



## **Is Information Stored in Your Photocopiers Causing Your Company Unnecessary Risk?**

Recent media coverage about the information stored on hard drives in photocopiers has highlighted a potential costly and avoidable risk that has existed for several years. Most photocopiers contain a hard drive which stores all documents printed or copied on the copier. The hard drive in the photocopier makes it similar to a laptop, desktop or network server in that it can store many documents that contain confidential or personal information for a long period of time. One of the greatest risks associated with the storage of this information is when the photocopier is returned at the end of the lease term or otherwise disposed of, all of the information is still on the hard drive and it can be accessed by the vendor or new owner of the copier, unless certain protective actions are taken. CBS recently aired a brief story on this situation that can be viewed at:

<http://www.cbsnews.com/video/watch/?id=6412572n&tag=contentMain;contentBody>.

If information stored on your photocopiers includes certain personal information such as a person's first initial or name and last name in combination with a credit card number, or social security number, or driver's license number, up to 45 State (including the District of Columbia) security breaches laws may be violated if the information is not encrypted or deleted. The consequences of violating these laws include costs associated with:

- Engaging forensic experts to analyze all of the data on the hard drive;
- Sending notification letters to the affected individuals whose information was on the hard drive;
- Following the de facto practice of offering at least one year of free credit monitoring service to each affected individual;
- Establishing or hiring a call center to handle questions;
- Legal fees;
- Lost productivity of employees that are part of the incident response effort;
- Potential FTC settlements; and
- Loss of customer, public and regulator trust.

You should consider taking the following steps to protect the information that may be stored on your photocopiers:

1. Contact the vendor that you acquired the photocopier from and confirm if the photocopier contains a hard drive. If it contains a hard drive, ask:
  - a. Is the hard drive encrypted?
  - b. How long images are stored on the hard drive?
  - c. What are the options to delete all information on the hard drive?
  - d. What are the options to prevent the storage of images going forward?

2. If the hard drive is encrypted, no further action is likely required. If not encrypted, steps c and d should be pursued and implemented.

Do not return a photocopier to the vendor/lessor at the end of the lease or dispose of it until you are sure that the information on the hard drive has been deleted.

**Important Note:** This paper is provided for informational purposes only, and is not intended and should not be considered to be legal advice.

---

### **About Navigate LLC**

Navigate LLC is a business consultancy that is focused on providing pragmatic, comprehensive, high value strategic and tactical information privacy advisory services. Navigate was founded by Chris Zoladz who most recently served as the Vice President of Information Protection & Privacy at Marriott International, Inc. from 1999-2009. For more information on how Navigate LLC can assist your company, please call 240-475-3640 or send an email to [info@navigatellc.net](mailto:info@navigatellc.net).

© Navigate LLC 2010.