Personally identifiable information can be manually redacted by creating a copy of the document and physically crossing out (i.e. with a black marker) or covering the information.<sup>10</sup> This method is often combined with a second human review, referred to as a “manual double pass.”
- **Semi-Automated Redaction:** Computer software allows a filing office to set its configuration options and identify certain phrases or words to locate. For example, an office can target data comprised of nine sequential numeric characters for redaction, such as Social Security numbers.<sup>11</sup> This method is then usually combined with a manual verification process.
- **Automated Redaction:** Automated redaction procedures rely upon software technology that uses optical character recognition (OCR) capabilities to convert scanned images into a machine-editable format. One of the many benefits of this approach is that sensitive information can be located within the document using a search engine.<sup>12</sup> Intelligent character recognition (ICR) software, which is able to recognize a wider range of data types and styles than OCR, allows for more advanced techniques, including feature analysis and artificial intelligence. It is not uncommon for a discussion of automated redaction tools to include combined OCR/ICR capabilities.

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

Automated redaction tools are particularly helpful to government offices dealing with backfile conversions, especially considering the variety of document types and layouts in legacy records. Rules-based, optical and intelligent character recognition software makes it possible to redact information from ever larger volumes of images with increasing speed and accuracy. It can also help government entities perform time-of-filing redaction to paper-based or online filings without requiring human interaction.

Nevertheless, redaction can be expensive and imperfect. Policymakers incorporating redaction into their solutions should develop an explicit understanding of the full costs and limitations of such a strategy, including the removal of information from legacy data or records. For example, questions remain about public records that have already been provided or sold to vendors that re-sell the information for legitimate business purposes, and what impacts—if any—redaction should have on these transactions.

Industry experts are also quick to caution leaders about trying to achieve 100% success rates. In addition to time and cost, they contend that such requirements may leave government bodies open to unreasonable liabilities, not to mention unrealistic outcomes. A number of NASS/eC3 symposium participants emphasized the vital importance of providing clear and detailed terms on this issue, among others, in preparing RFPs and procurement documents. Several noted that spot checking for a pre-determined accuracy rate seems to be the latest process for determining user acceptance of a redaction work product, but there was no consensus on the accuracy rate that should be targeted.

In trying to assess the true cost of redaction, it is important to look beyond the numbers associated with procuring hardware or software. Accuracy rates differ among redaction technologies, and some solutions cost more than others. There are personnel costs involved with manual approaches, so policymakers will need to take this into account. Furthermore, the state of the records (i.e. digital or paper-based) and the condition of the material that is in need of redaction will need to be examined. It is particularly necessary to ensure that the redaction technology being considered will work with legacy documents, especially if they have become weathered or damaged in storage. Finally, some types of public records are easier and less costly to work with than others (symposium participants noted that UCC filings tend to be less complicated than corporations filings).

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

As a final thought on calculating costs, symposium participants emphasized the importance of properly allocating resources to maintain quality customer service levels while undertaking a redaction project. They stressed the need for planning that focuses on every possible outcome, including any unintended impacts.

One insightful example came from Keith Whitelaw, Director of the Colorado Secretary of State's Business Division, who observed that when his office disabled Web access to secured transaction records in early 2007, they were relegated to the "brick and mortar" way of doing business. The office still had large numbers of records requests, but processing these manually was not as efficient. With a small staff trying to carry out the work, a noticeable backlog quickly developed. While officials aren't sure whether they prevented any identity theft, they do know that their office suffered in terms of customer service. They received numerous complaints and negative feedback from frustrated citizens until their system went back online in November 2007.<sup>13</sup>

Ultimately, choosing the right technology for a state or jurisdiction does not simply depend on the technology that is most effective. Officials must ask themselves a variety of questions before choosing an approach to redaction. They must determine what needs to be redacted, the document types that are affected, the resources that are available to them (i.e. budget, staffing levels) and how best to utilize those resources. One state's solution may require hiring additional staff to manually redact sensitive information, while another state's approach may involve automated redaction procedures with additional expenses for implementing and updating such software.

When it comes to redaction, policymakers must balance their resources and their goals as part of the decision-making process. With a variety of technologies available (with differing levels of cost and sophistication), today's leaders must educate themselves about their options and how these fit with their needs. Leaders should give close consideration to the outcomes they are expecting, and make those details very clear when issuing contracts for redaction projects. Budgets and staffing often play a large role in the technical approach that is ultimately adopted. The most effective method of redaction is not the type of technology, but rather the method that best suits the needs and resources of the state.

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### POLICY CONSIDERATIONS: ASKING THE RIGHT QUESTIONS

While there are specific questions that each state must ask in adopting redaction policies, basic considerations should include:

**1. Risk:** *The easiest way to minimize risk is to limit the amount of information that is collected, stored and shared. Questions should include:*

- Is the information that is available subjecting people to security or privacy risks, and if so, does the degree of risk provide government with a compelling interest to act on behalf of redacting that information?
- What information must be collected, and do current practices minimize the amount of personal information that is collected? Are there clear guidelines for what needs to be collected and what does not?
- Are there ways other than redaction to ensure that personal information that is unnecessary will be left out of filings/records?
- How is personal information being protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or accidental disclosure?
- Are there laws and/or policies currently in effect that protect the unlawful dissemination of this sensitive information, and if so, will making a certain document accessible to the public conflict with these laws? Could the jurisdiction be held liable for the publication of personal information that is the subject of a criminal offense?

**2. Scope:** Leaders should comprehensively articulate the scope of the information to be redacted, minimally identifying:

- Specifically, what types of personally identifiable information are at issue?

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

- How many documents and images are affected?
- Which applications and services are affected?
- How will users of those services be impacted? How will local officials be affected?
- What is the full list of agencies or other entities that will be impacted?
- What are the timeframes involved?

### **3. Outcomes:** *Policymakers should pay close attention to how they will measure success rates for redaction.*

- Are practices being employed to ensure that redaction policies are accurate and effective, and that the data is of the highest quality? What are these practices, and who is accountable for making sure they are carried out?
- What is the realistic success rate that redaction practices should be meeting? What is an acceptable error rate?
- How will success be defined and measured (success/error rates, reduction in risks to citizens, public satisfaction through perceived reduction in risks and increased education efforts, etc.)?
- How will records that are different over time (due to image quality, document structure, fonts, etc.) be treated during the redaction process?

### **4. Costs:** Removing information from legacy data or records, or even taking on the responsibility to ensure that certain personal information is not collected, can be very expensive.<sup>14</sup> Leaders should develop an explicit understanding of these costs.

- How much will it cost to implement a redaction policy in terms of technology, training and staffing? Who will pay for these costs? Who will manage the work?

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

- If a state database needs to be temporarily or permanently removed from the Internet, what is the cost to the state for taking it offline and processing records requests in a manual fashion? What is the cost, financial or otherwise, for consumers of these services?
- Will redaction of certain identifying information render certain functions useless (i.e. federal tax liens), and if so, how do you quantify the commercial impacts for the state/businesses that use the information for legitimate purposes?
- Who are the primary users of the system? What reaction can be anticipated, and how can it be effectively addressed?

**5. Education:** It is vitally important that leaders develop and conduct a comprehensive education and outreach plan.

- Is there a general policy that indicates a commitment to educating the public and other key stakeholders about redaction policies and practices?
- Does that dialogue aim to ensure that people comprehend what is available in public records that are accessible online and steps they can take to have their personal information redacted or removed from public documents?
- Does it emphasize why the personal information is required at the time of collection and how it will be disclosed (online or otherwise)?
- Does it stress to bulk filers and other stakeholders the importance of not collecting extraneous information and how the law and its penalties apply?
- Does it convey the importance of online government services?

Additionally, NASS/ec3 symposium participants offered the following specific considerations for redaction policymaking:



---

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

- Review old records to determine whether sensitive data exists in legacy files that is no longer needed.
- Make sure to obtain/retain personal information only when necessary.
- Add penalties for stakeholders who fail to remove personally identifiable information before submitting forms for processing.
- Use registration procedures (in many states and jurisdictions, this includes a fee for viewing or downloading records) to ensure that people who are accessing public records are doing so for legitimate purposes and that there is a way to track access to the information.
- Pay close attention to agreements with third parties who will have access to sensitive data and contractually obligate them to safeguard all data.
- Revise UCC forms so they no longer include an area for a Social Security number or Federal Employer Identification Number (FEIN), and until such occurs, educate the filing public that this information is not legally required or wanted.
- Include vigorous public education campaigns when implementing any changes to the filing process. Ensure that filers are notified that they may be disclosing sensitive personal information in public records.
- Consider changing policies to allow for instant redactions, application rejection and penalizing filers for including extraneous information.<sup>15</sup>

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### NEXT STEPS: INTEGRATING APPROACHES & DEVELOPING STANDARDS

When it comes to state redaction practices and policies, there is no such thing as uniformity. Each state has its own methods and technological approaches, in addition to varying resources available for carrying out the redaction work. For example, North Dakota performs manual redaction on a case-by-case basis when copies of documents are requested.<sup>16</sup> Contrast this with Ohio, where a combination method of automated redaction and visual verification have been employed for all filings processed since 2006.<sup>17</sup> Meanwhile, some states are beginning to require redaction prior to posting a document online (other states exempt certain records from being published online).

Symposium participants agreed that state policymakers should work together to establish a multi-level, integrated approach to redaction that achieves the following:

- Encourages the development of uniform, legally-recognizeable terms and standards for redaction, with a focus on the particular types of personal information that should be considered for heightened security and privacy concerns.
- Enables state and county agencies that handle records to conduct comprehensive training programs regarding federal and state redaction practices and privacy laws; ensures compliance with all applicable federal and state laws in redaction practices. Involves multiple state agencies and the state bar.
- Educates the public on personal rights and responsibilities under the law through vigorous state outreach efforts, with an emphasis on protecting personal information privacy and security online.

Clearly, there is much work and coordination that has yet to be completed. IACA and other national organizations have begun some of these efforts, and NASS and eC3 hope to encourage and facilitate this dialogue to the fullest extent possible.

---

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

### **STATE PRACTICES IN UCC REDACTION POLICY MAKING**

The push for redaction has significantly affected how state offices around the country handle public records, particularly when it comes to the disclosure of Uniform Commercial Code (UCC) filings, most often handled by secretary of state offices. Buyers, lenders, insurers and others use these records to verify ownership of property and check for liens, but privacy advocates are concerned that personal information on UCC forms can be co-opted and misused. High-profile lawsuits aimed at requiring state governments to redact personal information are becoming more common.

This section highlights two instances of redaction policymaking, beginning with a 2006 landmark lawsuit filed in Ohio. A short summary with other state updates submitted by symposium participants follows.

#### **STATE OF OHIO**

In March 2006, a man filed suit against the Ohio Secretary of State's office after he discovered that his Social Security number was available online as part of the state's UCC filings database.<sup>18</sup> The state contended that it was not its responsibility to remove information from the online records, because the state had not requested that the Social Security number be provided. Nevertheless, the court approved a settlement requiring the Secretary of State's office to remove Social Security numbers from all current and future UCC filings posted on its Web site and until the lawsuit is dismissed, the state must report monthly on its progress in meeting that requirement.<sup>19</sup>

As the work to redact this information progressed, state officials realized that it was nearly impossible for their vendors to achieve the contracted terms of 100% accuracy. The vendors were focusing on two areas of the UCC form and missed information that was contained in attachments and other parts of the document.

In 2006, Ohio voters elected Secretary of State Jennifer Brunner, who is committed to maintaining the advantages offered by online UCC services. The state contracted with another vendor to review its backfiles and to determine what needs to be reprocessed.

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

Although the office continues to work to meet the settlement obligations, Ohio officials say the experience is showing that achieving 100% success in redaction is extremely costly and may be impossible to achieve.

Ohio has taken these actions thus far:

- Temporarily taken down public access capabilities to UCC filings database on the state Web site
- Began conducting manual redaction of incoming paper filings
- Began conducting manual redaction of outgoing document orders
- Began freezing any new agreements to sell data and images in bulk
- Sought legislation to allow rejection of filings containing SSNs, along with other related measures
- Retained a vendor for backfile redactions; a programming error occurred and the vendor is still under retention

Ohio still performs electronic filings and is applying the new redaction software prospectively, though the state does not manually check the online filings. The online system allows for attachments and the software scans all data as it is being uploaded, but it is based on optical character recognition (OCR), and so again, it is not 100% accurate.

### **STATE OF CALIFORNIA<sup>20</sup>**

California began a comprehensive effort in early 2007 to redact Social Security numbers in UCC filings, though the state is not as far along as Ohio. California has about 2.3 million filings (6.6 million images) that are the focus of redaction efforts. The Secretary of State's UCC section processes about 450,000 filings each year and estimates about one-third of those filings contain Social Security numbers.

Prior to 2001, the Secretary of State's office captured Social Security numbers in its UCC database and made that information available; bankers and lenders requested the service at the time. When Revised Article 9 of the UCC (RA9) went into effect in July 2001, Social Security numbers were no longer captured on the UCC database. When California's UCC

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

Connect went online in August 2004, the state allowed online filing and database searches. In March 2007, the Secretary of State's office disabled the searchable database function of the UCC Connect Web site, effectively shutting it down. At that time, state officials say approximately 60% of UCC filings were filed online and 98% of information requests were transacted online without staff intervention. The state is now processing by hand all UCC information requests until the Web site is back online.

The Office of the California Secretary of State receives about 30,000 UCC filings per month online, in contrast to just five hundred by paper. The online filings are computer-to-computer, requiring no human interaction. The UCC form does not contain a field for collecting a Social Security number<sup>21</sup>, although such information is sometimes inadvertently included as part of collateral descriptions or attachments. For this reason, the office has carried out an enormous outreach effort to instruct filers—as well as the general public—that these are public documents and SSNs should not be included.

At the same time, the Secretary of State's office is very limited by the Uniform Commercial Code as to the specific reasons allowed for rejecting a UCC filing. In fact, inclusion of a SSN is not one of the permissible reasons for rejection.

Secretary of State Debra Bowen has worked with the state legislature to address these shortcomings. Assembly Bill 1168, which takes effect in January 2008, requires the secretary of state's office to redact at least the first five digits of Social Security numbers from UCC filings. The office has since determined, based on its work with IACA, that it will redact all nine digits.

For each redacted record, the Secretary of State's office must create both a redacted "public record" and an un-redacted "official record." The public record is the only record available for information requests, while the official record is only available subject to a court order or subpoena. The filing office is also permitted to make forms available with blacked out boxes typically used for stating a Social Security number. The bill includes liability protection language that covers state officials as long as they conduct due diligence in locating and redacting Social Security numbers while using the industry's best practices at the time. The new California law also allows people to request that their Social Security number be

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

redacted from public documents. The Secretary of State's office must respond to valid requests within ten days. Secretary Bowen plans to address a large portion of the Social Security issue through backfile redaction efforts.

Actions that California has taken so far include:

- Temporarily taken down public access capabilities to UCC filings database on the secretary of state Web site
- Launched a substantial public education effort
- Began conducting manual redaction of incoming paper filings
- Began conducting manual redaction of outgoing document orders
- Temporarily froze new agreements to sell data and images in bulk until the backfile is redacted
- Sought legislation to allow rejection of filings containing SSNs, along with other related measures
- Released a request for quote (RFQ) asking for backfile redaction services with a 99% accuracy rate

The most recent filing statistics indicate that California's public education efforts are working. While they were once receiving about 250 Social Security numbers per week on paper filings, they are now receiving fewer than 25 per week.

Once the redaction effort is complete, California plans to revise its bulk sales agreements to require those who wish to continue to get bulk purchases to perform a complete deletion of all of their older images and replace them with a complete set of the newer, redacted images.

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### OTHER STATE UPDATES:

**Mississippi** adopted Revised Article 9 for the UCC filings in 2002. At that time, the state authorized a rule that allowed for redaction of Social Security numbers at the time of filing, because of a state statute that said they were required to protect this information. The state built a manual redaction feature into its imaging software that incorporates language stating that the Social Security number was removed. The office is now focusing on the two million filings prior to 2002 that still contain this information.<sup>22</sup>

**New York** removed its UCC site from the Web in early 2007 due to increasing public concerns about the use and availability of Social Security numbers. The state corporations division is currently in the process of removing these numbers from online filings and will make the documents available via the Web once that process is complete.<sup>23</sup>

**North Carolina** has completed its statewide UCC redaction process and is now focused on other documents filed with the secretary of state's office, including old documents filed before online transactions were possible. The North Carolina General Assembly identified eleven specific items of personally identifying information that must be redacted. This has presented a significant challenge. It has also led to some inconsistencies in the availability of information. For example, if this information is filed with a local recorder, the information is allowed to remain on the record.<sup>24</sup> If the same document is part of the files of the Secretary of State's office, it must be redacted.

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### APPENDIX A: GLOSSARY OF TERMS

**Backfile Conversion:** The process of converting large volumes of documents, usually accumulated over time. Generally, backfile conversion consists of digitizing files or documents using high-speed scanning methods.

**Batch Processing:** A method of executing a series of items via computer, all at one time, without human intervention. A method of grouping a set of documents by a common factor.<sup>25</sup>

**Federal Employer Identification Number (FEIN):** A number issued by the federal government used to identify taxpayers that are required to file various business tax returns. It is also known as a Federal Tax Identification Number.<sup>26</sup>

**Intelligent Character Recognition (ICR):** An advanced optical character recognition (OCR) system that allows fonts and different styles of hand writing to be learned by a computer during processing to improve accuracy and recognition levels.<sup>27</sup>

**Manual Redaction:** Filing offices may redact information manually by creating a copy of the filing and manually crossing out or covering the information to be redacted. The redacted copy will then be added to the public record.<sup>28</sup>

**Optical Character Recognition (OCR):** The mechanical or electronic translation of images of handwritten or typewritten text (usually captured by a scanner) into machine-editable text.<sup>29</sup>

**Personally Identifiable Information (PII):** Any information relating to an identified or identifiable individual who is the subject of the information (i.e. social security number, date of birth, mother's maiden name, address, etc.).<sup>30</sup>

**Redaction:** The removal of information from the public record.<sup>31</sup>

**Uniform Commercial Code (UCC):** The UCC is a comprehensive model code addressing most aspects of commercial law. Currently, the UCC has been enacted in 49 states, the District of Columbia, the Virgin Islands, as well as partially in Louisiana.<sup>32</sup>



## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### APPENDIX B: IACA STATE REDACTION SURVEY (MAY 2007)

Note: Some states have updated their responses to this survey by providing information to NASS. NASS also re-formatted the survey results for this paper.

STATE	REDACTION PROCESS	DETAILS
ARIZONA	Manual Review (Redaction is carried out on a case-by-case basis.)	When customers request that personal information be redacted, the state accommodates them as long as the information is not required by statute.
CALIFORNIA	Manual Review	A copy of document is made, and a black felt pen or correction tape is used to redact. A copy of redacted document is then made. The general public is not authorized to receive specific confidential information. Depending on the document, law enforcement, government officials acting in their authorized capacities and select others are authorized to obtain this information.
COLORADO	Combination of Automated & Manual Review	<p>A 2001 state law removed the requirement to include SSNs on UCC documents. In 2002, another statute instructed officials to redact this information on older, stored filings. Colorado contracted with another state agency to redact the information, completing the work in 2003. IT stores documents in un-redacted form.</p> <p>In November 2007, the Business Division of the Colorado Secretary of State's Office completed an eight-month redaction project involving a combination of automated redactions with human review of results.</p>
FLORIDA	Combination of Automated & Manual Review	Florida began redacting Social Security numbers on Fictitious Name records in July 2000 and is 99% complete with the process. Two years later, Florida began the process on UCC records. To date, 95% of those records have been redacted.

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

STATE	REDACTION PROCESS	DETAILS
GEORGIA	Manual Review	The SSN/FEIN box of each UCC document is analyzed. Georgia began redaction of SSN/FEINs contained in UCC filings as of November 1, 2006.
ILLINOIS	Manual Review	Illinois began manually redacting in 2001 with Revised Article 9 of the UCC, filing by filing. All documents previously filed have not been redacted. Illinois would like to have a competitive comparison list of companies offering redaction products and prices in order to make an informed decision.
INDIANA	Manual Review	<p>Indiana is engaging in the manual review of documents for which they have received written or in person requests, or from entities not exempt from Indiana's Social Security Number Privacy Statute.</p> <p>Manual redaction only relates to the copy of the document that is sent out. Currently, previously filed UCC finance statements and new statements being filed are not being redacted. Indiana is in the process of reviewing software-based redaction technologies.</p>
MASSACHUSETTS	Manual Review	<p>Massachusetts makes a duplicate copy of the original submission and SSNs/FEINs are redacted at time of filing. Duplicate copy is made available to the public record without SSN/FEIN visible.</p> <p>Massachusetts redacts information at the time of filing and on a case-by-case basis for previously filed documents. The "time of filing" procedure was instituted in November 2006, and all documents filed prior to that time are redacted on a case-by-case basis. The plan is to redact all images dating back six (6) years with a software application.</p>

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

STATE	REDACTION PROCESS	DETAILS
MICHIGAN	Manual Review	Michigan manually redacts SSNs from Limited Liability Partnership (LLP) registration applications and from corporation annual reports (if such information was included on reports filed prior to 1996). No other information is redacted.
MISSOURI	Manual Review	Missouri is in the process of procuring software for automated redaction. Currently, all UCC records are being manually redacted. The state also redacts on a case-by-case basis. Redaction of SSNs and FEINs is done as a matter of course, and home addresses and signatures are redacted by request.
NORTH CAROLINA	Manual Review & RFP Currently Open	Redaction of all back-file UCCs was completed in April 2007 by using a software application to manually redact through visual identification and verification. Currently, an RFP is open to complete redaction on all corporation and other business entity documents online.
NORTH DAKOTA	Manual Review	SSNs and FEINs from documents on a case-by-case basis are redacted when copies of documents are requested.
OHIO	Combination Automated & Manual Review	Ohio began redacting in April 2006. Currently, the state is working on the redaction of newly and previously filed documents.
OREGON	Automated with Manual Review as needed	Oregon is implementing software that allows the business to set the rules of redaction. The state plans to process all of the images in their system.
PENNSYLVANIA	Manual Review	In August 2002, Pennsylvania began redacting SSNs and personal account information. When mail is opened, they attempt to redact manually. If not, redaction is accomplished through a computer application. Previously filed documents have not yet been redacted.

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

STATE	REDACTION PROCESS	DETAILS
RHODE ISLAND	Manual Review	Prior to Rhode Island providing information online, the state chose to backfile all records that were current at that time. This was done by taping the old 5x8 forms to the 8.5"x11" paper. During this process, redaction was done with correction tape.
TEXAS	Manual Review	Texas began redacting SSNs from documents filed as of June 17, 2005. They have not redacted previously filed documents, unless a customer makes such a request. UCC documents filed electronically are not reviewed, so if the filer includes their SSN in the collateral field, it would not be removed. Corporate documents filed electronically are reviewed before they are processed.
VIRGINIA	Manual Review	Virginia will be redacting five years worth of documents.
WASHINGTON	Manual Review	Secured Transactions Section (STS): Washington manually redacts SSNs and FEINs from copies before mailing them with a search. Business Organization Section (BOS): There is not an automated system in place for redaction. A filing that contains SSNs will be reviewed manually, either before scanning or upon request for a copy. STS: Data from that field is captured but not displayed on any output that is generated. These practices apply to all records in the database.

SOURCE: International Association of Commercial Administrators (IACA)/Revised by NASS Staff with Submitted State Office Updates in November 2007

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### APPENDIX C: ABOUT THE SYMPOSIUM

#### Organizers

##### National Association of Secretaries of State (NASS)

Founded in 1904, the National Association of Secretaries of State (NASS) is the oldest professional, non-partisan organization of public officials in the United States. Members include the 50 states, the District of Columbia and the territories of American Samoa, Guam, Puerto Rico and the U.S. Virgin Islands. For more information, visit [www.nass.org](http://www.nass.org).

##### National Electronic Commerce Coordinating Council (eC3)

The National Electronic Commerce Coordinating Council (eC3) is a consortium of national organizations that includes public & private sector leaders committed to identifying best practices for strategic change within government. For more information, visit [www.ec3.org](http://www.ec3.org).

#### Special Acknowledgements

NASS's eC3 Board Members responsible for organizing the redaction symposium:

Hon. Elaine F. Marshall,  
North Carolina Secretary of State

Hon. Matthew Dunlap,  
Maine Secretary of State

Hon. Brad Johnson,  
Montana Secretary of State



Pictured (L-R): Hon. Elaine Marshall (NC), Hon. Brad Johnson (MT), NC State Professor Julie Earp of ThePrivacyPlace.org, Hon. Kurt Browning (FL) & Hon. Matt Dunlap (ME).

---

## **PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES**

Working with these Secretaries of State, NASS Executive Director Leslie Reynolds and NASS Executive Assistant/Events Coordinator Rachel Becker served as chief coordinators of the symposium. NASS Communications & Special Projects Director Kay Stimson provided media training at the event and served as chief editor of this white paper. NASS Special Projects Assistant Juliana Milhofer provided white paper research and writing assistance. John Smith of the Office of the Maine Secretary of State also provided writing assistance and symposium notes.

Dan Combs, eC3 Board Member and President of Global Identity Solutions, served as moderator of the symposium.

### ***Sponsors***

The symposium and this white paper were made possible by the generous financial support and participation of the following sponsors:

- AmCad
- Appligent
- Celcorp
- Computing System Innovations (CSI)
- EDAC Systems
- Extract Systems
- ImageSoft
- Manatron, Inc. (Formerly Hart InterCivic Records Management Division)
- RapidRedact

### ***Presenters***

- Julie Earp, Ph.D, Associate Professor, North Carolina State University (representing ThePrivacyPlace.org)
- Tim Poulin, Maine Director of Corporations, International Association of Commercial Administrators (IACA) Representative
- Tim Hall, Attorney at Law, CT Corporation
- Kay Stimson, Director of Communications & Special Projects, NASS
- J. Kelley Wiltbank, Chief Counsel, University of Maine
- Debora Batta, Director of Business Services, Office of the Ohio Secretary of State
- Betsy Bogart, Chief of Business Programs Division, Office of the California Secretary

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

of State

- Jerry Handfield, State Archivist, Office of the Washington Secretary of State
- Dan Combs, ec3 Board Member, President of Global Identity Solutions

### ***Participants***

- Scott Bade, President, ImageSoft
- Randy Blevins, CEO, EDAC Systems
- Jim Blottman, Director of Business Development, Celcorp
- Hon Kurt Browning, Florida Secretary of State
- Hon. Lorraine Cortes-Vazquez, New York Secretary of State
- Virginia Gavin, President, Appligent
- Waylene Hiles, Director of Administrative Rules and Deputy Counsel, Office of the Missouri Secretary of State
- Mark Miller, Vice President of Sales, Extract Systems
- Cindy Philips, General Manager, Records Management Solutions, Hart InterCivic (Records Management Division now Manatron, Inc.)
- Henry Sal, President, Computing System Innovations (CSI)
- Dan Shapiro, First Deputy Secretary of State, Office of the New York Secretary of State
- Bill Thompson, Jr., Assistant Secretary of State, Business Services, Office of the Mississippi Secretary of State
- Kathleen Vasquez, UCC Manager, Office of the California Secretary of State
- Keith Whitelaw, Director of the Business Division, Office of the Colorado Secretary of State
- Glyn Williams, CEO, Rapid Redact
- Dallas Wolf, Chief Operations Officer, AmCad
- Val Wood, Director of the State Corporations Division, Office of the Washington Secretary of State

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### APPENDIX D: ADDITIONAL RESOURCES

NASS collected all of the handouts, research papers and other materials provided by symposium participants and made them available to the public. These resources are available online at: [http://www.nass.org/old\\_site/redaction07.htm](http://www.nass.org/old_site/redaction07.htm).

#### Presentations/Handouts from the Symposium

- [Defining the Issue - Why Are We Redacting?](#)  
Julie Earp, College of Management, North Carolina State University (August 2007)
- [Questions to Ask When Buying a Redaction Solution](#)  
Henry Sal, President, Computing System Innovations (CSI) (August 2007)

#### Federal Documents on Redaction Related Issues:

- [Combating Identity Theft: A Strategic Plan](#)  
The President's Identity Theft Task Force (April 2007)
- [Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain](#)  
U.S. Government Accountability Office (GAO), Statement of Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues (September 2005)
- [Common Risks Impeding the Adequate Protection of Government Information](#)  
The Department of Homeland Security (DHS) and Office of Management and Budget (OMB) (July 2007)
- [HR 3046: Social Security Number Privacy and Identity Theft Protection Act of 2007](#)
- [Private Sector Use of Social Security Numbers: Topics for Comment](#)  
Federal Trade Commission (FTC) (July 2007)

#### State Documents on Redaction Related Issues:

- [California Secretary of State UCC Website Notice Related to Redaction](#)  
California Secretary of State, Business Portal (2007)
- [Privacy Protection Recommendations: What to Do if Your Personal Information is Compromised](#)  
California Department of Consumer Affairs (February 2005)



## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

### Other Documents on Redaction Related Issues:

- [White Paper: Use of OCR in Redaction](#)  
AmCad (No date)
- [White Paper: Redaction of Personal Information from Digital Public Records](#)  
AmCad (No date)
- [End of Privacy](#)  
John Parkinson, CIO Insight Magazine (August 2007)
- [White Paper: Improving OCR and ICR Accuracy Through Expert Voting](#)  
Computing System Innovations (CSI), Presented by Michael Breithaupt, Océ Document Technologies (No date)
- [Case Study: Marion County Prevents Identity Theft With the Help of Kofax Ascent and VRS Technology](#)  
KOFAX, Computing System Innovations (CSI) (2006)
- [Important Uses of Social Security Numbers \(SSNs\) by Businesses and Government Agencies](#)  
Coalition for Sensible Public Records Access (CSPRA) (No date)
- [Identity Card Paranoia](#)  
Don Tennant, Computer World Magazine (August 2007)
- [The Public Record: Information Privacy and Access - A New Framework for Finding the Balance](#)  
Fred H. Cate and Richard J. Varn, Coalition for Sensible Public Records Access (CSPRA) (1999)
- [Identity Theft](#)  
Coalition for Sensible Public Records Access (CSPRA) (No date)
- [IACA Redaction Report](#)  
International Association of Commercial Administrators Redaction Committee (May 2007)
- [IACA Report - Jurisdictions Currently Redacting Information from Their Records](#)  
International Association of Commercial Administrators (January 2007)
- [What Rigorous Research Tells Us About Identity Risk Related to Payments and Financial Services](#)  
James Van Dyke, President and Founder, Javelin Strategy & Research, (June 2007)
- [White Paper: Privacy and Public Land Records - Making Practical Policy](#)  
Property Records Industry Association (PRIA) (January 2006)
- [SSN Remediation Project](#)  
University of Texas

---

**PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES****APPENDIX E: ENDNOTES**

---

<sup>1</sup> U.S. Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data*, January 25, 2006, p. 5.

<sup>2</sup> International Association of Commercial Administrators, *IACA Redaction Committee Report*, May 17, 2007, p. 3.

<sup>3</sup> National Conference of State Legislatures, "Introduced Social Security Legislation—2007 Session," available at [http://www.ncsl.org/programs/lis/privacy/SSN2007\\_Pending.htm](http://www.ncsl.org/programs/lis/privacy/SSN2007_Pending.htm).

<sup>4</sup> Symposium remarks by Keith Whitelaw, Colorado Secretary of State, Director of the Business Division.

<sup>5</sup> Symposium remarks by Randy Blevins, CEO, EDAC Systems.

<sup>6</sup> Zogby International, Zogby Poll: Most Americans Worry About Identity Theft, April 3, 2007.

<sup>7</sup> Zogby International, Zogby Poll: Most Americans Worry About Identity Theft, April 3, 2007.

<sup>8</sup> Symantec, *Internet Security Threat Report*, March 2007, p. 32.

<sup>9</sup> Symposium remarks by Dan Combs, eC3 board member and event moderator, who was referencing Symantec studies.

<sup>10</sup> International Association of Commercial Administrators, *IACA Redaction Committee Report*, May 17, 2007 p. 3.

<sup>11</sup> International Association of Commercial Administrators, *IACA Redaction Committee Report*, May 17, 2007 p. 3.

<sup>12</sup> Miller, Mark, Extract Systems, *Redaction 101*, January 2007, p. 2.

<sup>13</sup> Keith Whitelaw, director of the Colorado Secretary of State's Business Division, recently reported that the state has restored free, Web-based access to all images of secured transactions documents. The Division immediately contacted all customers with outstanding copy orders and informed them of the restored access. Whitelaw notes that customers were "thrilled" to hear the news, adding that they clearly prefer to obtain their copies via self-service through the Web.

<sup>14</sup> Symposium participant Henry Sal, President of Computing System Innovations, noted that the industry average cost is currently three to six cents (U.S.) per image, based upon the extent of data being redacted.

<sup>15</sup> For example, Indiana now requires an affirmation statement on its UCC filings to indicate that a filer has reviewed the entire document and that no Social Security numbers are contained in the document. The language guiding this practice specifically exempts county recorders from liability should a Social Security number be included. There is a \$500 penalty per transaction if someone doesn't properly complete the affirmation portion of the filing. Similar provisions exist in Wisconsin and Nevada.

<sup>16</sup> International Association of Commercial Administrators, *IACA Survey: Jurisdictions Currently Redacting Information*, p.4.

<sup>17</sup> International Association of Commercial Administrators, *IACA Survey: Jurisdictions Currently Redacting Information*, p.4.

<sup>18</sup> Excerpts of symposium remarks by Deborah Batta, Director of Business Services, Ohio Secretary of State's Office.

<sup>19</sup> Columbus Dispatch March 29, 2006, available online at

---

## PRIVACY, PUBLIC ACCESS & POLICYMAKING IN STATE REDACTION PRACTICES

---

[www.columbusdispatch.com/live/contentbe/EPIC\\_shim.php?story=175978](http://www.columbusdispatch.com/live/contentbe/EPIC_shim.php?story=175978).

<sup>20</sup> Excerpts from symposium remarks by Betsy Bogart, California Secretary of State Business Division.

<sup>21</sup> California's Information Practices Act protects the disclosure of Social Security numbers, along with home telephone numbers, home addresses, financial information and medical information, except in cases where disclosure of such information is required pursuant to the Public Records Act.

<sup>22</sup> Excerpts from symposium remarks by Bill Thompson, Jr., Assistant Secretary of State, Business Services, Mississippi Secretary of State's Office.

<sup>23</sup> Excerpts from symposium remarks by Dan Shapiro, First Deputy Secretary of State, Office of the New York Secretary of State.

<sup>24</sup> Excerpts from symposium remarks by Hon. Elaine Marshall, North Carolina Secretary of State. The statute referenced is *NCGS 14-113.20(b)*.

<sup>25</sup> Keymark, Inc., available online at [http://www.keymarkinc.com/page.php?id\\_mnu=55](http://www.keymarkinc.com/page.php?id_mnu=55).

<sup>26</sup> Internal Revenue Service, *Understanding Your EIN, Employer Identification Number*, p. 7

<sup>27</sup> Wikipedia, Online Encyclopedia, available online at [http://en.wikipedia.org/wiki/Intelligent\\_Character\\_Recognition](http://en.wikipedia.org/wiki/Intelligent_Character_Recognition).

<sup>28</sup> International Association of Commercial Administrators, *IACA Redaction Committee Report*, May 17, 2007, p. 3.

<sup>29</sup> Wikipedia, Online Encyclopedia, available online at [http://en.wikipedia.org/wiki/Optical\\_character\\_recognition](http://en.wikipedia.org/wiki/Optical_character_recognition).

<sup>30</sup> About.com: *Identity Theft*, available online at <http://idtheft.about.com/od/glossaryofterms/g/PII.htm>

<sup>31</sup> International Association of Commercial Administrators, *IACA Redaction Committee Report*, May 17, 2007, p. 3.

<sup>32</sup> Duke University School of Law, *UCC Research Guide*, February 2007, p.1.