PRIVACY ISSUES OF THE INTERNET SEARCH ENGINES - IN THE LIGHT OF EU DATA PROTECTION LEGISLATION

by

ZSUZSANNA BÓDOGH*

Nowadays we use the internet as our main source of information and the search engines such as the Google to lead us through the labyrinth of websites in order to find the certain piece of information we are looking for. And because we can find almost everything we want and because asking a computer - believing that we remain unidentifiable - is sometimes easier than asking a real person, we venture into this labyrinth more and more bravely and deeply. Our search queries, which are systematically logged and stored by the search engines, show the wide range of our interests, intentions, desires often kept secret even from the closest friends and relatives.

If the data stored by the search engines operators about the searches conducted by us made us identifiable, the pieces of our search history would be considered to be personal data, even sensitive personal data and should be treated as such.

But is that really the case? And if so, what do the search engine operators do to save our privacy?

The paper introduces the types of data processed and the privacy problems caused by the internet search engines and the lawfulness of their data processing activities in the light of the EU Data Protection Directive.

KEYWORDS

Search engine, Internet, data protection, privacy, Google

* zsuzsanna.bodogh@gmail.com

1. INTRODUCTION

Millions of people around the world use internet search engines such as Google every day to find information and contents they're interested in on the internet. Their development was closely linked to the growth of the internet, because without proper information locations tools it would be impossible to exploit its potential as information highway. Being able to find almost every kind of data and multimedia content on the internet, most people search not only for 'serious' types of information, useful in their work, studies, everyday life, but also for entertainment and other kinds of things they would never confess even to their closest friends and relatives that they're interested in, things which may reflect their medical condition, religious beliefs, political views, sexual orientation and sometimes their criminal intent. People are so brave at sharing their thoughts with the search engines not just because they are almost sure they will find answers to every question, but also because they think that every word typed in remains between them and the machine. The use of internet search engines does not require registration, authentication, so they believe that they can remain faceless, anonymous, no one will ever be able to connect their search queries with them.

If this really is the case, what kind of privacy threat do the internet search engines pose to their users? Why the privacy/data protection issues of the internet search engines should be dealt with?

2. TYPES OF USER DATA PROCESSED BY THE SEARCH ENGINE PROVIDERS

For the purpose of answering these questions, the types of data collected and stored in connection with the searches must be examined first. The servers of the internet search engines like that of every web service automatically and systematically log every event, every page request. The search log contains data such as the Internet Protocol (IP) address of the user's device, the type and the language of the browser used, the date and time of the request, the ID of the cookie set in the user's browser and the search query itself.

The IP (Internet Protocol) address[1] is a number that uniquely identifies a device (computer, mobile phone etc.) participating in a computer network

[1] Source: <http://computer.howstuffworks.com/internet/basics/question549.htm>

using Internet Protocol for communication. The IP address of a device connected to the internet is assigned by the internet service provider (ISP) either permanently (static IP address) or periodically (dynamic IP address). Knowing the IP address, the search engine providers are able to determine the ISP and the approximate geographical location of the device used, but they are not able to identify the person who conducted the search. This position can be compared to that of someone who knows another man's home address (city, street, house number), but in the absence of a city map is not able to find the place where his house is actually located. In case of IP addresses, the user's ISP alone has got this 'map' and is able to single out, knowing the IP address and the date and time of the request, the internet subscriber from whom the request came. But just as there can be more than one people living in the same house, there can be more than one computer and other device – more than one user – connected to the internet on the same IP address. It is, therefore, very unlikely, but not impossible to uniquely identify the user by combining the data processed by the search engine provider and the data processed by the ISP. Because of the widespread use of dynamic IP addresses, their capability to link together the search requests, web page requests coming from the same people is also very limited. Since the search engine providers just as many other web service providers need this capability e.g. in order to store user settings and preferences, improve their services by analyzing user behaviour, they also use HTTP cookies.

A HTTP cookie[2] is a small data file set on the user's computer by a web server the first time the user visits a web page. On the next page visit in the same domain, the web browser sends the cookie data back to the server, identifying its user thereby as a returning visitor. Without the use of cookies, each web page request would be independent of all others, which would render web services such as webmails and webshops inoperative.

Some cookies expire at the end of each session (i.e. when the user shuts down the browser), but the so called persistent cookies remain on the hard drive until their expiration date has passed.

In many cases, there are parts on a web page, such as advertisements, that belong to a different domain and they are also able to set cookies, so-called third-party cookies, on the hard drive of the user's computer. Using

[2] Sources: <http://www.pcmag.com/encyclopedia_term/0,2542,t=cookie&i=40334,00.asp> <http://computer.howstuffworks.com/cookie.htm>

them, the advertisers are able to track user's movement across multiple websites that contain their advertisements, which helps them to build up user profiles based on web surfing habits.

The cookies actually identify the user's web browser and not the user himself. Combining with the IP address, the identifier of the cookie set by the search engine can link different search requests to a certain computer, but in some cases it is impossible to tell who was sitting behind it when the requests were made.

The search engines store also the search queries made, along with the IP address and the cookie identifier. In cases where the IP address and cookie data allow user identification, the identified person can be associated with his/her search queries, which could pose a real threat to his/her privacy. In addition to that, the combination of the queries could be so unique in certain cases, which makes the identification possible, e.g. in cases when a user conducted 'ego searches' and besides searched for other specific things attributable only to a restricted group of people.

3. PRIVACY ISSUES RAISED BY INTERNET SEARCH ENGINES

The data processed by the search engine providers for the reasons explained above do not in themselves allow the identification of their users, which brings up the question whether people have serious reason to worry about privacy when using internet search engines.

In relation to this question, we should take account of the fact that most of the companies specialized in search services are engaged in other kinds of activity as well. Since most of the people are not willing to pay for search services, the search engine providers had to find other sources of revenue they need in order to sustain and improve their services and gain profit. For this reason, they sell advertising space and provide sponsored links on the result page. Because of the widespread pay-per-click billing method of advertising, which means that the advertiser pays the host only when its ad is clicked on, they must provide the advertisers with the tools necessary to make their advertisements more effective to attract them. The combination of data collected by the advertising companies with the use of third party cookies about the user's site visits, surfing habits and the search queries collected and processed by the search engine providers allows for building up user profiles which are used to select ads according to the user's interest.

Google also runs a service called AdSense[3] which makes possible for the website owners to make revenue by letting Google place ads on their websites. From the user's point of view it means that his/her movement became traceable on a wider section of the internet. The Google's Ads Preferences Manager[4] service enables the users to check which customer interest categories they are put into based on their website visits, and they are also able to opt out of this categorization, but many users do not have knowledge of this possibility. In addition to that, in order to opt out permanently a specific plugin[5] must be installed, which makes the cookie management to some inexperienced users complicated.

In order to attract more users and to make more advertising revenue thereby, some search engine providers also run other services such as webmail. Some of these services require registration to use and many people register with their full name and other identifiers. Many users are unaware of the fact that these identifiers given to the search engine providers voluntarily can easily be correlated with their search queries conducted while they were logged into their e.g. email account. In case of Google, the Google Dashboard service[6] enables the users to check and manage the data stored in connection with them, but just like in the case of the Ads Preferences Manager, this possibility is not in the spotlight. Besides, deleting the data using the Dashboard service does not necessarily mean that they have disappeared also from the servers of the service provider, not to mention the backup tapes.[7]

The attention of the wider public was drawn for the first time to the possible threats to the users' privacy in 1999, when Amazon.com, Inc., the world's biggest online book retailer bought Alexa Internet, Inc., a company offering a toolbar which, among other features, gives suggestions on where to go next on the internet based on its users' site visits. The merger made possible the correlation and thereby the abuse of customer data by bringing together the internet surfing habits obtained by Alexa Internet and the personally identifiable data stored by the Amazon.com. Some customers filed lawsuits[8] against Alexa Internet and Amazon in 2000, accusing the Alexa Internet of sending confidential information about them to Amazon without

[3] Further see: <https://www.google.com/adsense/static/hu/Publishertools.html>
[4] Further see: <http://www.google.com/ads/preferences>
[5] Further see: <http://www.google.com/ads/preferences/plugin/>
[6] Further see: <https://www.google.com/dashboard/>
[7] Further see: <http://www.google.com/privacy/privacy-policy.html>

their consent. The lawsuits ended with a settlement[9] in which the defendant agreed to delete four digits of the IP addresses in its databases, add privacy policy information to its Web site, require customers to opt-in to having their data collected before they are permitted to download Alexa software, and pay up to $40 to each customer whose data was found in Alexa's database. Because of the settlement, the courts were not in the position to examine thoroughly whether there was any abuse of customer data actually.

The search engine providers, their subsidiaries and partners collect many data about their users for advertising purposes. They use these data to categorize users according to their interests, trying to find out what kind of products would they buy, what kind of services they are willing to pay for, in order to make the advertisements more effective. For that reason, they want to know that a certain user is e.g. a middle-aged, he works as a doctor and lives in small town etc., but for advertising purposes is not strictly necessary for them to know who the users as named persons really are – though they are not unhappy if they are able to find it out. There are, however, others, to whom the large amount of data processed by the search engine providers seems very attractive and useful for their not always innocent purposes.

In 2006, Alberto R. Gonzalez, Attorney General of the USA, acting on behalf of the Department of Justice served a subpoena against Google, Yahoo, Microsoft and America Online[10], demanding to hand over all the URLs in their indexes and all the search queries that had been entered in a period of two months. The Department of Justice wanted to use these data in a court case in which they tried to defend the Child Online Protection Act by proving how easy to stumble upon pornographic material on the internet.[11] Only the Google refused to comply with the subpoena, mentioning its trade secrets, the undue burden the fulfilment of the request would impose on the company and the privacy of its users. The court ordered the Google to hand over 50,000 random URLs, but denied the motion concerning the disclosure

---

[8] Source: Privacy: Key Cases, at <http://ilt.eff.org/index.php/Privacy:_Key_Cases> accessed on 20 November 2010

[9] Source: Settlement Agreement, at <http://pages.alexa.com/settlement/settle.html> accessed on 11 March 2009. Note: The file has been removed since then.

[10] Source: <www.google.com/press/images/subpoena_20060317.pdf>, accessed on 8 March 2009.

[11] Declan McCullagh, Elinor Mills, '*Feds take porn fight to Google*', at <http://news.cnet.com/Feds-take-porn-fight-to-Google/2100-1030_3-6028701.html?tag=mncol>, CNET News, January 19, 2006, accessed on 22 November 2010.

of search queries[12]. This case[13] showed clearly that the state authorities are aware of the amount of data processed by the search engine providers. Three out of the four subpoenaed companies did not even try to reject the claim, although it was made openly in a court case, which could have caused a reputation loss among their customers. The large amount and type of data processed could encourage civil litigants and others to try to get hold of these data by legal process or otherwise.

Collecting and storing large amount of data holds also the possibility of an accidental disclosure, just like it happened to AOL in 2006, which case was mentioned in the media as the AOL 'Data Valdez'[14]. Some researchers of AOL released for research purposes a file containing the search queries for over 650,000 users over a period of 3 months. The AOL removed the file from the internet as soon as it realized the problem, but by then it had been downloaded by many and it is still available on mirror sites today. The AOL usernames in that file had been changed to random ID numbers, but since these numbers could also be used to link the different search queries together, many people analyzed these data for fun, trying to identify the real person to whom they belonged. In August 2006, some journalists of New York Times succeeded in identifying the user No. 4417749 as a 62-year-old widow who lives Georgia, named Thelma Arnold[15]. Surprisingly, she did not even conducted an ego search, i.e. she did not search for her own name, which could make the identification easier. She searched for other specific things like several people with the last name Arnold, homes sold in her neighbourhood and '60 single men', which lead to the identification. This case showed that even when the IP address and the account data are anonymised, it is still possible to identify someone just by analyzing the

---

[12] Further see: <www.google.com/press/images/ruling_20060317.pdf>

[13] Sources: Nicole Wong, '*Judge tells DoJ "No" on search queries*', at <http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html>, The Official Google Blog, March 17, 2006, accessed on 22 November 2010.
Danny Sullivan, '*Bush Administration Demands Search Records*', at <http://blog.searchenginewatch.com/060119-060352>, January 19, 2006, accessed on 22 November 2010.
Declan McCullag, '*FAQ: What does the Google subpoena mean?*' at <http://news.cnet.com/FAQ-What-does-the-Google-subpoena-mean/2100-1029_3-6029042.html?tag=mncol;txt>, CNET News January 20, 2006, accessed on 22 November.

[14] The incidents like that are called 'data valdez' after the famous accident of the oil tanker Exxon Valdez, see further:
<http://www.doubletongued.org/index.php/dictionary/data_valdez/>

[15] Source: Michael Barbaro, Tom Zeller Jr., '*A Face Is Exposed for AOL Searcher No. 4417749*', at <http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1>, The New York Times, August 9, 2006, accessed on 11 March 2009

unique combination of his/her search terms. The case of Thelma Arnold also showed that the conclusion drawn from the search data could be misleading: e.g. she searched for some medical ailments, but she was not the one who suffered from them, she just wanted to help some friends of hers.

4. THE LAWFULNESS OF THE DATA PROCESSING ACTIVITIES OF THE SEARCH ENGINE PROVIDERS – IN THE LIGHT OF THE EU LEGISLATION

These cases drew the attention of the privacy experts to the privacy issues of the internet search engines. It became obvious, that the lawfulness of the data processing of the search engine providers and the legal instruments available to restrict their activities in order to avoid privacy harms needed a thorough examination. In the European Union where the data protection legislation addresses the privacy issues, it had to be examined whether the search engine providers process personal data, whether they are under the jurisdiction of one or more EU Members States, and if it's so, whether their data processing activities are in accordance with the provisions of the EU Data Protection Directive[16].

In 2007, the EU Article 29 Working Party[17] sent a questionnaire to several search engine providers across Member States as well as to several US-based companies. The questionnaire was aimed at revealing what kind of information they store and for how long, for which purposes and on what legal basis they justify the storage of these data. In April, 2008, the Working Party published its opinion 1/2008 on data protection issues related to search engines[18] which partially relied on the analysis of the replies to the questionnaire. In its opinion, the Working Party concluded the following.

The Working Party stated that when a cookie contains a unique user ID, this ID is clearly a personal data. Concerning the IP addresses, it cited from its former opinion WP 136[19] that *"unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that*

---

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter referred to as the Data Protection Directive

[17] The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC. Hereinafter referred to as Working Party

[18] Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, adopted on 4April , available at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm>

cannot be identified, it will have to treat all IP information as personal data, to be on the safe side", stating that these considerations will apply equally to search engine operators.

The search engine providers which process user data including IP addresses and/or cookies with a unique ID, fall within the material scope of the definition of the data controller, since they effectively determine the purposes and means of the processing of these personal data.

Based on Article 4 of the Data Protection Directive, the Working Party came to a conclusion that the Data Protection Directive generally applies to the processing of personal data by search engines, even when the headquarters of the search engine companies are outside the EEA, provided that they have an establishment here which plays a relevant role in the processing operation, e.g. it is responsible for relations with users or involved in the selling of targeted advertisements on the territory of a Member State or they use equipment such as data centres or users' computers storing cookies[20] on the territory of a Member State.

The Working Party analyzed the grounds and purposes of data processing mentioned in the replies to the questionnaire, taking into account the provisions Article 6 and Article 7 of the Data Protection Directive. It stated that there are three grounds which search engine providers may appeal to for different purposes:

The consent of the data subject [Article 7 (a)], which cannot be construed for anonymous users or for users who have chosen not to authenticate themselves.

The necessity for the performance of a contract [Article 7 (b)], which legal basis may be used to collect personal data on the registered and authenticated users, but cannot be a ground of processing the data of anonymous users, because it is not strictly necessary for the performance of the de facto contracts they entered into when they conducted a search.

---

[19] Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, adopted on 20 June 2007, available at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm>

[20] *"…the user's PC can be viewed as equipment in the sense of Article 4 (1) c of Directive 95/46/EC"*, cited from 'Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites', 5035/01/EN/Final, WP 56, adopted on 30 May 2002, available at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2002_en.htm>

The necessity for the purposes of a legitimate interest pursued by the controller [Article 7 (f)], except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

In their replies to the questionnaire, the search engine providers mentioned the following purposes for processing user data, which were thoroughly analyzed by the Working Party using the above mentioned criteria:

Improving the service: The server log analysis is an important tool in the improvement of the search services, e.g. in refining the search results, which was admitted by the Working Party as a legitimate interest, but it added that for this purpose the search queries do not need to be attributable to identified individuals. In addition the Working Party observed that the development of new services, whose nature is as yet undecided, cannot constitute a lawful purpose of the data processing, because it is too vaguely defined to meet the requirements of the Data Protection Directive.

Securing the system: The search engine providers mentioned the system security as a legitimate interest justifying the data processing, because they need sufficient historical sample of server log data in order to detect patterns and analyze security threats. The Working Party accepted this argument on condition that the data stored for security purposes must be subject to strict purpose limitation and a reasonable retention period meeting the requirement of necessity must be defined.

*Fraud prevention***:** Using the pay-per-click billing method in advertising, the search engine providers are exposed to the risk of being unfairly charged, if an attacker uses a software to click systematically on the advertisements. For that reason the fraud prevention can also be considered as a legitimate interest justifying the data processing, but the amount of personal data processed and the data retention period should be limited to the extent necessary for this purpose.

Accounting requirements: The search engine providers claimed that because of the pay-per-click billing method, there is a contractual and accounting obligation to retain data, at a minimum until invoices are paid and the period for legal disputes has expired. The Working Party observed that this purpose cannot justify the processing of personal data in case of users who did not click on a sponsored link and expressed doubts as to whether the personal data of search engine users are really essential for accounting purposes –further research would be needed on this subject.

Personalized advertising: Search engine providers seek personalized advertising in order to increase their revenues, which makes it necessary to have knowledge about the behaviour of the users. The Working Party noted that user consent and the performance of a contract can be used as a ground for the legitimate processing of some personal data, but it could not find a legitimate interest which would justify the processing of personal data on users who had not specifically signed up to that service.

Law enforcement and legal requests: Some search engine providers stated that there are legal obligations to store user data for law enforcement purposes. In this context, the Working Party, citing Article 2 sub c of the Framework Directive[21] and Article 5 (2) of the Data Retention Directive[22], made it clear that because the search queries would be considered content rather than traffic data and the search engine providers exercise editorial control over content transmitted, the search engines fall outside of the scope of the definition of electronic communication services and the Data Retention Directive would not justify their data retention practices. The search engine providers have to comply with valid legal orders in individual cases demanding the supply of some information, but this obligation should not be mistaken for a legal obligation or justification for storing personal data for this purpose only.

In addition, the Working Party emphasised some issues to be solved by the search engine industry:

The retention period of personal data stored should be defined precisely for each purpose and should not be longer than strictly necessary. Based on the possible purposes mentioned by the search engine providers, a retention period beyond 6 months does not seem justifiable. Without adequate justification for continued storage, the data must be deleted after the end of a search session.

In *using cookies*, the provisions of the Data Protection Directive and the Article 5 (3) of the ePrivacy Directive[23], read in conjunction with Recital 25

[21] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

[22] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[23] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

shall be complied with. Users should be informed about the use and effect of cookies fully and distinctly, not just as a part of the privacy policy. Because the search engine providers are the controllers of the data stored in the cookies, the responsibility for their processing cannot be transferred to the users based on the assumption that they are able to refuse or delete them any time. The search engine providers shall ensure that the expiration date of the cookies is not excessive in relation to the purposes for which the data contained in them is processed.

The Working Party are aware of the fact that many search engine providers offer also personalized services such as email and it is concerned about the possibility that a central personal account made easy the correlation of customer behaviour across different services. The covert surveillance of people's behaviour is not in accordance with the principles of fair and legitimate processing of the Data Protection Directive, and for this reason correlation can only be legitimately done based on informed consent of the user. The search engine providers may not suggest that the use of the search engines require registration, because the collection of personal data through a personalised account is not necessary for the provision of search services.

The Working Party emphasised also that a special attention should be paid to informing data subjects about the collection and use of their data, because most of them are unaware of the amount of data processed and the purposes for which they are used. The privacy policy of the search engines should be as complete and detailed as possible and it should be easily accessible by the users before conducting any search. Moreover, the search engine providers should ensure that the right of access pursuant to Article 12 of Data Protection Directive is exercisable by their users.

Although the Data Protection Directive and the WP Opinion applicable only in the Member States, their effect extends beyond the borders of the EU. Since the provision laid down in Article 25 of the Directive requires adequate level of protection from third countries where personal data originating in the EU are processed, these countries and their companies are forced to adjust themselves to its strict requirements if they want to participate in the European market. Consequently, the EU legislation serves as a reference point on the field of data protection and privacy in the globalized world.

In the USA, where there is no general data protection legislation at federal level and the generally applicable common-law tort covering invasion of

privacy mostly helps only to compensate harm a posteriori, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework[24] to which the U.S. organizations such as the search engine companies can join in order to prove that their data processing activities are in accordance with the EU regulations.

5. CONCLUSION

Although the Working Party explained in details the issues which need solution on the part of the search engine providers to ensure the lawfulness of their data processing activities, the progress in this field has been slow so far. There has been continuous correspondence[25] between the Working Party and the biggest search engine companies since the Opinion was published, concerning mostly the length of the retention period of data, the expiration period of the cookies, the deletion/anonymization methods and the applicability of the EU law, but neither of them provided full cooperation.

The Microsoft for example de-identifies search history immediately by storing search logs separately from registration data and effectively anonymizes search logs by removing full IP addresses and all cross session identifiers, but on the other hand it is willing to reduce the retention period before anonymization to 6 months only on condition that the others follow suit.

The Google made its privacy policy easily accessible from the home page and reduced the data retention period, but to 9 months only instead of the recommended 6 months. Additionally, instead of the full anonymization it deletes only the last octet of the IP addresses and retains cookies for a period of 18 months, which allows for the correlation of individual search queries for a considerable lengths of time.

The Yahoo reduced the retention period to 90 days with certain exceptions and it deletes the full IP addresses, but it have not provided sufficient technical information about anonymization methods used with regard to user identifiers and cookies.

---

[24] Further see: <http://export.gov/safeharbor/>

[25] The letters from the Article 29 Working Party addressed to search engine operators see at: <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm> and <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en-.htm>

In addition to that, there are new problems to be solved, like the privacy issues of behavioural advertising provided also by the search engine companies, which would require further examination.

Although the fact that in recent years the users and the privacy experts have begun to take the privacy issues of the search engines more seriously is positive, I dare say that there is no real progress on the subject. For example, in addition to the problems mentioned above, the search engine providers still have not made it clear in their privacy policies that what are the exact purposes for which they process user data and to what extent these data are reprocessed for other purposes. The issue of lawful and fully privacy-friendly operation is yet to be solved.

REFERENCES

[1] Tene Omer, 2008, 'What Google Knows: Privacy and Internet Search Engines', Utah Law Review, Vol. 2008, Issue 4 (2008), pp. 1433-1492.

[2] Declan McCullagh, Elinor Mills, 'Feds take porn fight to Google', *CNET News*, January 19 2006 [Online]. Available at: http://news.cnet.com/Feds-take-porn-fight-to-Google/2100-1030_3-6028701.html?tag=mncol [Accessed on 22 November 2010].

[3] Nicole Wong, 'Judge tells DoJ "No" on search queries', *The Official Google Blog*, March 17 2006 [Online]. Available at: http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html [Accessed on 22 November 2010].

[4] Danny Sullivan, 'Bush Administration Demands Search Records', January 19 2006 [Online]. Available at: http://blog.searchenginewatch.com/060119-060352 [Accessed on 22 November 2010].

[5] Declan McCullag, 'FAQ: What does the Google subpoena mean?', *CNET News* January 20, 2006 [Online]. Available at: http://news.cnet.com/FAQ-What-does-the-Google-subpoena-mean/2100-1029_36029042.html?tag=mncol;txt [Accessed on 22 November].

[6] Michael Barbaro, Tom Zeller Jr., 'A Face Is Exposed for AOL Searcher No. 4417749', *The New York Times*, August 9 2006 [Online]. Available at: http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1 [Accessed on 11 March 2009].