

TALKING TECH

Redaction Tips for Electronic Documents

By Kristin Nimsger, Esq.¹

Electronic evidence is multi-faceted, and even those individuals who consider themselves digital data gurus inevitably find it impossible to master every detail. One nuance of electronic evidence that may seem mundane, but actually warrants closer attention by all practitioners, is the process of redacting documents. A redaction is defined as the removal of protected information from a document before producing it to a court, opposing counsel, the public, or the media.

Obviously, redactions are an essential tool for “blocking out” sensitive data, such as company trade secrets, classified government documents, or legally privileged information from documents produced to other parties. Failing to redact documents so that the sensitive data is actually removed or made unavailable may result in handing over information the other side was never supposed to view, leading to damaging results for attorneys and their clients. Among other potential legal problems, failure to consider this danger could place the client at risk for privilege waiver based on inadvertent production.

A recent case in point proves instructive. In the spring of 2005, U.S. government intelligence officials undertook an investigation into the death of an Italian intelligence agent who transported journalist Giuliana Sgrena in Iraq.² Supported by the Italian government, Sgrena claimed the U.S. military specifically targeted her vehicle and deliberately opened fire at a security checkpoint.³ U.S. officials located in Iraq issued a classified report—detailing their findings in the incident—in PDF format to journalists located in Iraq.⁴ The officials believed they had redacted out classified names, dates and facts.⁵ However, it was widely reported in the press that by simply opening the document in Adobe’s free Acrobat Reader, hitting the “select text” button, copying and then pasting all the text into any word processor, any reader was able to see the highly classified information buried beneath the redactions.⁶ Using this technique, one journalist uncovered the “classified” information after cutting and pasting the redaction into a new document; the information ultimately found its way onto the Internet.⁷

One can easily imagine similar nightmare scenarios in the practice of law. Given the stakes involved in today’s complex litigation, corporate clients would no doubt take this type of information release as seriously as the government’s response to the release of classified information. Understanding these dangers, corporations involved in discovery must determine redaction best practices in

advance. How should a review team properly deal with redacted information? How can the team avoid inadvertently producing privileged or confidential information? This article will address potential dangers with redacting electronic documents as well as offer best practice solutions for review teams to consider when redacting digital data.

In the days of paper-based document discovery, document review teams redacted information using a black marker, white-out, or sticky white redaction tape. Reviewers who redacted the sensitive information in this hard copy format and then photocopied the document could rest assured that the information was “removed” from the document. However, digital documents present a whole new set of challenges. Attorneys conducting electronic discovery must take special actions to ensure privileged or other sensitive data is properly redacted from an electronic document. Failing to follow these precautions may mean delivering sensitive data into the opposing party’s hands. To ensure they are delivering only the information intended for the other side’s eyes, a review team should consider the issues below when conducting their next electronic discovery review.

- **Creating Redactions in Online Repositories.** Most online repository tools allow reviewers to create redactions while categorizing documents for responsiveness and privilege in a document set. Redacting in a repository is vastly different than using a black marker to block out sensitive information on a paper document. When a reviewer redacts an electronic document in an online repository tool, they place a black rectangle on top of the document image, covering up the text underneath. The review team should ask the service provider how that redaction is treated for purposes of review (i.e. is it moveable or transparent?). Can any reviewer or administrator see the text behind the redaction? Unless these questions are adequately addressed, such as through the use of various security settings in the online repository tool, any of the document review team will be able to see the hidden text behind the redaction.

- **Producing Electronic Documents as Redacted Images and Text.** The document review team must take special precautions if the party produces TIFF or PDF images, extracted text, and/or litigation support load files to the opposing party. This is true regardless of the document review format. During the production preparation process, the document review and production team must ensure that the expert selected to

assist with the production guarantees the redactions are “burned” into the document images. The team must work with the expert to ensure they do not produce redacted text located in the extracted text file that goes along with the image. The producing party should either produce only the non-redacted text or simply wipe out the entire text file.

- **Producing Redacted Documents in Online Repositories.** One of the fastest-growing electronic discovery trends is producing responsive documents in an online repository database. Online production databases can save parties considerable time and money because of the technology advantages they offer (searching features within the tool, hosting conducted by the electronic evidence expert, etc.). When production occurs in an online repository, typically the receiving party is given a set of logins and passwords to a separate database containing the relevant production documents. Comments, categorizations and other attorney work products are not transferred to the production database. Alternatively, this information is “locked down” and hidden from the opposing party. If producing in a repository, the review team should work with the e-evidence expert to ensure that redactions and redaction comments are locked down, ensuring the opposing party cannot see what is behind the redaction box. Additionally, if the online repository has an option to see extracted text or native views of the document, these options should be

disabled in the production database, so that redacted information is not inadvertently revealed.

The bottom line is clear: if precautions are not taken to protect redacted documents when preparing for a production, the danger of inadvertently producing confidential information is high.

Savvy receiving parties will be able to view what is buried beneath the redaction with little effort, just as the journalists did with the intelligence report released by the U.S. government. Understanding the technical loopholes relating to document redaction will put the producing party in the best position to verify all security measures have been taken to secure privileged or confidential information.

Endnotes

¹ Kristin Nimsger, Esq., is vice president of Legal Technologies at Kroll Ontrack in Eden Prairie, Minnesota. Ms. Nimsger is responsible for the evolution of products and service offerings for the Legal Technologies group at Kroll Ontrack.

² News story available at: <http://www.npr.org/templates/story/story.php?storyId=4626839>.

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

Redaction Best Practices

In the electronic age, parties should look for an online review repository that provides robust redaction capabilities and flexible administration of the redaction process. At a minimum, the tool should offer the features and capabilities listed below:

1. **Ease of creating redactions.** Seek an online repository that allows reviewers to create redactions while reviewing a document set for responsiveness and privilege. This functionality should be user-friendly (i.e., straightforward, like creating a text box in a word processing document).

2. **Redaction coding and ability to create redaction comments.** Reviewers should be able to select a redaction code (trade secret, attorney-client privilege, etc.) to label the redaction and enter comments at the time the redaction is created.

3. **Ability to export redaction information to a privilege or redaction log.** The tool should allow reviewers to export redaction codes and comments to a privilege log for the opposing party or court.

4. **Capability of locking down redactions with various security settings for review.** Redactions should have various security settings so that administrators can shield redaction codes and comments from low-level reviewers working on the document review or from the opposing party.

5. **Option to lock redactions for production and remove redacted text from extracted text.** When the redacted documents are produced, the tool should have the option to “lock down” the redactions, ensuring redactions are burned into the document images and redacted text is removed from any extracted text files.