

APRIL 19, 2004

TECHNOLOGY & YOU

Don't Let Word Give Away Your Secrets

Hidden data can reveal too much about a document's murky past

When SCO Group ([SCOX](#)), a litigious Lindon (Utah) software company, filed a breach-of-contract suit in Michigan against DaimlerChrysler ([DCX](#)) in March, it revealed a lot more than it intended. A CNET News reporter, poking through the Microsoft Word ([MSFT](#)) filing, discovered that the case had originally been drawn up as a suit against Bank of America ([BA](#)) in a California court.

There's a lot more than meets the eye in many Word documents, a fact often overlooked when people e-mail Word files or post them to Web sites. The information that may be hidden in a Word, Excel, or PowerPoint file may include the names of the author and anyone who edited the document, reviewers' comments, the types and identification of computers on which the file was opened, and deleted text.

Most problems involve Word documents. One useful, but potentially dangerous, feature of Word is "track changes." When turned on, it keeps a record of who made what alterations and when. Unless you carefully clean up the document, which can sometimes be done with a single mouse click, anyone receiving it can see the record of changes by using the "show markup" mode. This is what trapped SCO. Another feature lets you keep an audit trail by saving versions of a Word document as it goes through revisions. Unless all but the last version is deleted before the file is circulated, a recipient will be able to see them.

OTHER INFO CONCEALED INSIDE A WORD FILE requires more skill and effort to retrieve. The most straightforward way to see the information is to open a Word document in a text editor such as Windows Notepad. Most of what appears on the screen will be gibberish, but there can be a lot of interesting information buried in the nonsense, such as the names of everyone who worked on the document. For example, a *Wired News* analysis of a Word document circulated by California Attorney General Bill Lockyer urging other attorneys general to crack down on file-sharing showed that the text had been edited or reviewed by an official of the Motion Picture Association of America.

Nearly every business exchanges electronic documents with partners, competitors, and customers. If those documents are written in Word, they are likely to contain information you would rather not share outside your own organization. How do you prevent it? One way is to select "Track Changes" from the tools menu and view the document as "Final Showing Markup." Make sure that all your changes have been either accepted or rejected by the program -- a step that removes the tracking information. And make sure all versions but the last have been deleted. But, as the electronic newsletter *Woody's Office Watch* notes, "it's very, very difficult to delete potentially embarrassing information all of the time."

One tool that helps get the job done is Microsoft's Remove Hidden Data, a free add-in to Office XP and 2003. But it's a better idea to avoid distributing Microsoft Office files unless absolutely necessary. People need to share information, but they don't need to give the recipients access to the original documents. One way to do that is to use Adobe Systems' ([ADBE](#)) portable document format (PDF), which can be displayed in the free and ubiquitous Acrobat Reader. It retains the formatting of the original document -- but strips all hidden data. Adobe's program for creating PDFs, Acrobat 6.0 (\$149), has extensive document-management features but is overkill for many uses. However, many other products can convert

Office files to it, including Macromedia's ([MACR](#)) RoboPDF (\$79) and ScanSoft's ([SSFT](#)) PDF Converter for Word (\$50). Apple Computer's ([AAPL](#)) Mac OS X has PDF conversion built in.

Computers, alas, are filled with traps to snare the unwary. Hidden data in Office files are just one more thing to worry about. Fortunately, precautions will keep danger at bay.

For a collection of past columns and online-only reviews of technology products, [click here](#)

By [Stephen H. Wildstrom](#)

Copyright 2000-2004, by The McGraw-Hill Companies Inc. All rights reserved.

[Terms of Use](#) [Privacy Notice](#)

BusinessWeek online



A Division of The McGraw-Hill Companies