American Bar Association Young Lawyers Division
The Young Lawyer

Copier Data Security Threat Puts Lawyers at Risk of Ethics Violations

By Paul Unger

You and your employer probably take data security very seriously. But if you are like many people, you are overlooking one data security threat that you use every day—your photocopier.

Did you know that your office copier could have gigabytes worth of confidential client information stored on its internal hard drive? ABA Model Rule of Professional Conduct 1.6 imposes a duty for lawyers to act competently and take reasonable steps to protect client information and confidences. To comply with Rule 1.6, lawyers must properly dispose of their copiers so that confidential information does not fall into others' hands.

Today's copiers are not one-trick ponies. They can scan, fax, and handle multiple print jobs at one time. A modern-day copier first scans an image to a hard drive and then prints copies. Anyone who gains access to your copier's hard drive can find images of documents that have been copied, potentially compromising such sensitive data as medical records, confidential papers, and documents subject to protective orders.

In February 2010, CBS News and a copier security expert went to a New Jersey warehouse to find out how difficult it would be to buy a used copier with data left on its hard drive. *See* Armen Keteyian, *Digital Photocopiers Loaded with Secrets: Your Office Copy Machine Might Digitally Store Thousands of Documents That Get Passed on at Resale*, CBS Evening News (Apr. 15, 2010), *available at* www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml. In a matter of hours, four copiers were purchased, packed, and loaded onto a truck for approximately $300 each.

One of the copiers still had documents on the copier glass from a major city's Police Sex Crimes Division. In only thirty minutes, the copier security expert found tens of thousands of documents using a forensic software program available for free on the Internet. The results were frightening—there were documents from the Sex Crimes Division; detailed domestic violence complaints; a list of targets in a major drug raid; ninety-five pages of pay stubs with names, addresses, and social security numbers; $40,000 in copied checks; and 300 pages of individual medical records, including everything from drug prescriptions, to blood test results, to a cancer diagnosis.

The lesson learned here is to take the simple steps necessary to protect yourself and your clients. Investigate your copier's capabilities. Some brands (e.g., Canon and Xerox) have protective settings that can encrypt or erase data on your machine. Talk to your copier vendor to ensure they enable these features. Before returning a leased copier to your vendor, selling it, or otherwise disposing of it, "scrub" the hard drive. Manufacturers sell this as a service or include it as part of a service contract. Lastly, remove the hard drive and keep it with you, or find a private copier service company to scrub the hard drive and provide you written verification of the same.

Photocopiers are easily overlooked when it comes to data security concerns. As a lawyer, you cannot afford to make mistakes with confidentiality. Find an experienced copier vendor that can help you ensure that data going through your copier stays under your control, even when the equipment is long gone.

***NEXT*STEPS**

- NEW! *The Tech Contracts Handbook: Software Licenses and Technology Services Agreements for Lawyers and Businesspeople*. 2010. PC # 5370188. Section of Intellectual Property Law.
- *Risk Management: Survival Tools for Law Firms*, Second Ed. w/CD-ROM. 2007. PC # 5110653. Center for Professional Responsibility and the Law Practice Management Section.

Paul J. Unger is chair of the 25th Anniversary of the ABA TECHSHOW (www.techshow.com) to be held April 11–13, 2011 in Chicago. He is a founding partner of Affinity Consulting Group in Columbus, Ohio, and can be contacted at punger@affinityconsulting.com.