Recently Google announced an additional feature to its popular Google Desktop search engine – the ability to store indexing information remotely, on Google’s own servers. The description at <http://tinyurl.com/gso84> includes the following explanation:

Search Across Computers makes the following files searchable from your other computers:
* Web history (from Internet Explorer, Firefox, Netscape, and Mozilla)
* Microsoft Word documents
* Microsoft Excel spreadsheets
* Microsoft PowerPoint presentations
* PDF files and Text files in My Documents

Note: Your HTTPS web history will never be shared with your other computers, whether or not you allow indexing HTTPS items on one of your computers.<

The explanation goes on to say, “In order to share your indexed files between your computers, we securely transmit this content to Google Desktop servers located at Google. This is necessary, for example, if one of your computers is turned off or otherwise offline when new or updated items are indexed on another of your machines. We store this data temporarily on Google Desktop servers and automatically delete older files, and your data is never accessible by anyone doing a Google search. You can learn more by reading the Google Desktop privacy policy.”

The privacy policy dated October 14, 2005 <http://www.google.com/privacy.html> details how Google collects information about searches, customizes advertisements, aggregates information, and provides details to law enforcement or uses the data in fraud-prevention processes.

Reader Jon Chorney, Systems Administrator at Master, Sidlow & Associates in Wilmington, Delaware sent me the following thoughtful analysis of liability issues for corporate employees contemplating use of Google’s Search Across Computers.

* * *

If I were to use that tool to remotely access any computer with confidential data (think health care, investments, etc.), it seems that I would compromise any precautions put in place to comply with applicable legislation. This is true no matter how secure the method I choose to connect to the remote computer.

Although Google may swear that access will be limited, no one with any care for confidentiality would want to place their trust in unvetted staff at another organization.

In February, the Electronic Frontier Foundation (EFF) issued a press release <http://tinyurl.com/7tk3s> warning that Google’s new tool would greatly increase government access to private information using a subpoena against Google instead of a warrant against an
individual – a drastic reduction in the burden of proof required for such access.

So, the implications of Dell pre-installing the tool on computers that it sells to business are, in my view, serious indeed <http://tinyurl.com/ethqg> and underline the need for strong, enforced policies regarding software installed on a business computer.

* * *

[Mich here again.] With respect to Jon’s concern about unvetted staff, I note that Google’s Privacy Policy states, “We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data. We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to operate, develop or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.” To the extent that we trust Google to follow its own rules, these are encouraging assertions.

However, many other commentators have noted that although the configuration of Google Desktop allows exclusion of specific directories from the search domain, few novices will pay attention to this security feature. Any system with Google Desktop using the Search Across Computers feature must be considered compromised until proven otherwise. Security administrators beware.

My thanks to Jon Chorney for his contribution. Readers -- keep those ideas coming!

* * *

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay & Jon Chorney. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.