

Take The Extra Time To Make Sure Your Documents Are Secure

Issues involving problems with metadata have been around for years. Due to client confidentiality and the sensitive nature of legal matters in general, metadata has historically been of particular interest and importance to the legal community. More recently, however, corporate, government and other non-legal entities are becoming acutely aware of the need to protect their sensitive files—and are dealing with the unpleasant consequences when they are not handled properly.

As an example, an unclassified Pentagon document containing highly sensitive information related to the death of an Italian secret agent in Iraq was exposed. Confidential information, including the names of the secret agent and the name of the U.S. soldier who shot her, were revealed. The report in question, a Word document containing large sections of redacted text, had been converted to PDF file format. The PDF file was made public by the Pentagon with the thought that it was secure—unfortunately, that was not the case. When the text of the PDF file was copied and pasted back into Word (or Notepad), all of the ‘redacted’ text appeared for all to plainly see.

What Went Wrong?

To the casual observer, it would appear that all of the necessary precautions had been taken. First, the sensitive text was redacted, and then the Word file was converted to PDF format as an extra precaution. So what happened? Well, digging a little deeper reveals a slightly different set of details.

For starters, the confidential text was not blacked out using standard redaction software; instead, Word’s highlighting tool was used—mistake number one. Secondly, the converted PDF file did not include the appropriate protections to prevent others from copying content from the PDF file—mistake number two. As a result, instead of creating what was supposed to be a secure file, the opposite occurred.

How To Prevent Something Like This From Happening

This was a classic case of improper document handling combined with poor protection applied on the PDF side. If you, or your firm, possess sensitive files that include redacted text, you should probably use redaction software specifically designed for this function. Alternatively, you can hand redact the text manually (with a black marker), scan the files with an OCR and then convert the files to PDF file format. Either of these two methods will ensure that the redacted information cannot be exposed, because the resultant files are a graphical rendering of the text that has been converted to PDF format.

If you don’t want to manually redact files and then scan them using an OCR and you don’t own redaction software, make sure that you apply the necessary protections to all files, including those converted to PDF file format. After first removing metadata from Word documents, use the Metadata Assistant’s set of PDF options that, when converting the cleaned files to PDF format, automatically add protections to prohibit the converted PDF file from being printed, modified,



copied, or annotated. For additional security, you can also have the Metadata Assistant automatically apply a password to the PDF file.

Go The Extra Mile

What can you do to protect yourself? Clean files with the Metadata Assistant first before sending them to others. When the recipient does not need the document in native format (e.g., Word, Excel, PowerPoint), convert the cleaned document to PDF file format and use the securities settings available to further lockdown protection of the PDF file. If you need to redact text within the file, use software specifically designed for redacting or manually redact the file, scan the file into an OCR and then convert it to PDF file format. An ounce of prevention is worth a pound of cure. Take the time to make sure that your sensitive files are protected. After all—they are your most important asset.

For more information, contact Payne Consulting Group at info@payneconsulting.com.