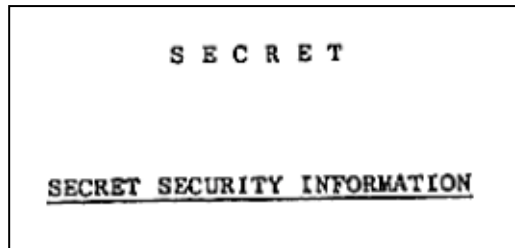


By [Kurt Foss](#), Planet PDF Editor

PDF Secrets Revealed

PDF file redaction snafu exposes agents' identities



The intertwined subjects of foreign agents, political intrigue and government overthrows almost always make for good reading -- especially when they are eyewitnessed reports of real events from our not-too-distant history.

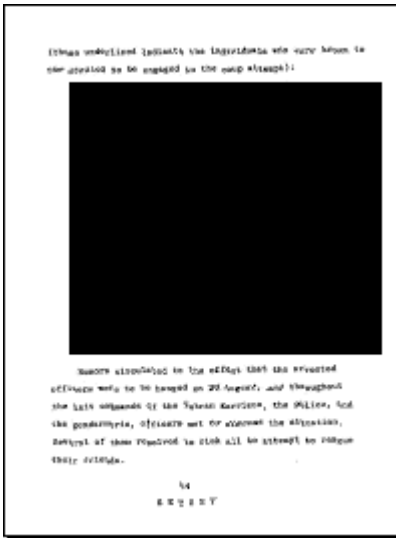
The challenge often is to tell a believable (and ideally accurate) tale without revealing too much - which might compromise current "information-gathering" activities, or at worst, put the lives of those involved in such past efforts in jeopardy.

Working for a globally recognized newspaper covering international affairs, The New York Times editors and reporters understand that some of their coverage may have consequences for others (and sometimes for Times' staff, too).

In mid-April 2000, the Times published a special report based on leaked, until-then secret CIA documents, a few of which they also made available for download as PDF files at its NYTimes.com Web site. The series of articles also referenced additional CIA documents in the Times' possession that editors concluded could not be made public - some of those identified might face retribution if exposed.

As expected, the publication of "[Secrets of History: The C.I.A. in Iran](#)" sparked lively, opinionated discussion within the newspaper's Web-based forums. Among the questions posted by readers was whether the Times planned to release all of the classified CIA documents, rather than selectively deciding what citizens should know about our government's questionable undercover activities in Iran at that time.

The editors apparently had a change of attitude in the following months. In mid-June, the Times updated the online coverage of the CIA-instigated military coup, making all of the intelligence agency's documents -- nearly 20 in total -- likewise available as PDFs. There was one key difference from the previously released set, one that added an extra touch of suspense -- and later, surprise.



After consulting with various historians, the Times determined it would be inappropriate - and potentially life-threatening for some - to name names. A bit like secret agents themselves, the Times opted to shield certain identities by electronically blacking out those names throughout the collection of scanned-to-PDF files. Once completed, the remainder of the CIA files from the 1953 overthrow went public.

Of course, as always seems to be the case for some segment of users, simply converting the documents to PDF provided a more than adequate protection scheme. Many of the scanned CIA documents weighed in between 2 and 3 MBs each, so failed downloads thwarted a certain percentage.

One such person maintained a sense of humor about his lack of success, posting to a Times' forum the following:

"Did anyone else have a hard time using the PDF file? I got an internal error message. What is this world coming to when you can't download a national secret on the web?"

No such problems for New York architect John Young who, despite working on an older, slower computer, was among those who downloaded the newly released documents in the first few days. Young easily noticed where identifiable details in the PDFs had been digitally obscured to mask out certain sensitive text.

Running Acrobat Reader 3.01 under Windows 98, along with several other bandwidth-taxing applications on his aging 166Mhz PC, Young also noticed something else -- that there were NO secrets in these once-secret documents.

With the computer's heavy workload causing the PDF documents to appear slowly on screen, Young watched as one file in particular first displayed the full page of text, and then the black mask fell into place a fraction of time later. But for an instant, he saw names where he was supposed to see only solid black.

"One page had a half-page redaction, which loaded slowly compared to the smaller redactions," Young says, "so I got a surprising glimpse of the text below."

"I experimented by careful manipulation of loading the target page in order to freeze it just before the redaction occurred."

The same technique worked throughout that section of the report, and in many other -- but not all -- sections, Young says. He eventually compiled a lengthy list of no-longer-secret names, and sent an email to the Times alerting them to the shortcoming in their redaction technique -- including a block of revealed names as proof.

How was this possible to defeat the security in such a highly sensitive document?

The PDF pages are in fact scanned images, opened and modified in Adobe Photoshop. Times staff didn't respond to several Planet PDF queries about the specific technique(s) used, and whether the redaction took place at the newspaper or elsewhere.

One of the real strengths of the Acrobat software suite is the ability for third-party vendors to create and sell [add-on tools](#) for specific niche applications. Among the numerous commercial plug-ins available is a product called Redax from [Digital Applications](#) that's designed for this exact task. Many government agencies and companies use it to protect vital information within private documents that later need to be made public.

Young credits his happenstance discovery on the use of a slower-than-average computer, noting in his comments about the incident -- posted at the [Cryptome.org](#) Web site he also administers, and where he later posted the full report including all names -- that people working on more current models wouldn't see the delayed display.

However, in inspecting one of the PDF files, we quickly determined that while that Young's reasoning might be true for anyone viewing the CIA documents with only the free Reader, it is definitely not the case for anyone using the full commercial Acrobat 4.x software.

Using Acrobat's Touchup Object Tool -- hidden from view by default, accessible (see below) in a pop-out window behind the TouchUp Text Tool in Acrobat 4.x -- it took a matter of seconds to [manually remove](#) a large redaction on one page, quickly revealing some 20 names.



After being notified by Young, the Times temporarily removed the CIA PDF files from its Web site "until we can delete the names in a more secure fashion."

The versions of the documents currently available at the Times' site appear to utilize a slightly different method -- an image with sections containing names cut out. Times' staff did not reply to Planet PDF's questions regarding the specifics of the second technique used.

Also, unlike the first set of PDF files, examining the later versions indicates the use of Acrobat's standard security settings. Just one problem.

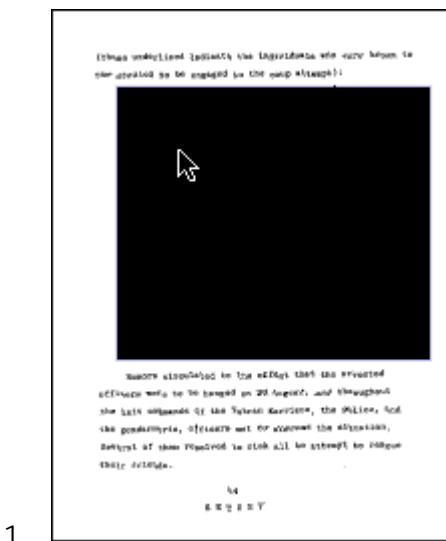
There was no password set to prevent anyone from changing the document's internal security -- a quick "Save As" allows for [easy removal](#) of the security setting -- by changing it from "Standard" to "None."

[NOTE: In this case, as the documents had been saved as a low-resolution image files, there was no benefit to using Acrobat's internal security settings. However, as there was an apparently deliberate attempt to use it in the second redaction effort, we felt it was important to point out for the sake of others that it was improperly configured. Had it been a necessary aspect of protecting these documents, the security would have been easily defeated.]

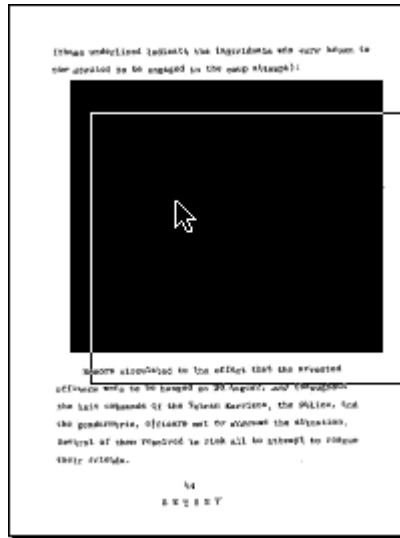
Another publicly posted comment in the Times' online forums -- that "some people know about the problem associated with PDF files" -- reflects a perception we're certain others will get from hearing about this incident.

To suggest that the weak link in the process was the chosen file format, however, doesn't match the facts.

Step-by-Step Removal of Attempted Redaction

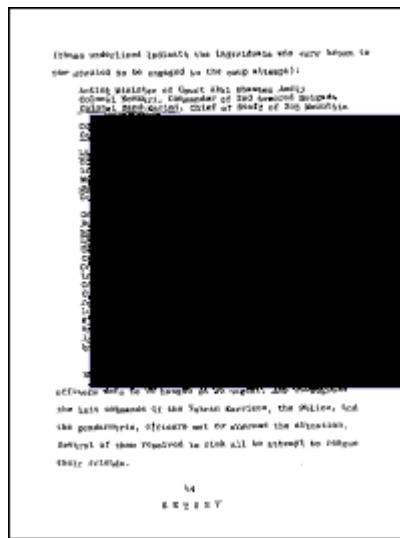


After selecting the TouchUp Object Tool (NOT the TouchUp Text Tool) in Acrobat 4, click and hold on the darkened overlay concealing the names.



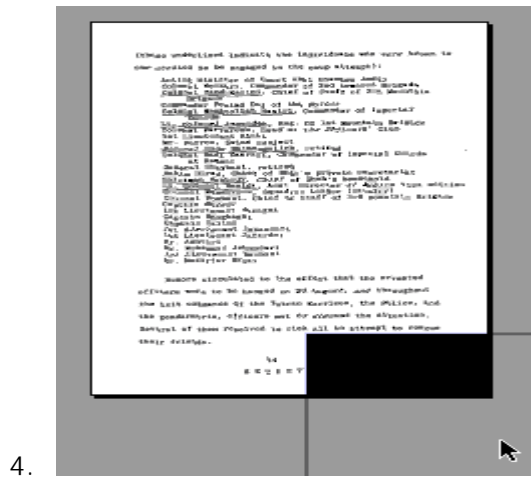
2.

Continue to hold the pointer on the dark overlay, then begin dragging it down or across the page.



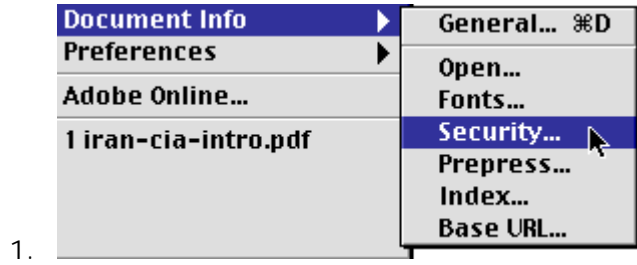
3.

As you continue dragging the overlay, the hidden text begins to appear.

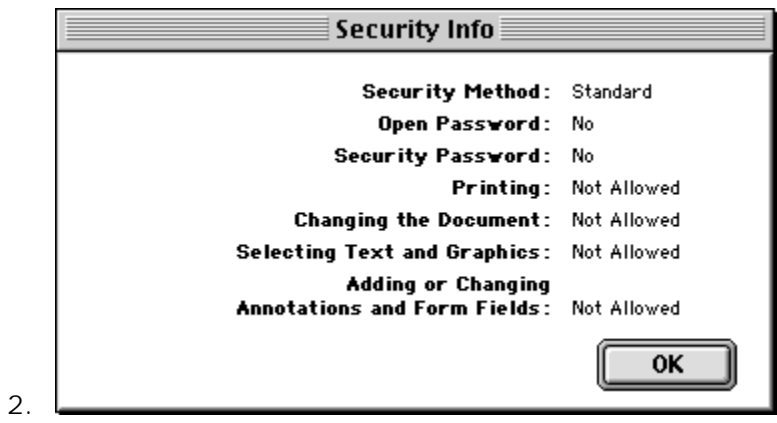


After the overlay has been completely removed, the names become easy to read -- and if not, use Acrobat's zoom tool to increase the size of the text on screen.

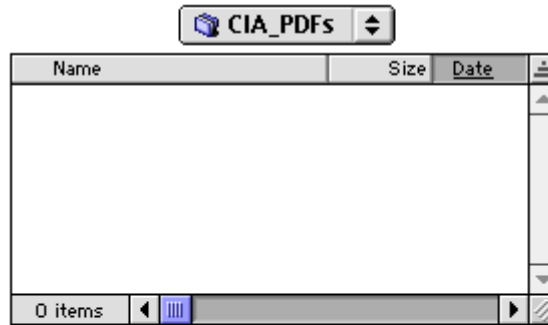
If your life depends on the file remaining secure, use a Security Password



Go to "File - Document Info - Security" to check the internal security settings of any PDF file.



This settings window shows that a level of "Standard" security was applied to the PDF file. However, an error was made that makes the security easy to override.



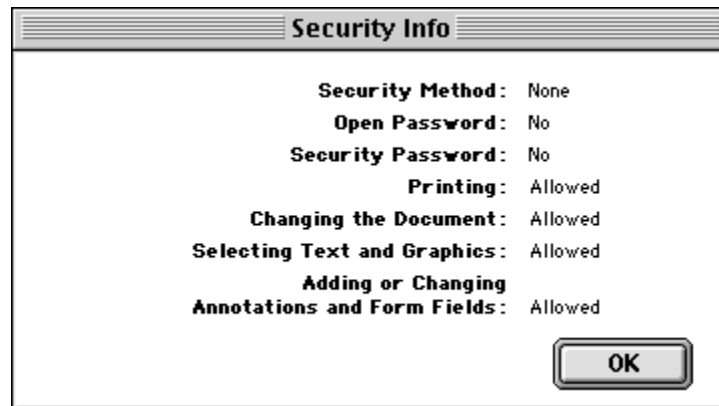
Save PDF File As:

iran-cia-intro.pdf



3.

Security in a PDF file is set when performing a "Save As" of the file; choose the appropriate option needed for your file. But ALWAYS set a password that MUST be used to change your security settings.



4.

In the Security Settings window in item 1 above, notice that the author failed to set a Security Password. [This may be where the phrase "false sense of security began!"] Without such a password, anyone can perform a "Save As" with the PDF file and change your intended setting back to NONE. That's as in 'NO Security.' No more secrets. Just hope that your life (or someone else's) doesn't hinge on an improperly configured PDF security setting.

<http://www.planetpdf.com/mainpage.asp?webpageid=808>