

The Associated Press/New York

# Military Mistake caused data leak

By Anick Jesdanum  
AP Staff Writer

**MAY. 2 4:21 P.M. ET** Just a few clicks were enough to reveal names, training procedures and other secrets the U.S. military thought it had blacked out from an electronic report.

The data leak resulted from a type of mistake that is becoming increasingly common as government agencies and corporations scrap paper in favor of cheaper, faster distribution online.

"Software is basically a lot more complicated than mechanical typewriters, whiteout and black ink," said Richard M. Smith, a privacy and security consultant in Cambridge, Mass.

The U.S. military command in Baghdad produced the report in Adobe Systems Inc.'s popular Portable Document Format, or PDF, and posted it on the command's Web site Saturday. Its investigation cleared American soldiers of wrongdoing in the shooting of an Italian agent in Baghdad.

The blacked-out portions included names of soldiers at Iraqi checkpoints and their units. The material also discussed training for checkpoint duty, checkpoint procedures and general security in the Baghdad area, including the number of attacks since November.

John Landwehr, Adobe's director of security solutions and strategies, examined the document Monday and suggested its censors "simply put black rectangles over the text and did not delete any of the text itself from the documents. They were trying to do redaction with something not designed to do redaction."

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, readers can see what's buried beneath.

The military admits it goofed.

"We need to improve our procedures. We regret this happened. We obviously didn't take sufficient precautions," said U.S. Air Force Col. Donald Alston, a spokesman for U.S.-led forces. He added that some of the leaked information appeared classified.

Landwehr said companies and governments needing to delete secrets should turn to third-party redaction tools like Appligent Inc.'s Redax.

Smith suggested going further: Print the document, use markers to black out text and scan the document back in. Relying on a purely electronic copy, he said, spells trouble.

"Generally, it's a bad idea to send out electronic documents in sensitive situations," Smith said. "There can be all sorts of little things that can pop out."

Besides offering the ability to uncover blacked-out text, many documents carry "metadata" -- embedded information like the document's author and company. Users of Microsoft Corp.'s Word also routinely send files embedded with previous drafts, all revealed with a few clicks.

Smith used details hidden in one document years ago to help the FBI track down the author of the damaging "Melissa" computer virus.

Many lawyers have turned to PDF to prevent the Word leakage, said Albert Barsocchini, an attorney and director of professional services at Guidance Software Inc., which makes tools for recovering data.

The military breach is "another wake up that they have to go another step further," Barsocchini said.

The U.S. government has made similar mistakes before.

Large portions of a sensitive, 186-page Justice Department report about hiring and promoting minorities as federal prosecutors was digitally blacked out in late 2003, but savvy computer users could read the entire report.

The Department of Homeland Security warned businesses about hackers breaking into PBX telephone networks in June 2003, but every word of its electronic warning -- even passages thought deleted -- could be viewed.

And the Army in March 2001 inadvertently disclosed a rash of drowning during training exercises at one post by crews aboard Bradley armored vehicles.

"I'm surprised there hasn't been a more formal review that says when you release documents electronically, they have to be scrubbed with certain tools or procedures," said Ron Gula, who runs Tenable Network Security Inc. and used to test the security of government computers for the National Security Agency. Placing blame for such breaches is difficult, though.

"I would hesitate to call it stupidity," said Steven Aftergood, senior research analyst with the Federation of American Scientists' Project on Government Secrecy. "It's something no one would know unless they learn it, and it's an easy mistake to make. Unfortunately, sometimes the only way to learn is to do it the wrong way."

----

[http://www.businessweek.com/ap/financialnews/D89R8NR80.htm?campaign\\_id=apn\\_tech\\_down](http://www.businessweek.com/ap/financialnews/D89R8NR80.htm?campaign_id=apn_tech_down)

Associated Press writer Ted Bridis in Washington and Jamie Tarabay in Baghdad contributed to this report.

**Copyright 2005, by The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.**