White Paper

Are You Googling Your Privacy Away?

By:
Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.

This white paper explains in detail how Google and online search can be a threat to your internet privacy. As Google is the most preferred search engine, it digs deeper into everyday computing and gather personal and sensitive data from users. Google collects important information not only related to your query but also other sensitive information like the type of browser you're running, the sites you visited, the language your browser uses, your log-in details and your IP address. Google's policy to retain highly detailed search data for the analysis of marketing purposes is posing serious privacy threat for US residents.

Why does consumer privacy matter?

Since 2005, PrivacyRights.org has been tracking publicly reported data breaches.

In the year 2006, 243,000 records of Ernst & Young were breached. The situation is getting worse day by day. In June 2008, 2.2 million records of the University of Utah Hospitals and Clinics were breached. (See add. Table 1)

What's Google role in all of this?

So far, Google hasn't lost information, other institutions have.

However, Google plays an ever-increasing role in our lives, and the panoptical that Google has built, along with it's acquisition of DoubleClick and other firms, poses a serious threat to consumer privacy worldwide.

Let's tie the threads together….

Google Search

Google Search marked the onset of the Spider's Web and is gathering vital information of our online activities. Its future products will include data gathering and targeting as a primary business goal.

All of Google's properties including Google Search, Gmail, Orkut, and Google Desktop etc. have deep-linked cookies that will expire in 2038. Each of these cookies has a unique GUID, and can store search queries every time you search the web. Note, Google does not delete any information from these cookies.

Hence, if a list of search terms is given, Google can produce a list of people who searched for that term, which is identified either by IP address and/or Google cookie value. Conversely, if an IP address or Google cookie value is given, Google can also produce a list of the terms searched by the user of that IP address or cookie value.

Orkut

Orkut, Google's popular social networking site contains confidential information such as Name/ E-mail Address / Phone numbers / Age / Postal Address / Relationship Status / No of Children / Religion / Hobbies etc.

As per Orkut's Terms of Service, submitting, posting or displaying any information on or through the orkut.com service, automatically grants Orkut a worldwide, nonexclusive, sub-licensable, transferable, royalty-free, perpetual, irrevocable right to copy, distribute, create derivative works of, and publicly perform and display such data.

GMail

The primary risk in using GMail lies in the fact that most of its users give their consent to make GMail more than an e-mail delivery service and enable features such as searching, storage and shopping. This correlation of search and mail can lead to the potential risks, like:

- Mails may not get the legal protection, the ECPA gives on E-mail.
- The storage of e-mail on third party servers for more than 180 days can lead to the loss of those privileges.
- This in turn creates a danger that we may redefine whether an e-mail has the "reasonable expectation of privacy" needed for 4th amendment protection.

ECPA – Electronic Communications Privacy Act

ECPA, an act enacted in 1986, includes provisions for access, use, disclosure, interception and privacy protection of all electronic communications.
It declared e-mail as a private means of communication that has the same level of privacy as phone calls and letters. The employees of email companies cannot disclose emails to others and even the police would need a wiretap warrant to read emails.

Though Email in transit is protected, but those in law enforcement believe that once the mail is processed and stored, it is no longer a private letter, but simply a database service.

The biggest selling point of GMail is that they don't simply deliver your mail, but also store and index it so that you can search for it.

> **Is Gmail an email service or a database? The law is unclear.**
>
> **Law enforcement (and other entities) can access your online emails without notice after 180 days.**
>
> **Criminals / spyware / Trojans are actively targeting Gmail users for access to your contacts and inbox.**

GMail Mobile

GMail can now be linked to a cell phone number through a GMail invite on the phone. Here comes the all-important question

> **"How uniquely does your cell phone identify you?" When was the last time you changed your cell #?**

GMail Patents

Gmail's Patent #20040059712 emphasizes on "Serving advertisements using information associated with email". This allows Google to create profiles based on various information derived from e-mails related to senders, recipients, address books, subject line texts, path name of attachments etc.

Google Desktop

Google Desktop allows users to search their desktops using a Google-like interface. All word files, spreadsheets, emails, images on a computer are instantly searchable. Index information is stored on the local computer. Google Desktop 3 allows users to search across multiple computers. GD3 stores index and copies of files on Google's servers for nearly a month.

Using Gmail and Google Desktop on computers containing health records, financial records, educational records, credit applications, etc. could be a violation FERPA (Family Educational Rights and Privacy Act), HIPAA, Gramm-Leach Bliley, PCI-DSS and state privacy laws.

Potential abuses of Desktop Search products

- With Desktop Search products employers can always access their employee's computers. So, if an employee considers taking up a new job and writes a email to this effect, it can always be traced by the employer.
- Desktop search products enable spouses to read emails and discover secret love affairs.
- Desktop search can easily recover porn sites viewed in a computer.
- In a business negotiation, if a computer is left alone, then your competitor can easily scan for sensitive information with the help of desktop search.

Chrome

Google's browser Chrome logs every key-stroke typed in the address bar and stores it in the Servers along with your IP address so that Google's Suggest feature can automatically recommend terms or URLs you may be looking for, next time you search the web. This information can also be linked with your main Google Account because Google sends your cookie along with every automatic search it performs from the address bar.

Another new Chrome feature shows the six most visited pages when opening any new tab. Chrome gets these linkable thumbnails by taking snapshots of most pages you visit.

Android

Google Android, an open source cell phone operating system, poses a privacy risk as it stores the user's search and calls histories and also has the ability to reveal the user's location.

Google has more capabilities than anyone else to capture personal information with or without your knowledge.

What the CIA and the KGB never dreamed of collecting, consumers and users give to Google unknowingly.

What can you do about it?

- Using a dedicated browser for online searches
- Uninstall the desktop search products
- Restrict or ban the use of Gmail, Hotmail, Yahoo! Mail, other free online services.
- Restrict or ban the use of Orkut, MySpace, Friendster, etc.
- Using web anonymizers or TOR to scramble the online traffic paths
- Regularly conducting a data privacy and information security audit

Contact Information:

Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
C: 917-685-7731
P: 212-221-8660 x 202
raj@brainlink.com
www.brainlink.com

Table 1: Information leakages/ breaches of records from year 2006 - till date

Date	Organization	Cause	Records Spilled
02/13/06	Ernst & Young (UK)	Stolen Laptop	38,000
02/23/06	Deloitte & Touche (McAfee employee information)	Lost CD with names, Social Security numbers and stock holdings	9,290
06/01/06	Ernst & Young (UK)	Stolen Laptop	243,000
06/14/06	American Insurance Group (AIG), Indiana Office of Medical Excess, LLC (New York, NY)	Computer server containing personal information was stolen	930,000
08/09/06	U.S Dept. of Transportation	Stolen laptop from a government-owned vehicle	132,470
10/23/06	Chicago Voter Database (Chicago, IL)	Hacking	1.35 million
12/13/06	Boeing (Seattle, WA)	Stolen laptop	382,000
01/22/07	Chicago Board of Elections (Chicago, IL)	Mistakenly distributed Computer discs	1.3 million
05/17/07	Georgia Div. of Public Health (statewide)	Discarded paper records containing parents' SSNs and medical histories	140,000
05/19/07	Illinois Dept. of Financial and Professional Regulation (Chicago, IL)	Hacking a computer server	300,000
07/23/07	Fox News	Hackers accessed names, phone numbers, and email addresses	1.5 million
08/23/07	New York City Financial Information Services Agency (New York, NY)	Stolen laptop	280,000
11/16/07	U.S. Department of Veteran Affairs (Washington D.C)	Dishonest Insider	185,000
12/05/07	Memorial Blood Centers (Duluth, MN)	Stolen laptop	268,000

12/28/07	Davidson County Election Commission (Nashville, TN)	Stolen hard drive	337,000
01/08/08	Wisconsin Department of Health and Family Services (Madison, WI)	Printed Social Security numbers on informational brochures	260,000
02/27/08	Health Net Federal Services (Rancho Cordova, CA)	Openly posted personal information like Social Security numbers, etc.	103,000
03/17/08	Hannaford Bros. supermarket chain (Portland, ME)	Stolen credit and debit card numbers during the card authorization transmission process	4.2 million
04/17/08	University of Miami (Miami, FL)	Stolen Computer tapes containing confidential information	2,100,000
06/10/08	University of Utah Hospitals and Clinics (Salt Lake City, UT)	Stolen Billing records	2.2 million
11/01/08	Baylor Health Care System Inc. (Dallas, TX)	Stolen laptop	100,000 7,400 were SSN