

Privacy at Google

Google™

Contents

Introduction	2
Google's privacy principles: Transparency and user choice	3
Putting principles into practice	5
Search	5
Strengthening Google's privacy practices	8
Why Google stores data	10
Personalization	12
Targeted advertising	16
Other Google products	18
Helping to protect users	21
Frequently asked questions	23
Glossary	27
Appendix	29

Introduction

As the information age becomes a reality for increasing numbers of people globally, the technologies that underpin it are getting more sophisticated and useful. The opportunities are immense. For individuals, a quantum leap forward in their ability to communicate and create, speak and be heard; for national economies, accelerated growth and innovation.

However, these technological advances do sometimes make it feel as if our lives are now an open book. Credit cards record where we shop and what we buy. Mobile phones track our every movement. Emails leave a trail of who we 'talk' to, and what we say. And blogs, video sharing sites and social networks make it possible to share almost anything (photos, home movies, one's innermost thoughts) with almost anyone.

That's why Google believes it's so important to have clear privacy policies - policies that are based on the principles of transparency and choice. Our users deserve to know what information is being collected and stored, and why, so that they can make informed decisions about the Google services they use.

We hope that this booklet will help you better understand what Google is doing to protect our users' privacy and to help raise standards across the industry.



Peter Fleischer
Global Privacy Counsel

Google's privacy principles: Transparency and user choice

All of us now trust companies with information online that is personal or sensitive. But it's sometimes difficult to work out exactly what information these organizations collect, or how they use it. For a start, most privacy policies are long, complicated documents that are hard to understand. And technology is changing all the time.

That's why Google believes it's critical to be transparent about our approach to privacy and to give users meaningful control – we want people to understand what data we store and why, so that they can make informed decisions about the services they use. Transparency and user choice are the principles on which all Google's privacy policies are based.

Google designs products to put the user in control

We build privacy protections into our services from the ground up. Take Web History for example, a sign-in feature which allows users to look back over sites they have visited or searched for in the past. If people don't want particular entries stored they can delete them. Or Google Talk, our instant messaging service. If users want their conversations to be "off the record," all they have to do is click a button.

None of Google's products use personal data unless fully disclosed in a privacy policy

Privacy policies are legal documents that provide people with notice about the information companies collect, and obtain their consent to its use. Personal data is information that relates to a particular identifiable individual.

At Google we aim to write our privacy policies in clear, simple language

Google tries to keep our privacy policies as short and simple as possible – with a one page summary at the top, followed by more detail underneath for users who are interested.

To read our privacy policies go to <http://www.google.com/privacy>. In addition Google is experimenting with privacy videos to help inform users about what we do and why: just visit <http://www.youtube.com/googleprivacy> to see them all.

We always ask people actively to opt in to services that use their sensitive data

Sensitive data is information about a person's health, sexual orientation or political beliefs, for example. So for a product like Gmail – which may store sensitive personal data contained in people's email – we always ask users to opt in to the storage of sensitive data in the service by opening an account.

Putting principles into practice

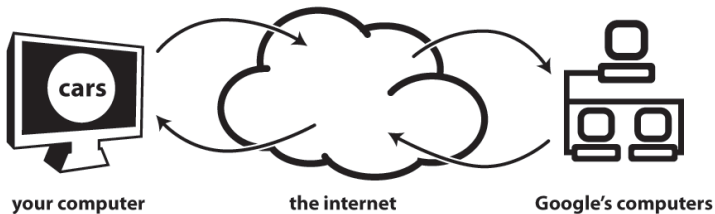
Search

Search - the ability to deliver relevant information on any topic to anyone, anywhere, instantly - is at the heart of what Google does. Today millions of people globally use our search engine. But what happens when people type their query into that box on our homepage – and what data, if any, do we store about that search?

Data retention practices

Let's take a simple search like cars.

When someone types the word “cars” into our search engine, the request gets sent from that user's computer over the Internet to our computers, which look for the right search results. Once our computers have found the results, they send these results back to the user's computer – again via the Internet. All this takes milliseconds.



This is the information that Google keeps: the **search query (i.e., “cars”)**, the time and date it was typed, the IP address and cookie of the computer it was entered from, and its browser type and operating system. Like almost all websites, we keep these records in our logs. Here's what a typical log entry at Google looks like:

```
123.45.67.89 - 25/Mar/2007 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 2.0.0.7; Windows NT 5.1 - 740674ce2123e969.
```

But what does this all mean?

IP addresses:

123.45.67.89 is the IP address assigned to the user's computer by his or her service provider. An IP address is a number assigned to each individual computer. When a user searches on Google, we use his computer's IP address to ensure that we get the right results back to the right computer.

It's important to remember that IP addresses don't say exactly where an individual user is, or who they are. In fact, some Internet Service Providers (ISPs) give users a different IP address every time they log onto the web. At best, all Google can tell about a user from his computer's IP address is that user's general location (for example London), and possibly the ISP they use to connect to the Internet. Only the ISP (who actually controls the user's account), can match an individual with an IP address.

Time and date:

25/Mar/2007 10:15:32 is the date and time the user typed the query into Google.

Search query:

<http://www.google.com/search?q=cars> is the search query, in this specific case "cars."

Browsers and operating systems:

Firefox 2.0.0.7; Windows NT 5.1 is the browser and operating system being used.

A browser - like Internet Explorer, Mozilla Firefox, Safari or Opera - is the software that enables computers to access the web. An operating system - like Windows - is the software that manages a user's computer.

Cookies:

740674ce2123a969 is the unique cookie ID assigned to a computer the first time a user visits Google. A cookie is, a cookie is a small file that gets stored on a user's computer; it looks like a lot of numbers, letters and symbols strung together. Like an IP address, a cookie doesn't tell Google who a user actually is or where they live - it only identifies a computer. A user can delete cookies at any time through the cookie-control panel in his computer's browser, as explained in detail below. A cookie records users'

preferences, for example whether a user wants his results in English or French, or if he wants to use a SafeSearch filter.

Strengthening Google's privacy practices

Time limits on data retention

While none of the data Google stores in its search logs identifies individuals personally, it can sometimes have personal elements, because it involves specific queries. For example, if a user runs a search on her own name and city, that search query reveals more information about a user than our prior example of a search for "cars." That's why earlier this year Google decided to delete the last two digits from the IP addresses and alter the cookie numbers in our logs permanently after 18 months. This breaks the link between the search query and the computer it was entered from. It's similar to the way in which credit card receipts replace digits with hash marks to improve customer security.

Here is what an IP address will look like in our logs after 18 months: 123.45.67.XX. After the same time period, the cookie will be replaced by a newly-generated cookie number.

Google was the first search engine to place time limits on the retention of logs data and we're pleased that others in the industry have followed our lead.

Time limits on cookies

In addition Google has decided to limit the lifetime of its cookies. When we originally designed them, we set our cookies to expire well into the future - 2038, to be exact - because their primary purpose was to preserve people's preferences, not to allow them to be forgotten.

But Google now plans to start issuing cookies that auto-expire after two years - unless they belong to someone who uses our services regularly, in which case the cookie will automatically renew itself. In other words, people who do not return to Google will have their cookies deleted after two years, while those who use the service regularly will have a cookie renewed for two years from the point that they use our services, and consequently will not lose their preferences.

Google has always allowed people to use its services without cookies (though this may mean losing the use of some features or functions of particular products).

For more information on managing cookies, please refer to the Appendix.

Why Google stores data

People often ask why Google needs to keep these logs at all. We store logs data for a number of reasons, the most important of which are to improve our search results and to maintain the security of our systems.

Innovation

Collecting data enables our engineers to analyze search patterns, which helps them to develop new, improved features for our users.

Google Spell Checker is a good example. If people misspell a word or name – say they type in David Beckham instead of David Beckham - they will not get the most relevant search results. So we ask them “Did you mean: David Beckham?” Google is able to do that because we’ve studied our search logs determine the most common spellings of words and names.

Logs data also helps Google improve the search algorithms that determine the order our search results appear. If our engineers can see that people are consistently clicking on the top result for any given query, they know they are doing something right. If people are hitting ‘next page’ or typing in another query, they know something is wrong, and can then take action to try and improve the search algorithms.

Protecting our systems from abuse

Search logs help Google improve the security of our systems. Without going into a level of detail that might compromise our security, here are some general principles.

There are lots of different search patterns, all of which have their own cycles - some are hourly, others monthly and a few even yearly. Understanding them helps us to distinguish between legitimate web traffic and malicious traffic generated by hackers or bots that probe for security vulnerabilities. When trying to distinguish between fraud and legitimate new patterns of behavior, it helps if we have old data to use as a benchmark.

Logs data helps our engineers fight web spam, which undermines the quality of our search results and is bad for users. This helps us fight attempts to manipulate our search engine rankings by people who create fake sites, links or traffic, all with the goal of influencing our search results.

Balancing security and privacy

There are no simple answers to the question of how long companies like Google should retain their logs data. Privacy legislation around the world requires us to strike a reasonable balance between the competing pressures we face – such as the privacy of our users, the security of our systems and the need for innovation.

Retaining data for shorter periods can help protect user privacy. But the longer Google keeps data, the more chance we have of protecting our systems from fraud and improving the services we offer – both of which are good for our users. We believe that keeping our logs data intact for 18 months strikes the right balance between the competing obligations we face.

Personalization

There was a survey conducted in America in the 1980s that asked people a deceptively simple question: “Who was shot in Dallas?” For many who had lived through the national trauma of 1963, the deliberations of the Warren Commission, the theories about the grassy knoll and the magic bullet, there was only one answer: JFK. For others, who had followed every twist and turn of the Ewing family saga, the oil barons’ ball and Cliff Barnes’ drink problem, there was also only one answer: JR.

The point of the survey was to show how exactly the same words can have very different meanings to different people depending on their background and their interests. It is the same idea that drives personalization at Google.

Personalized search

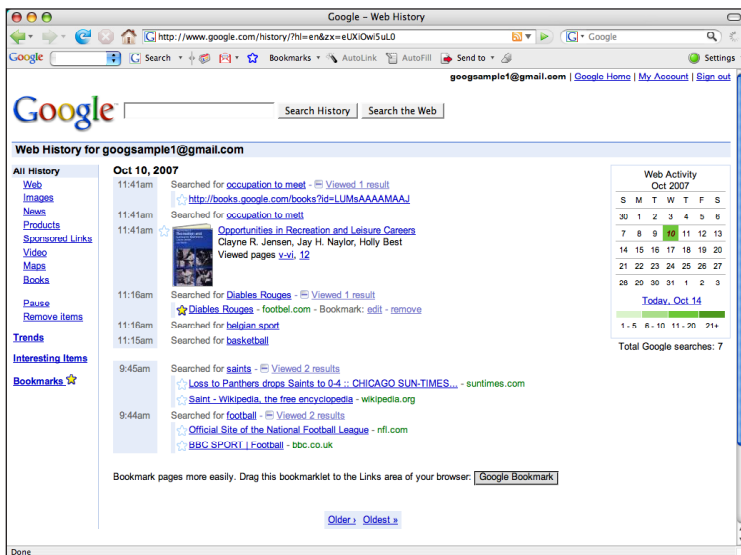
Google’s search engine is sophisticated - and most people end up with what they are looking for most of the time. Our search results aren’t always what a user was looking for, though, and that is because there is inevitably an element of guesswork involved. Do people searching for Paris Hilton want a hotel in the French capital or celebrity gossip? If users type in Chelsea are they looking for information about the football club or about different neighborhoods in London or New York?

An algorithm cannot provide all these answers. But if it can take account of an individual’s preferences it has much more chance of finding out what that person is looking for – closing the gap between what they typed and the result they actually want. The easiest way to think about personalized search is as a partnership between Google and the individual concerned – the user shares information about what they’re interested in with us and we give them better, more relevant results in return. Of course, not everyone will be comfortable sharing that kind of information with Google, which is why we leave the choice to the user. Users can choose whether to use the personalized service by opening a Google account and turning it on – and once they have we make it easy for users to opt-out again by closing their account.

Developing more personalized search results is crucial given how much new information is coming online every day. The University of California Berkley estimates that humankind created five exabytes of information in 2002 – double the amount generated in 1999. To translate that into something more familiar, absorbing five exabytes of data on television would require sitting in front of a screen for over 40,000 years. In a world of almost unlimited information and limited time, more targeted, personal results can really add to people’s quality of life.

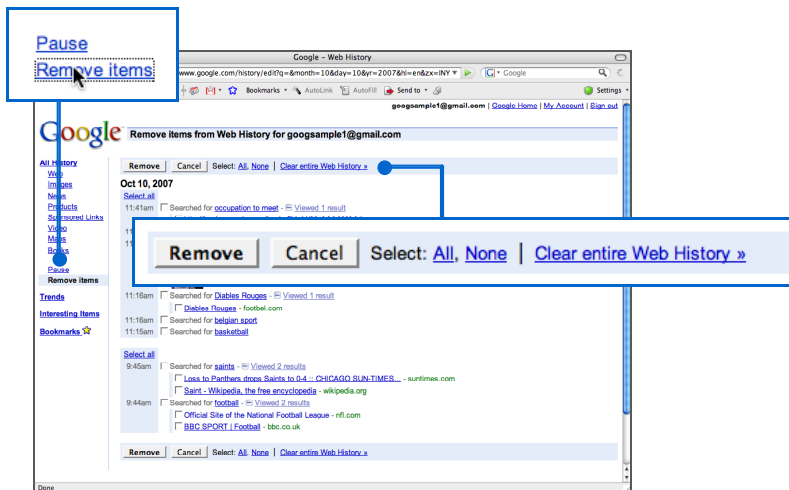
Web history

Lots of people find things on the web that they really like – a funny video, a great recipe for chocolate cake, a newspaper article – but then lose them. Web History enables users to find websites they have visited in the past quickly and easily (browsing the entire text of these pages) or look back over old search queries. Google also uses this data to help personalize a user’s search results.



Google not only requires users to actively choose to use Web History (it requires a user to have created a Google Account and to have installed the Google Toolbar) but we also enable users to make the service as personalized as they want. If someone's history, for example, contains queries or websites they would rather keep private, we enable them to edit, pause or delete these items. Users can opt out of Web History at any time.

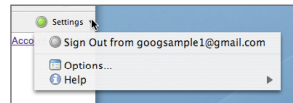
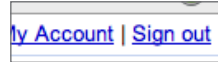
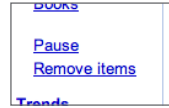
To remove items from Web History:



- Click on 'remove items'
- Check the items you want to remove
- Click 'remove' or if you want to delete all Web History items click 'clear entire Web History'

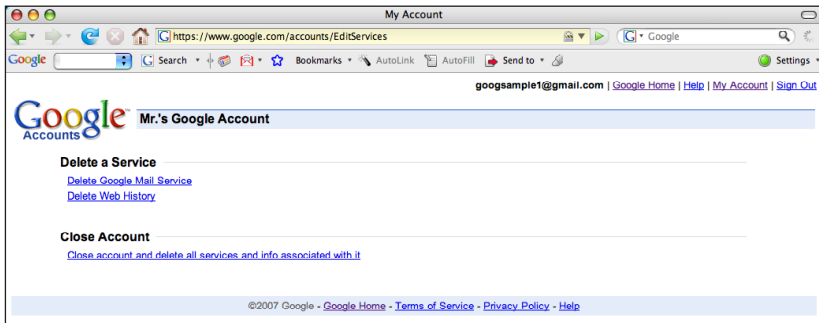
To pause Web History:

- From the Web History interface, click on 'Pause' or
- Sign out of your Google Account using the 'sign out' link on the top right of the screen or
- Sign out from the Google toolbar from the 'settings' menu on the right-hand edge of the toolbar



Web history will resume when you log in again

To opt out of Web History all together:



- Click on the 'My Account' link on the top right of the Google search page
- Click on 'edit' next to 'My services'
- Click on 'Delete Web History'
- If for any reason you'd like to terminate your Google Account, you can do so from this screen

Targeted advertising

Without ads, the Internet would be less useful and accessible than it is today. Advertising pays for most of the free content and free services that everyone now enjoys online. The more targeted the advertising, the more valuable it becomes – not just for advertisers or the websites they fund, but also for users who benefit from relevant rather than random ads.

There are many different types of online advertising, but the two most prominent are search and display ads.

Text-based ads

These are ads that are targeted based on search queries. If a user types “cheap flights”, for example, into Google, they will see lots of sponsored links on the right hand side of the page showing ads to travel companies. The ranking of these sponsored links is determined by a combination of what the advertiser paid for the ad in our auction (what is known as the cost per click) and the quality of the ad itself (what is known as its click through rate). The ranking of these ads is completely unrelated to Google’s basic search results.

Display advertising

In the early years, Internet ads were simple banners on web sites. Advertisers would buy these ads on the web sites their customers were most likely to visit. A tire company, for example, would place its ads on sites about cars. But display ads are now much more sophisticated. New technology platforms provided by ad serving companies like DoubleClick, Atlas and MediaPlex enable advertisers and web sites to target campaigns much more effectively based on user behavior. So if a user visits a web site with an ad that’s been served there using one of these company’s technology, a cookie is placed on that user’s computer recording data for the advertiser – including things like when the ad was delivered, what page it appeared on, the ads the user looked at and the IP address of the computer. This helps advertisers determine how successful their campaigns are and also helps to ensure that users see ads that are relevant and pertain to their interests.

A lot of online ad targeting does not raise particular privacy concerns – for

example, matching ads to the search queries people type in, targeting by location and language (information that is available from the geographic numbers included in an IP address) or age (for instance, placing ads on web sites which pensioners visit). Where privacy can become more of a concern is when cookies are used to target ads based on past user behavior, previous web sites people have visited, or ads they have clicked on before. This type of targeting is known as “behavioral targeting”.

This is new territory for Google. In April of 2007 we announced plans to buy DoubleClick.

In our ad serving, we’re going to experiment with a number of different ways to improve transparency – ideas which we hope will be adopted by the industry more generally.

These include:

- Providing better forms of ‘notice’ within ads, so that users can more easily understand who is serving them and what data is being collected; and
- Giving users the ability to provide feedback to us about the ads they like and don’t like.

Like all experiments, these ideas may or may not work out. But we are excited to start innovating in this particular area, not just for our users but for our advertising customers as well.

Other Google products

Gmail

Gmail is Google's web-based email service. It's easy to use, with virtually unlimited storage, great search and built in features like Google Talk, which enables users to chat with each other. However, people's emails are often highly personal and may involve sensitive information – that's why we require all our users proactively to sign up for a Gmail account. Contrary to many other email services, Google only asks for minimal data when a person opens an account: the user's first name; their surname; a login name; and password. People can even sign in using a pseudonym if they want, since we don't ask for proof of identity.

Google also places advertising on Gmail (it's a good example of ads helping to pay for the free services we all enjoy online) - so if you're emailing a friend about a trip to Paris, for example, ads might appear on the right hand side of the page for trains to France. Google does this using software similar to the kind that scans emails for viruses, to filter out spam and turn the bits of data received into the characters on the screen. No human being other than the user ever reads the messages sent or received on Gmail – it's simply a computer matching up key words in peoples' emails with targeted ads.

Google Desktop

Google Desktop enables users to search their computers as easily as they search the web – including all their emails and documents. This saves users a lot of wasted time looking for old files or messages they have sent. Of course a lot of this data is sensitive, so we require people to opt-in to the service when they download this software. People can remove any folders, documents, or emails they don't want included in the index at any time.

Lots of people work off of different computers. As a result, their information may be stored in different places. The optional Google Desktop Search Across Computers feature enables users to search all the documents they have saved – no matter what computer's desktop they're on. For example, people can find files that they edited on their desktop from their laptop. It's an opt -in feature and to use it users have to install Google Desktop on all of the computers they want covered – in other words they actively have to opt-

in to the service for each computer they use.

If users change their mind and want to turn off the Google Desktop Search Across Computers feature, their private index is deleted from our servers (the computers where we store data) and in no case will the index be stored on our servers for more than 10 days. To uninstall Google Desktop from a computer, users simply have to click on the 'Uninstall Google Desktop' program in their Google Desktop folder.

Google Earth

Google Earth provides users with a view of any point on the planet. This information enables users to do lots of different things - from planning a vacation (checking out that the hotel really is next to the beach as it says in the brochure) to organizing rescue efforts after a disaster. Users can search the globe, or view data on top of Google Earth, like maps, terrain, traffic and restaurants.

Much of the imagery on Google Earth is publicly available elsewhere, and it's imagery that users could also see if they were flying over properties or driving past them. There are different laws in different countries about what imagery can and cannot be shown. That's why the satellite and aerial imagery companies that provide the pictures are sometimes required to blur parts of them before they get to Google. Take a look at the Royal Palace in the Netherlands for example.

Google Maps and Street View

Google recently launched a feature on Google Maps called 'Street View,' which provides users with street-level imagery for select cities in the United States. Occasionally, an individual on the streets may be identifiable in Street View. The service gives users the ability to easily flag images like these and request that they be removed. The imagery available in this service complies with law in the United States relating to "public spaces,"— and we've worked with a number of different privacy groups on the product before we launched it. That said, we have publicly discussed different approaches we may take in other countries to comply with local privacy laws, which you can read about here: <http://google-latlong.blogspot.com/2007/09/street-view-and-privacy.html>

Orkut

Orkut, Google's online community with tens of millions of users, allows users to create profiles and interact with their social network to share stories, pictures, and meet new people. Privacy is obviously important on all social networking sites. That's why we've created tools that enable orkut users to control access to their online profiles. Users are given the option to restrict who sees their profile or friends information.

Google Docs

Google Docs is a suite of products that allows people to create and share their projects online and access them from anywhere. For each individual document, spreadsheet, or presentation that a user creates, he has the ability to be the sole user of that document, to share it with friends or co-workers, or to publish it and allow anyone to view it. No documents are shared by default, and users have to alter a document's 'share' controls to allow others to view it.

Helping to protect users

At Google we're fully aware of some of the dangers of using online services and we are working hard to help educate our users about them. Here are some scams to be aware of.

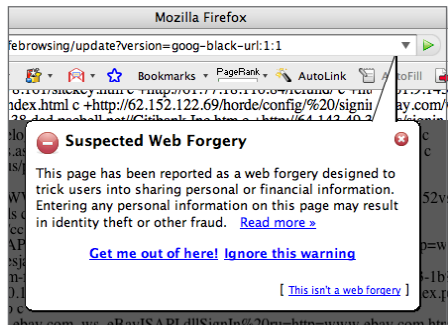
Identity theft

Some web sites use malicious software known as spyware to collect personal, sensitive information without a user's consent. People can often accidentally download this software onto their computers, or receive it in an e-mail. As part of our commitment to protecting the security of our users, we warn users before they visit sites that might be dangerous. We're also a member of the advisory board of StopBadware.org, a "Neighborhood Watch"-style campaign aimed at fighting spyware by identifying dangerous applications and sites. People can also use Google Pack - a collection of useful software, including Google Toolbar, Norton Security Scan and Spyware Doctor (Starter Edition) - to prevent spyware from being downloaded onto their computers.

Phishing

Phishers fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email or instant messaging, and often directs users to give their details at a particular web site.

Google services like Gmail automatically scan emails to try to filter out potentially malicious spam which is often the vehicle used for phishing, but unfortunately some phishers are successful in defrauding our users. We advise all web users to be careful when disclosing personal and financial information over the internet and to report any incidences of phishing to us whenever they arise. We also offer protection from phishing to users of the Google Toolbar.



Hacking

Hacking refers to the process of illegally gaining access to a computer through the use and modification of computer code. Hackers employ these measures to gain control of a device, take personal information without consent or to install malicious code. Enabling a firewall, like that included on your computer or available from many software companies, helps users to protect their computers from outside interference.

Badware

Spyware, malware, and other deceptive software can harm or take control of a user's computer. Through Google's relationship with StopBadware.org, we are helping to put a stop to this type of harmful software on the Internet. Google search results also warn users before they click through to a page that may contain Badware, helping them keep their computers secure.

Frequently asked questions

What data do you hold on me?

This depends on the service. For search, we store the following data in our logs records: your search query, the time and date you typed it, the IP address and cookie of the computer you used, and the type of your browser (Internet Explorer, Firefox etc.) and operating system (for example Windows Vista). It's important to note that IP addresses and cookies cannot by themselves identify individuals. They don't tell us where someone lives, or who they are. In fact some internet service providers give users a different IP address every time they log onto the web. At best, all Google can tell about someone from an IP address is their general location (for example London). Only the service provider, who actually controls the user's account, can match the individual with the IP address.

How long do you keep data in your search logs?

Eighteen months. At that point we permanently delete the last two digits from the IP address and randomly assign a new cookie number. This breaks the link between the search query and the browser it was entered from. It's similar to the way in which receipts from credit card transactions replace digits with hash marks to improve customer security.

If your logs data cannot identify individuals why bother to make this change at 18 months?

We break the link between the search query and the computer it was entered from at 18 months to give our users additional protection. While none of the data Google stores on its search logs identifies individuals personally (it doesn't tell us who people are), it is to some extent personal because it involves specific queries.

Why do you store it at all – surely you could delete it all immediately?

We store this data for a number of reasons, the most important of which are to improve our search results and to maintain the security of our systems. For example, the greater our engineers' understanding of the different search patterns that occur on our site, the better the chance we have of fighting fraud. And there are lots of different patterns all of which have their own cycles – some are hourly, others monthly and a few even yearly.

Why did you choose 18 months?

We strike a reasonable balance between the competing pressures we face – such as the privacy of our users, the security of our systems and the need for innovation. We believe 18 months strikes the right balance.

Who has access to this information – and can governments demand access to it?

Within Google a limited number of engineers can access this information – they use it primarily to help with research aimed at improving our services and protecting our systems from attack. There are strict protocols at Google for access to this data. In terms of the police and other law enforcement agencies, we comply with valid legal requests, like search warrants, court orders and subpoenas, as all responsible companies must.

Can the US Government, for example, demand European users' data – and would you make American users' data available to a government in Europe?

Yes to both of these questions, because we must comply with valid legal requests for information. It's important to stress that we only ever give data to third parties, including the US or other governments, if they have been through the proper legal process. Two years ago Google was the only search engine to resist the American Justice Department's demands for millions of user queries because we believed their request went too far. The presiding judge ruled with us over the government, which we feel was a resolute victory for user privacy. For more information about this case go to: <http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html>.

What happens when different privacy laws in different countries conflict?

Our privacy policy is pretty clear that most of our services are provided by Google Inc., which is subject to US law. But we are committed to complying with the law in the countries we operate in and we take EU requirements very seriously.

Why do you use cookies?

Cookies record users' preferences, for example whether they want their results in English or French, and if they use a safe search filter. Without them, Google wouldn't be able to remember what different people like and

most users don't want to re-set their computers every time they log on. If users are worried about cookies they can delete them and still search on Google (though they will obviously lose some functionality).

How long do your cookies last?

Google recently announced that we would start issuing cookies that auto-expire after two years – unless they belong to a regular user, in which case the cookie will automatically renew itself so that we don't lose that person's preferences.

Can personalized search identify people – what protections do you offer them?

Personalized search uses people's past search and browsing activity to give them more relevant, targeted results. Without this kind of information it's hard, for example, to know whether someone is looking for information about the football club or a district in London when they type "Chelsea" into our search box. Of course some people may not be comfortable sharing this information with Google – that's why we have made personalized search an optional service that's only available once someone has signed up for a Google account.

What is a Google Account?

There are certain services we offer, like Gmail or personalized search, which people can only use if they sign up for a Google Account. To do this people need to provide us with basic information - typically their name, email address and a password. This information is used to authenticate users and protect their accounts from unauthorized access by others.

Do you share your server logs with advertisers?

We only share anonymous, statistical information about our users with advertisers (e.g. how many users visited their site or clicked on their ad.)

I have targeted ads on Gmail – is someone actually looking at what I write to match the ads with my emails? Is this legal?

Except in the case where we are producing email in response to a lawful request for information, the only human being to read the emails sent or received on Gmail is the account holder. Like most email services, Gmail

uses software to scan emails for viruses and to filter out spam. Google uses the same kind of software to scan for keywords in users' emails which we can then match ads to. The whole process is automatic.

Do the images in Google Earth violate privacy?

Most of the imagery on Google Earth is publicly available elsewhere from governments and private sector providers. In addition, anyone who flies above or drives by a piece of property will see exactly the same pictures.

Google blurs imagery on Earth for governments – do you do the same to protect individuals' privacy?

There are different laws in different countries about what imagery can and cannot be commercially distributed or published. Where buildings are blurred on Google Earth – for example the Royal Palace in the Netherlands – this is actually done by the organization that provided the images to Google.

Street View captures images of people on the street? Is that legal?

Street View makes it easy for people to look at very local imagery. These pictures are useful when working out travel directions for example. If anyone wants pictures of themselves taken down, all they have to do is flag the image and we remove it. The images in this service are legal given the laws around “public spaces” in the United States – and we worked with a number of different privacy groups on the product before we launched it. That said, we have publicly discussed different approaches we may take in other countries to comply with local privacy laws, which you can read about here: <http://google-latlong.blogspot.com/2007/09/street-view-and-privacy.html>

How can I contact Google if I have a privacy question or complaint?

If users have any additional questions or concerns they can contact us any time through this web site http://www.google.com/support/bin/request.py?contact_type=privacy. People can also write to Privacy Matters, c/o Google Inc., 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA.

GLOSSARY

Badware

Spyware, malware, and other deceptive software can harm or take control of a user's computer.

Consent

A legal term describing the need for service providers to seek user's agreement before offering them a product.

Cookie

A small file stored by a web browser to record a user's preferences or activities for a specific website.

Display ads

Visually-based web advertisements, such as banners or skyscrapers.

IP address

A unique number assigned to an electronic device (such as a computer) connected to the internet.

Malware

Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a general term used by computer professionals for many forms of hostile, intrusive, or annoying software.

Notice

A legal term describing the need for service providers to give users information about, for example, their privacy policies.

Personal data

Information that can personally identify someone, such as their name, government ID number, or their photograph.

Phishing

An attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

Search query

The word or words entered into a search engine.

Sensitive data

Information that is intimate or confidential in its nature, such as health, sexual orientation, religious beliefs.

Server log

A file automatically created and maintained by a computer that records the activity it performs. See pg XX.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spyware

Computer software installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's consent

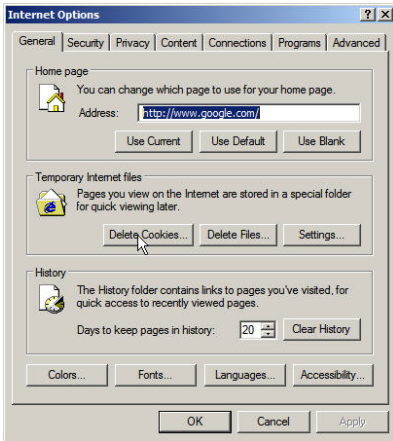
Text ads

Advertisements on a website that are text-based (rather than image-based). Text ads are often contextually targeted, based on the content of a web page or on a search term, etc.

Appendix

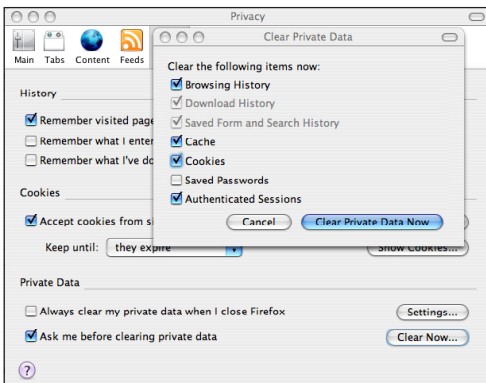
Managing Cookies

Users can easily delete cookies through Internet options (on Internet Explorer).



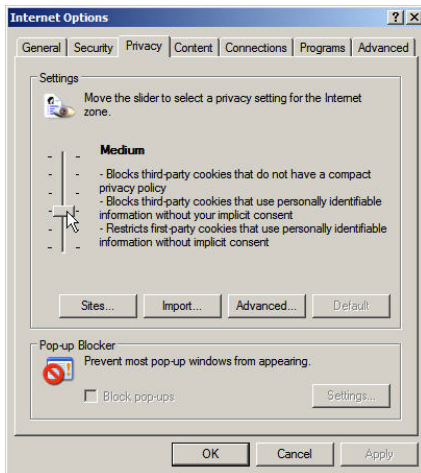
- Go to the 'tools' menu
- Select 'internet options'
- Select the 'general' tab
- Click 'delete cookies'

Firefox users can delete cookies through the Firefox preferences screen



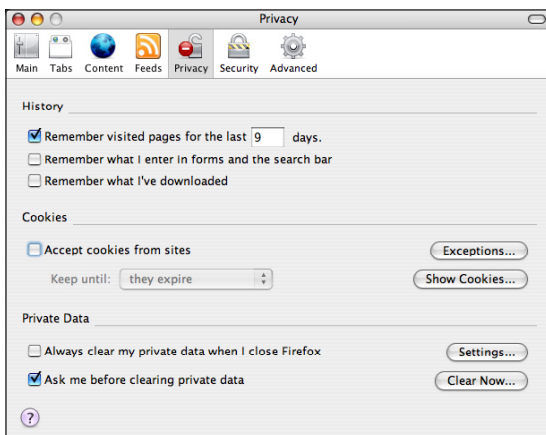
- Open the Firefox preferences screen
- Click on the 'privacy' tab
- Below 'Private Data', click 'Clear now'
- Select 'cookies,' and click 'Clear Private Data Now'

In addition users can reset their browsers to let them know when a cookie is being sent or even to refuse all cookies. This feature can be found in the 'advanced internet options' section of the 'tools' menu.



- Go to the 'tools' menu
- Select 'internet options'
- Select the 'privacy' tab
- Move slide to select a privacy setting or click 'advanced' to choose how cookies are handled

Firefox users can do the same through their privacy preferences.



- Open the Firefox preferences screen
- Click on the 'privacy' tab
- Uncheck 'accept cookies from sites'

Looking for more?

Google Privacy Center - – www.google.com/privacy

Google Privacy Channel on YouTube – www.youtube.com/GooglePrivacy

Google Public Policy blog – googlepublicpolicy.blogspot.com

Google™