New version of Google Desktop threatens user privacy

Mike Ingram
14 February 2006

The announcement last week of a new version of the popular Desktop utility from Google has provoked criticism from privacy groups and stern warnings to users from the digital rights advocate, the Electronic Frontier Foundation (EFF).

The EFF urged consumers not to use a feature called "Search Across Computers," warning that it makes their personal data vulnerable to government subpoena, private litigants, and hackers. "Coming on the heels of serious consumer concern about government snooping into Google's search logs, it's shocking that Google expects its users to now trust it with the contents of their personal computers," EFF Staff Attorney Kevin Bankston said in a statement published on the EFF web site.

"If you use the Search Across Computers feature and don't configure Google Desktop very carefully—and most people won't—Google will have copies of your tax returns, love letters, business records, financial and medical files, and whatever other text-based documents the Desktop software can index. The government could then demand these personal files with only a subpoena rather than the search warrant it would need to seize the same things from your home or business, and in many cases you wouldn't even be notified in time to challenge it. Other litigants—your spouse, your business partners or rivals, whoever—could also try to cut out the middleman (you) and subpoena Google for your files."

Google Desktop has been marketed under the slogan of "All your information in one place" and became popular due to its provision of desktop search facilities to allow full text searches over e-mail, documents, photos, chats, Gmail messages, web pages that have been viewed, in fact just about any data format can be searched through the use of third-party software through "plugins".

This functionality, however, carries with it a heavy price in terms of privacy. Google Vice President of Search Products and User Experience Marissa Mayer told BBC News, "We think this will be a very useful tool, but you will have to give up some of your privacy," adding, "For many of us, that tradeoff will make a lot of sense."

It is worth examining in some detail what is involved in this "tradeoff." Under the heading, "Information we collect," Google's privacy policy states, "The Google Desktop application indexes and stores versions of your files and other computer activity, such as email, chats, and web history. These versions may also be mixed with your Web search results to produce results pages for you that integrate relevant content from your computer and information from the Web. Your computer's content is not made accessible through Google Desktop to Google without your explicit permission."

The central issue here is not whether Google has access to your local data, but the fact that this is stored on their servers in the first place. This is particularly troubling in light of the US government's recent subpoena for search information. Though Google has so far refused to hand over details of searches made through its site, in contrast to rivals Yahoo and Microsoft, the Justice Department is seeking to enforce the subpoena through the courts. US officials insist they are not interested in data that will identify individuals, only what is being searched for. But privacy campaigners have warned that the subpoena is aimed at setting a precedent that will result in ever more invasive requests.

Google's privacy policy continues, "Your copy of Google Desktop includes a unique application number. When you install Google Desktop, this number and a

message indicating whether the installation succeeded are sent back to Google. Also, when Google Desktop automatically checks to see if a new version is available, the current version number and the unique application number are sent to Google. The unique application number is required for Google Desktop to work and cannot be disabled."

So, if you choose to use the features of Google Desktop, you are providing Google with a record of all your web activity, together with the contents of your hard disk and a unique identification number.

Version 3 of the Google Desktop introduces a new feature that, according to its web site, "now lets you securely find documents and web pages that you've seen on any of your computers from any of your other computers by using your Google Account." In order to use this facility, users have to consent to have their personal files stored on Google's servers for 30 days.

In addition to the very serious privacy issues raised by Google Desktop, there are basic security concerns. Only with this latest version has Google introduced password protection to allow computer users to block searches of their desktop being done either remotely or by gaining physical access to the computer. Not providing such basic protection was highly irresponsible given the number of security exploits of the Windows operating system upon which the Google Desktop runs.

Additional security concerns arise with the use of Google Accounts to facilitate shared access to data across the Internet. If the log-in details of your Google Account become compromised, then so does all of your personal data.

By its nature, this software is aimed at users with less understanding of computer technology. Those more familiar with the technology and corporate IT departments already have ways to make data on one computer securely available to others and will have less need for the Google enhancements. Unfortunately, the target users for Google Desktop are also less likely to configure the software correctly or choose strong passwords for their Google Account, thus making themselves more vulnerable to unwanted access to their information.

The privacy and security concerns far outweigh the benefits of software such as Google Desktop. Under conditions of recent revelations of illegal use of the National Security Agency (NSA) to conduct warrantless wiretapping of American citizens and the government subpoena for Google data, the launch of Google Desktop 3 threatens to further erode the privacy of Internet users.