AN ANALYSIS OF GOOGLE'S PRIVACY POLICY AND RELATED FAQs

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, MARCH 2012

AN ANALYSIS OF GOOGLE'S PRIVACY POLICY AND RELATED FAQs

MANAGEMENT SUMMARY

Google's new combined Privacy Policy (March 2012) has been widely criticised by privacy professionals and Data Protection Authorities (in particular the CNIL – the French Data Protection Authority). However the reasons for this criticism have been made in general terms; my analysis provides a detailed explanation.

The analysis shows that Google's Privacy Policy is incoherent because it uses overlapping terms. This makes the Policy difficult to follow and to understand what type of information the Policy is claiming to protect. It cannot be fair to users if they cannot understand what the Policy means for them. The Policy is also unfair in conventional terms as it does not, in many instances, fully describe the purposes of the processing.

Secondly, my analysis also confirms the claim of the CNIL that the Privacy Policy is in breach of the Data Protection Directive. However, I also show that it is in breach of the USA's Safe Harbor Principles. As the Privacy Policy states that "Google complies with the US-EU Safe Harbour Framework", I show that this claim **cannot be substantiated** if Google's new Privacy Policy is implemented.

Contradictory and confusing?

The Privacy Policy uses a wide range of similar terms in different circumstances which I think are contradictory. For example, it uses the following terms: "information", "personal information", "personal data", "data", "non-personally identifiable information", "personally identifiable information", "sensitive personal information", and "other information that identifies you". Are these terms talking about the same thing? We don't know.

So when one part of the Policy offers protection for "personal information", another offers protection for "personal data", another for "personally identifiable information" and yet another for "other information that identifies you" is the Policy referring to the same type of information or not? Answers on a post-card to Google.

This is not the only problem as sometimes the Policy uses a qualifier (e.g. "log information" or "location information"). "Log information" by the way are the "details of how **you** used our service, such as **your** search queries" whilst "location information" which is "information about **your** actual location". (My emphasis on **you** and **your**).

Can we have a quick quiz? Can you tell me whether "information" about **your use** or **your location** is "non-personally identifiable information" or "personal information"? My own view is that, because the Policy uses the word "information"

to describe logs and locations, that Google thinks it to be the former, but I suspect you think it could well be the latter.

Confused? You can now safely join the ranks of those who do not know what Google's Privacy Policy means in practice.

In breach of the Directive and Safe Harbor?

The CNIL has claimed that Google's Privacy Policy is in breach of the Directive, a claim so far not accepted by Google. As the Directive is the legislation mentioned in the Safe Harbor Framework, I have checked whether Google's Privacy Policy is consistent with the terms of the Framework.

There are demonstrable areas where Google's Privacy Policy is inconsistent with the Safe Harbor Principles (see Appendix 1 of the analysis); it follows that the Policy is inconsistent with the Directive. These areas include the following:

1. Safe Harbor requires acceptance of the EU Directive definition of "personal data" – Google's Privacy Policy uses a definition which is close to that used by the old UK's Data Protection Act 1984 (and ignores the Directive definition of personal data completely).

2. Safe Harbor requires acceptance of the EU Directive definition of sensitive personal data – Google's Privacy Policy does not include all items of sensitive personal data identified in the Directive.

3. Safe Harbor requires acceptance of the right of access to personal data – Google's Privacy Policy includes some administrative exemptions from the right of access to personal data that are not authorised by Safe Harbor.

4. The confusion in the Privacy Policy does not meet the Safe Harbor requirement for clarity; there are several places where the purposes of the processing are not fully described by the Policy.

5. Google's co-operation with data protection authorities specified in the Privacy Policy relates only to the transfer of personal data; Safe Harbor requires co-operation across the whole Framework.

Comment about the analysis

The analysis takes each paragraph of the text of the Privacy Policy as it is written and makes a comment if it is relevant. This means the reader can easily agree or disagree with the comment made.

Preview: Privacy Policy

This Privacy Policy will be effective from 1 March 2012 and will replace the existing Privacy Policy. Please see our overview page for additional details.

Last modified: 1 March 2012 (view archived versions)

There are many different ways for you to use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms, such as cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google, so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions, contact us.

Information that we collect

We collect information to provide better services to all of our users – from basics, such as which language you speak to more complex things, such as which ads you'll find most useful or the people who matter most to you online.

We collect information in two ways:

- **Information that you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, such as your name, email address, telephone number or credit card number. If you want to take full advantage of the sharing features that we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

- **Information that we get from your use of our services.** We may collect information about the services that you use and how you use them, such as when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:

Comment [U1]: The text refers to the sharing of "information". Does this mean sharing "personal information" or the sharing of information that is "not personal" or the sharing of "information" in general (i.e. sharing of information including "personal information"?)

As we shall see, the Policy uses a wide range of terms in different circumstances. These terms include: "information", "personal information", "personal data", "data", "non-personally identifiable information", "personally identifiable information", "sensitive personal information", "other information that identifies you" and "certain information" etc. This is not the complete list as sometimes there is a qualifier (e.g. "device information", "log data").

Any Privacy Policy needs a degree of precision; the use of a multitude of terms looses that precision. This, in summary, explains the press reports stating that privacy professionals are uncertain as to what the Privacy Policy actually means.

Comment [U2]: We are still unclear as to what kind of information the Policy is talking about.

However, it is reasonable to start from an assumption that the text means "any information" (i.e. personal information and other information).

Comment [U3]: Ditto – see U2

Comment [U4]: Here the Policy is using "personal information". So does this exclude the information that is not personal information?. Does this mean that the use of "information" by the Policy is now a reference to information that is "not personal information"?

If our starting assumption is correct, "information" means "**any** information" (e.g. includes personal information), so we do not need a definition of "personal information". So perhaps the starting assumption is wrong – "information" as used in the Policy excludes "personal information".

As we shall also see, "personal information" is defined in a FAQ (see **U47**); we discover the definition is **NOT** the European Directive definition.

Comment [U5]: Many will assume that the information about the services used by a specific individual would fall within the category of "personal information".

But the text uses the word "information" so one assumes that Google **may** think that this information is **NOT personal data**.

Comment [U6]: The use of "includes" means that the following list of items is incomplete. So should Google spell out the "other things" collected?

- **Device information**

  We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers and mobile network information, including phone number). Google may associate your device identifiers or phone number with your Google Account.

- **Log information**

  When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

  - details of how you used our service, such as your search queries.
  - telephony log information, such as your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
  - Internet protocol address.
  - device event information, such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
  - cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use a location-enabled Google service, we may collect and process information about your actual location, such as GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and mobile towers.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device, using mechanisms such as browser web storage (including HTML 5) and application data caches.

Comment [U7]: Is this information about a device specific or owned by, or unique to a particular individual, "personal information" or not?

If Google links "Your device to Your Account" I think the information is very likely to be "personal information" but the word used by the Policy is "information" on its own. So Google might think it is **not personal data.**

Comment [U8]: Is this log information about the use of Google services by a specific individual "personal information" or not? Google might think it is **not personal data**.

Note that the use of "This **may** include..." (highlighted in the leading paragraph) means that the description of the data collected in a log is incomplete.

Comment [U9]: Is this location information referring to the location of a specific individual "personal information" or not? Google might think location information is **not personal data**.

Comment [U10]: Are the "application numbers" information about the software used by a specific individual "personal information" or not? Google might think it is **not personal data**.

Comment [U11]: Note here the text uses "information (including personal information)".

This implies that the use of mere "information" in the Policy excludes "personal information" (because it has to be mentioned explicitly!).

This use of "personal information" reinforces the confusion! Does "information" include "personal information" or exclude "personal information". If it is the latter, the Policy should explain why, for example, "**your** actual location" information is not personal data.

I am not going to labour this point again; in subsequent comments, I reference U11.

- **Cookies and anonymous identifiers**

  We use various technologies to collect and store information when you visit a Google service, which may include one or more cookies or anonymous identifiers sent to your device. We also use cookies and anonymous identifiers when you interact with services that we offer to our partners, such as advertising services or Google features that may appear on other sites.

How we use information that we collect

We use the information that we collect from all of our services to provide, maintain, protect and improve them, to develop new ones and to protect Google and our users. We also use this information to offer you tailored content – such as giving you more relevant search results and ads.

We may use the name that you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account, so that you are represented consistently across all our services. If other users already have your email or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

When you contact Google, we may keep a record of your communication to help resolve any issues that you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to provide you our services in your preferred language. When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

We may combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

We will ask for your consent before using information for a purpose other than those set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and control certain types of information tied to your Google Account by using Google Dashboard.

Comment [U12]: Lets take some extreme possibilities here.

Let us suppose you have changed your name for security reasons; Google could link names that you have used but no longer wish to be linked to.

Let us suppose you want to exclude someone for whatever reason; if that person has your email address, Google may provide updated information to them.

These actions, as we shall see, might occur in the **absence** of consent (see U17/U18)

Comment [U13]: Confused use of information again – see U11. Is "Other information that identifies you" the same as "personal information" as defined?

Comment [U14]: Does not say how long the record is kept, but will use the email address for a form of "marketing" (without an opt-out being offered). The use of "such as" means the list of uses of the email is incomplete.

Comment [U15]: Infers that this association **may** be made with non sensitive categories.

Comment [U16]: Now the text uses "personally identifiable information" but not "personal information". See U11

Comment [U17]: There is no definition of consent? Does Google mean "implied consent"? Who knows? If it does, then it falls short of European Data Protection Directive's definition of "consent".

Comment [U18]: This implies that consent is **NOT NEEDED FOR THE PURPOSES IN THIS POLICY –** in particular all of the purposes identified in this **"How we use information that we collect"** section of the Policy**.**

In terms of legitimising the processing of personal data as required by the First Data Protection Principle (or Article 7 of the Directive), Google can't rely on "consent".

I also suspect that much of the processing cannot be legitimised in terms of "necessary for a contract with the data subject" (in case it is argued that there is some kind of contract" with users).

If the justification for the processing resides with the balance of interests in Schedule 6, para 2 it engages the right to object to the processing (which does not appear to be part of this privacy policy – even though the Policy refers to "rights" – see U36/U37).

Comment [U19]: From the European DP perspective, there is no mention of whether or not there has been an assessment of adequacy. A surprising omission.

- View and edit your ad preferences, such as which categories might interest you, using the Ad Preferences Manager. You can also opt out of certain Google advertising services here.
- Use our editor to see and adjust how your Google Profile appears to particular individuals.
- Control who you share information with.
- Take information out of many of our services.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

Information that you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options for sharing and removing your content.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others or would be extremely impractical (for instance, requests concerning information residing on backup tapes).

Where we can provide information access and correction, we will do so free of charge, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information that we share

We do not share personal information with companies, organisations and individuals outside Google unless one of the following circumstances applies:

Comment [U20]: Note the use of "many". Means that **NOT** all services are covered by the "take out" provision.

Comment [U21]: Just a side comment: when you share information publicly it is **NO LONGER PRIVATE.** Many USA companies will assume there is no privacy rules associated with such personal data See http://amberhawk.typepad.com/amberhawk/2010/11/north-americas-generally-accepted-privacy-principles-establish-an-inadequate-data-protection-regime.html)

Comment [U22]: It is not clear whether Accessing means "on-line access" or "subject access" in DP terms. Some paragraphs look like the latter, so I am assuming access includes "subject access" under a DP regime.

Comment [U23]: These business or legal purposes for keeping **uncorrected** personal data are not defined fully here – one assumes Google knows them (e.g. crime, libel). What is the purpose of keeping **out of date** personal data?

Comment [U24]: Apart from "unreasonably repetitive" exclusion from the right of access, the right of access to personal data in UK's Data Protection Act is not restricted by administrative conditions chosen by the data controller.

In addition, there is no need to make the statement "we do not obtain personal data from "back up" tapes" as the tapes are just "back-up" for accessible online personal data. However, if the "back-up" tapes are archive tapes, then DP law does not exempt access. The Policy is unclear here.

In the DP law one can protect the identity of another individual in certain circumstances; here there is a general exemption from the right of access which is linked to "risk the privacy of others".

There is no exemption from the right of access in the DPA which linked to "disproportionate" effort to provide access to personal data

The right of access to personal data is not enshrined properly in the Policy, and the Policy is inconsistent with the Safe Harbor rules (see U55).

Comment [U25]: The policy does not say what "disproportionate" means or what happens if the "disproportionate" threshold is reached. Is there a "fee" for access (i.e. it is no longer free) or is the request rejected?

In the UK, the max fee is £10 and claiming "disproportionate effort" to provide the data subject with the personal data is not a valid reason for not providing access to personal data.

- **With your consent**

  We will share personal information with companies, organisations or individuals outside Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organisation will have access to your Google Account information (including your emails and other data). Your domain administrator may be able to:

  - view statistics regarding your account, such as statistics regarding applications that you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy any applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

  We will share personal information with companies, organisations or individuals outside Google if we have a belief in good faith that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation, legal process or enforceable governmental request.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of Google, our users or the public, as required or permitted by law.

We may share aggregated, non-personally identifiable information publicly and with our partners, such as publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

Comment [U26]: This implies OPT-OUT consent or possibly implied consent may be used otherwise. There is no definition of what "consent" is.

If implied consent is used (e.g. where consent does not include any indication of the data subject's wishes), then "consent" is not the European standard of "consent".

In other words, providing a notice to the data subject is **NOT** consent; in European DP law, the data subject has to do something to signify agreement.

Comment [U27]: The word "necessary" is often used in the DPA; it is **never** qualified to read "reasonably necessary".

One assumes, given the comments about rights of access (see U24) that "reasonably necessary" mean what Google thinks is reasonably necessary? If so, this is not the proper legal test to use in connection with disclosure. One is either obliged to disclose or volunteering a disclosure; the Policy could say "we only disclose if we are legally obliged to do so except for ..... (list of disclosures)"

In the UK there is a statutory code of practice covering these disclosures.

Comment [U28]: Google could identify examples of important laws, regulations that apply here etc

Comment [U29]: Similarly "Permitted by law" – what laws? Includes voluntary disclosures. See comment above and U27

Comment [U30]: We now have the use of "non-personally identifiable information" – isn't this mere "information"? See U11

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Google and our users from unauthorised access to or unauthorised alteration, disclosure or destruction of information that we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two-step verification when you access your Google Account and a Safe Browsing feature in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorised access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us and who are subject to strict contractual confidentiality obligations. They may be disciplined or their contract terminated if they fail to meet these obligations.

Application

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services), but excludes services with separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organisations that advertise our services and that may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Enforcement

We regularly review our compliance with our Privacy Policy. We also adhere to several self-regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Comment [U31]: Note that Google, like many USA orgs, assume that if you have provided a notice, then it's OK to process. It overlooks the right to object to the processing which can apply in DP law.

Comment [U32]: This contradicts the Policy statement that requirement that "We will ask for your consent before using information for a purpose other than those set out in this Privacy Policy" – see U18

Comment [U33]: The Data Protection Directive requires "recovery from accidental loss and destruction" and reporting data losses – this aspect is missing from the Policy.

Comment [U34]: Because this only applies to "personal information", it infers there is no such restriction on accessing mere "information".

Comment [U35]: Now we have "personal data". Is this different to "personal information?".

I think the single use of the correct DP terminology could be deliberate here. It means that Google will only co-operate with Data Protection Authorities if the personal information is personal data. It appears to be a commitment to restrict co-operation with Europe's data protection authorities to the minimum legal requirements.

This provision also states that they will only co-operate with data protection authorities with respect to **the transfer of personal data**.

Comment [U36]: There are **no rights** identified in the Privacy Policy**!** This is the only place where the word "**rights**" in the context of an individual is used. There is a reference to Google's rights, however.

Comment [U37]:

Technically, one could argue that as there are no rights granted by the Privacy Policy, then Google can change the Privacy Policy without consent.

Comment [U38]: Again this Notice point. Google say if they tell you prominently, it is by notice and **not consent**.

This also appears to contradict the reassurance offered in U18 ("We will ask for your consent before using information for a purpose other than those set out in this Privacy Policy")

Preview: Privacy FAQ

This Privacy Policy will be effective from 1 March 2012 and will replace the existing Privacy Policy. Please see our overview page for additional details.

1. How does Google protect my privacy?
2. Why does Google store search engine log data?
3. Why are search engine logs kept before being anonymised?
4. How can I remove information about myself from Google's search results?
5. Does Google use cookies?
6. What happens when different privacy laws in different countries conflict?
7. How often are you asked by governments to provide data on users?
8. How can I contact Google if I have a privacy question or complaint?
9. Key terms
    1. Personal information
    2. Google Account
    3. Cookie
    4. Anonymous identifier
    5. IP address
    6. Server logs
    7. Sensitive personal information
    8. Non-personally identifiable information
    9. Pixel tag

How does Google protect my privacy?

At Google, we are keenly aware of the trust that our users place in us and our responsibility to protect their privacy. We believe that transparency and choice are the foundations of privacy. To help you make informed decisions about your own privacy, we work to let you know what information we collect when you use our products and services, and how we use that information to improve your service. We also work to give you meaningful choices, when possible, about the information that you provide to Google and to others. We encourage you to watch our videos, read our Privacy Policy and consult our Help Centres to find out more about privacy at Google.

Why does Google store search engine log data?

Comment [U39]: Now the further explanation of the Privacy Policy uses "data" instead of "information" – see U11

We store this data for a number of reasons. Most importantly, we store data to improve our search results and to maintain the security of our systems. Analysing logs data helps our engineers both improve your search quality and build helpful innovative services. Take the example of Google Spell Checker. Google's spell-checking software automatically looks at a user's query and checks to see if that user is using the most common version of the word's spelling. If we calculate that a user is likely to get more relevant search results with an alternative spelling, we'll ask "Did you mean: (more common spelling)?" In order to provide this service, we study the data in our logs. Log data also helps us improve our search results. If we know that users are clicking the #1 result, we know that we're probably doing something right and if they're hitting next page or reformulating their query, we're probably

doing something wrong. In addition, log data helps us prevent fraud and other abuse, such as phishing, scripting attacks and spam, including query-click spam and ad-click spam.

Why are search engine logs kept before being anonymised?

We strike a reasonable balance between the competing pressures that we face, such as the privacy of our users, the security of our systems and the need for innovation. We believe that anonymising IP addresses after 9 months and cookies in our search engine logs after 18 months strikes the right balance.

How can I remove information about myself from Google's search results?

Like all search engines, Google is a reflection of the content and information publicly available on the web. Search engines do not have the ability to remove content directly from the web, so removing search results from Google or another search engine leaves the underlying content unaffected. If you want to remove something from the web, you should contact the webmaster of the site and ask him or her to make a change. Once the content has been removed and Google's search engine crawl has visited the page again, the information will no longer appear in Google's search results. If you have an urgent removal request, you can also visit our Help page for more information.

Does Google use cookies?

Yes, like most websites and search engines, Google uses cookies to improve your experience and to provide services and advertising. Cookies help us keep a record of your preferences, such as whether you want your search results in English or French, or if you use our SafeSearch filter. Without cookies, Google wouldn't be able to remember what different people like. We also use cookies to provide advertising that's more relevant to your interests.

We've been told that most users don't want to reset their computers every time they log on. If you don't want to receive cookies, you can change your browsers to notify you when cookies are sent and then refuse cookies from certain websites (or altogether). You can also delete cookies from your browser. Google's search engine does work without cookies, but you will lose some functionality if you choose to disable cookies.

What happens when different privacy laws in different countries conflict?

Many countries approach privacy issues differently and there is no consistent global standard on which all countries agree. Google's Privacy Policy is designed to be a single, clear, global statement of our approach to privacy, and our privacy practices under it are designed to meet applicable law around the world.

Comment [U40]: Implies the logs are personal data prior to anonymisation. But according to the Policy, logs only contain "information" – see U8 (and then U11!)

Comment [U41]: The use of "such as" here means that the list of purposes is incomplete. Fair processing requirements mean that all purposes of retention should be identified.

Comment [U42]: The purposes identified in the FAQs do not justify this retention period. If Google were interested in security and privacy of users, it could achieve both by having a very short retention criteria before anonymising.

Re innovation – normally it enhances security not to use live personal data at the out-set!

Some purposes of retention (e.g. the law enforcement element) have been omitted.

Fair processing requirements in DP law cover ALL the purpose of retention – not some of them.

Comment [U43]: There is a trend to equate "privacy" with "data protection" probably because many USA organisations like Google like to use the "p-word" quite a lot and there is a common desire to be "privacy friendly".

However, when you make this equation, it can be at the expense of ignoring many important data protection safeguards.

See http://amberhawk.typepad.com/amberhawk/2010/11/north-americas-generally-accepted-privacy-principles-establish-an-inadequate-data-protection-regime.html

Comment [U44]: My translation of this section is as follows. Google are not going to bother with the detailed requirements such as those found in the European Data Protection Law or other national laws. Instead Google's own chosen data protection procedures will be applied.

Google will use its own definition of "personal information", "consent" and what is in a Notice. Google will decide what to put in its Privacy Policy about that standard.

Google are so big that any data protection authority might not have the resources to challenge them. It could be "put up" or "shut up" time for data protection authorities perhaps – or possible wait till the fines in the Regulation are in place!

How often are you asked by governments to provide data on users?

Like other technology and communications companies, we receive requests from government agencies around the world to provide information about users of our services and products. To help increase transparency about these requests, we have created the Government Requests Tool, which shows the number of requests that we have received that relate primarily to criminal investigations. For more information about the tool and the nature of these requests, please check the Government Requests Tool FAQ.

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

You can contact us at any time through our privacy contact form. If you prefer, you can also write to:

Privacy Matters;
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

Key terms

Personal information

This is information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google.

> The relevant part of the UK definition of "personal data", for comparison, is as follows:
>
> **personal data**" means data which relate to a living individual who can be identified- (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller" .....

Note: I have chosen the UK definition as comparison as it is one of the weaker ones in Europe. (see http://amberhawk.typepad.com/amberhawk/2011/05/privacy-new-government-revelations-amplify-concerns-surrounding-deficiencies-in-uks-data-protection-.html - where following *Durant*, the European Commission state that the UK definition of personal data is not the definition found in the Directive).

Comment [U45]: Either I am making a mistake or there is something wrong with the statistics Google is publishing re UK "Government Requests" for user data.

In the last period (Jan-June 2011) where stats have been published by Google, Google reports that there has been "1,279 User Data Requests" from Government relating to requests for disclosure of user data from Google accounts or services" and 63% of them had been approved.

The latest Annual Report of the Interception of Communications Commisioner reports that there were more than 552,550 requests for Communications data, of which very few can be refused under RIPA. This includes User account data. So do Google only get 0.2% of all RIPA requests and refuse one third of them? I wonder whether this is correct?

Comment [U46]: I have added the relevant part of the UK Act's definition of personal information for convenience.

Comment [U47]: To be close to UK data protection law, the words "reasonably linked" have to be removed.

Assuming Google is the data controller, the UK's DP Act definition of "personal data" asks whether identification of an individual can occur from the data (or from the data plus other information in the possession of Google). There is no "**reasonably**" identified criteria

There is **no** requirement for a "**linkage**" (unlike the Google definition); just that the identifying information is in the possession of Google or likely to come into the possession of Google.

Google by contrast states that the data has either to contain the identity of the individual or the data can be reasonably linked to the identity of an individual. (As an aside, this definition of personal data would just meet the standard of the UK's old Data Protection Act 1984 definition – that is how old Google's thinking is)

The conclusion I have reached is that when the Privacy Policy uses the word "information" then some of this "information" is likely to be "personal data" whereas Google thinks it is not "personal data", using its own definition.

This position is storing up trouble.

Google Account

You may access some of our services by signing up for a Google Account and providing us with some personal information (typically, your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorised access by others. You can edit or terminate your account at any time through your Google Account settings.

Cookie

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognise your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies.

Anonymous identifier

An anonymous identifier is a random string of characters that is used for the same purposes as a cookie on platforms, including certain mobile devices, where cookie technology is not available.

IP address

Every computer connected to the Internet is assigned a unique number known as an Internet protocol (IP) address. Since these numbers are usually assigned in country-based blocks, an IP address can often be used to identify the country from which a computer is connecting to the Internet.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time that they connect to the Internet;
- `25/Mar/2003 10:15:32` is the date and time of the query;

- http://www.google.co.uk/search?q=cars is the URL requested, including the search query;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used; and
- 740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time that it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time that s/he visits Google from that particular computer.)

Sensitive personal information

This is a particular category of personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually identifiable user.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking activity on websites, or when emails are opened or accessed, and is often used in combination with cookies.

Preview: Self-Regulatory Frameworks

This Privacy Policy will be effective from 1 March 2012 and will replace the existing Privacy Policy. Please see our overview page for additional details.

Last modified: 1 March 2012

Google complies with the US-EU Safe Harbour Framework and the US-Swiss Safe Harbour Framework, as set forth by the US Department of Commerce, regarding the collection, use and retention of personal information from European Union member countries and Switzerland. Google has certified that it adheres to the Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. To learn more about the Safe Harbour programme and to view Google's certification, please visit the Safe Harbour website.

Google is a member of the Network Advertising Initiative (NAI), a cooperative of companies committed to building responsible advertising policies across the Internet. Using a tool created by the NAI, you can learn more about other ad-serving companies and opt out from their use of cookies at the NAI website.

Google also adheres to the UK Internet Advertising Bureau Good Practice Principles for Online Behavioural Advertising, the Australian Best Practice Guideline for Online Behavioural Advertising and IAB Europe's European Framework for Online Behavioural Advertising.

Comment [U48]: This is **not** the list of sensitive personal data as identified in the Directive (e.g. crime, trades unions are missing; "confidential medical facts" is far more restrictive that data about an individual's physical health, mental health or condition).

The text implies that medical facts that are not confidential are not sensitive personal data.

Comment [U49]: Note that in terms of the Directive, some **Non-personally identifiable information** will be in fact "personal data" under European DP law – see U47.

Google in effect has determined for itself what personal information means and therefore what is not personal information.

Such a position, if it continues to ignore legal definitions of personal data, will result in an inevitable clash.

Comment [U50]: Google's claims to conformity with Safe Harbor Framework, is inconsistent with its Privacy Policy. There are several reasons for this. They are:

1.Safe Harbor requires acceptance of the EU Directive definition of personal data – Google's Privacy Police does not.

2.Safe Harbor requires acceptance of the EU Directive definition of sensitive personal data – Google's Privacy Police does not.

3.Safe Harbor requires acceptance of the right of access to personal data – Google's Privacy Police does not.

4.The confusion in the Privacy Policy and the non-declaration of processing purposes does not meet the Safe Harbor requirement for clarity (e.g. of Notice).

5.Google's co-operation with data protection authorities specified in the Privacy Policy relates only to the transfers of personal data.

The references of the above 5 issues follow on below, in the text of the Safe Harbor provisions.

APPENDIX 1: The Safe Harbor Principles

From: http://export.gov/safeharbor/eu/eg_main_018475.asp

SAFE HARBOR PRIVACY PRINCIPLES

ISSUED BY THE U.S. DEPARTMENT OF COMMERCE ON JULY 21, 2000

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self- regulatory privacy policies provided that they conform with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self- regulation, its failure to comply with such self- regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. *(See the annex for the list of U.S. statutory bodies recognized by the EU.)* In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbor benefits. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification**.**

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these Principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the safe harbor. An organization that wishes to extend safe harbor benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self-Certification. Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense

Comment [U51]: Google's co-operation, according to the Policy, is only in relation to transfer of personal data – see U35

Comment [U52]: My emphasis to show that Google's Privacy Policy - see U47 does not use the Directive definition of personal data

Comment [U53]: The Privacy Policy is so confused – it cannot meet these "clear and conspicuous" requirements.

The Policy also does not specify all the purposes of the processing – see U6, U8, U14, U20, U23, U28, U29 and U41

Comment [U54]: My emphasis to show that the Safe Harbor definition of sensitive information is inconsistent with the definition of Sensitive Personal Information in the Policy – see U48

For some reason, criminal personal data seems to be missing from Safe Harbor – it is also missing from Google's list.

Comment [U55]: The access provision is inconsistent with Google's Privacy Policy in relation to Safe Harbor requirements – see U24, U25 (for example, administrative exemptions from the right of access are excluded by Google's Policy, but are not exempted here)

Also Safe Harbor states that any disproportionality from the right of access has to be linked to the risks to an individual's privacy or another's privacy.

Google's policy just requires disproportionality in terms of the effort expended to facilitate access to personal data. The link to "risk" has gone.

of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

1. It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

ADVERT

COURSES FOR INFORMATION LAW OFFICERS, PRIVACY PRACTITIONERS OR DATA PROTECTION OFFICERS

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection which can be held on-site.

With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, CCTV, human resources, data sharing, direct marketing) or targeted at specific staff members (e.g. managers) or on specialist aspects (e.g. social work functions, anti-fraud functions).

We have day long public courses in Data Protection Audit, Privacy Impact Assessments and RIPA courses.

We hope to offer the ISEB syllabus into Information Security Management soon; if interested email info@amberhawk.com

COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification.

With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.

If interested please contact us at ***info@amberhawk.com***