

Google and your Privacy By: Noor Kharrat

Many take Google.com for granted. The number one most used website to search and the number two most visited site has recently been under criticism by many individuals and groups about its privacy. Google is based in Mountain View, California and is regulated according to US laws. This means that Google has to follow the USA Patriot Act, which is a controversial Act of Congress that U.S. President George Bush signed into law on October 26, 2001. All Google's applications and services that it opens to the public are bound under that act. Google.ca, Google.co.uk, Google.cn all fall under google.com. The servers that hold international sites for Google are still located in US grounds. The rights group "Privacy International" rated the search giant as "hostile" to privacy in a report ranking web firms by how they handle personal data. The group said Google was leading a "race to the bottom" among Internet firms many of whom had policies that did little to substantially protect users. (BBC news channel)

Here are some of the reasons why Google was declared "hostile to privacy":¹

- IP addresses are not considered personal information. They do not believe that they collect sensitive information. (privacyinternational.org, 2007)
- Google maintains records of all search strings and the associated IP-addresses and time stamps for at least 18 to 24 months and does not provide users with an option. (privacyinternational.org, 2007)
- Google has access to additional personal information, including hobbies, employment, address, and phone number, contained within user profiles in Orkut, which is a social network similar to the much popular Facebook. (privacyinternational.org, 2007)
- Google collects all search results entered through Google Toolbar and identifies all Google Toolbar users with a unique cookie that allows Google to track the user's web movement. (privacyinternational.org, 2007)

On the bright side, Google is a member of Safe Harbour, a set of standards created by the European Commission that focus on data protection. The compliance standards were set up to bridge the gap between European and U.S. privacy laws. "Google has also gone to court in the past to defend its user's data on YouTube from a demand by Viacom that it hand it over in July. Google struck a deal with the media conglomerate to provide the data only after making the user information and IP addresses anonymous." (Jackson, 2009). However, when it comes to government, it is another issue. Google would have no power but to comply when dealing with national security which is predefined under the Patriot Act. After heavy criticism by Internet users and organizations concerning Google's vague privacy policies, Google launched a program called "Google Dashboard"² which is a service that allows a person with a Google account to view their personal information associated with their account. The website also shows whether the information is public or not. This website was launched in November, 2009.

Google has been releasing applications to educational institutions promising "free services" such as email, calendaring, and collaboration tools right from the browser. Let us look further into these applications and see how "private" they are.

Lakehead University was the first Canadian educational institute to offer its members "Google Apps for Education". It saved the university significant manpower by not having to maintain their own servers; a cost that can be very substantial. It took just 16 hours of staff time to put the system in place, and the rest

¹ To see how Google and other companies did in Privacy, please see:
<http://www.privacyinternational.org/issues/internet/interimrankings.pdf>

² Google's Dashboard website: <http://www.google.com/dashboard>

was taken care of by Google with its superior network infrastructure. It also promised its members low downtime and 24/7 technical support. It has saved Lakehead millions of dollars as well as a lot of time and effort (Jackson, 2009). Google Apps offers a built-in backup system and allows Lakehead to maintain administrative control over the accounts. However, this free service raised eyebrows concerning user privacy, especially after the USA Patriot Act that gives the American government great powers to seize data on a whim and can prevent the user from ever knowing they are under investigation. Having an environment free of information being recorded is particularly important at universities because of many sensitive research studies that are being conducted. For example, a political scientist doing research on the rise of terrorism may trigger an algorithm labeling that researcher a person of interest if the data is being stored in the US, like the case of a Google email system.

Let us now take a further look into Google's privacy policies and try to read between the lines. An interesting fact is that Google's servers automatically record the following information when you visit their website or use their products: URL, IP address, browser type and language, and the date and time of your request. Google may share information with third parties in situations to comply with the legal process, to prevent fraud or imminent harm, and to ensure the security of their network and services.

In the case of Google Apps for Education, the domain administrator, who is the person in the organization responsible for managing Google Apps, has access to modify your account, suspend access or retain information stored as part of the account, including your email, contacts and other information. Also, the administrator can receive account information in order to satisfy applicable law. An important issue to point out is that no one has access to your password; it can only be reset. Also, the password stored with Google is not the same as your password, they are typically encrypted. However, the good news is that you can sign up with Google Apps using your own domain host, which makes all the information local. The rule of thumb is that what one sees publicly is what Google sees as well. It is up to Google to store this information in whatever fashion it wants. Google hides IP addresses after 9 months and hides cookies after 18 months. (FAQ Google privacy, 2009)

Now the question is how to protect the educational institution or any organization from privacy-theft. One way is to minimize any product or service from being public. Allowing a third-party to manage information that should only be read by an individual in the organization is not the best way for protecting identity. Take Google's webmail for education as an example; all the emails that are being sent back-and-forth are being kept in Google's servers. A solution would be installing in-house server that would manage email, calendaring, and collaboration tools right from the University. Another way of protection is to let a company within the same country manage anything that must be public. For example, letting a Canadian company manage webmail for a Canadian university would be a smart choice since the Canadian company and the Canadian university are governed by one law: the Canadian law. A Canadian company that would provide email servers is <http://www.exchangehosting.ca>.

In conclusion, total online privacy is virtually unattainable: the Internet is all about communication, and communication is inherently public. However, that is not to say that you cannot attain a reasonable level of privacy. It starts by administrators and the key is regulation. Just as the administrators carry the duties of protecting the users, the users have the duty of protecting themselves by being cautious when they are online. Although the abuse of privacy is widespread, there are very simple steps the user can take to ensure that the personal information is not leaked onto the web. The best part of the Internet privacy problem is that it is simple to avoid and users can educate themselves to be aware of risks associated with surfing online.

References:

- Jackson, Brian. "Privacy controversy mars Google Apps rollout at Canadian university." itbusiness.ca 11/7/2008 19 Jan 2009 <<http://www.itbusiness.ca/it/client/en/home/News.asp?id=50660&PageMem=1>>.
- Google.com, "Google Apps Education Edition." Free email and collaboration tools for your school 19 Jan 2009 <<http://www.google.com/a/help/intl/en/edu/index.html>>.
- Brownlee, John. "Keep Your Data Safe Online: Complete Guide to Online Privacy." October 20, 2008 19 Jan 2009 <http://www.popularmechanics.com/technology/how_to/4287844.html>.
- "Consultation Report: Race to the Bottom?." privacyinternational.org 2007 19 Jan 2009 <<http://www.privacyinternational.org/issues/internet/interimrankings.pdf>>.
- BBC NEWS CHANNEL, "Google ranked 'worst' on privacy." Google has the worst privacy policy of popular net firms, says a report. 11 June 2007 19 Jan 2009 <<http://news.bbc.co.uk/1/hi/technology/6740075.stm>>.
- Abaya, Eleanor. "Lakehead deploys Google Email for Education Campus Wide." AGORA online Volume 24. No.1 January/February 2007 19 Jan 2009 <<http://agora.lakeheadu.ca/agora.php?st=150>>.
- "Privacy FAQ." Privacy Center. 28 Jan 2009. Google.com. 28 Jan 2009 <http://www.google.com/privacy_faq.html>.

About the author:

[Noor Kharrat](#) is a third year Electrical Engineering student at the University of Windsor and a graduate of Fanshawe College holding a Technology Diploma in Controls Engineering Technology. For feedbacks, corrections or suggestions, please email: kharrat@uwindsor.ca