GOOGLE PRIVACY POLICY – "IN BREACH OF EU LAW"?

by

ALICJA GNIEWEK*

On the 1st of March 2011, one of the biggest service providers in the Internet domain — Google (search engine, web mail, social networking site, Google Aps etc.) — changed its Privacy Policy. Instead of different privacy policies for each service, one single Privacy Policy was adopted for all its services. An information campaign was made in advance: Google gave its users two options — either agree to adopt its new Privacy Policy or cease using Google services altogether. The latter option proved to be quite difficult (but not impossible) to enforce. Google's near total market domination gave it no incentive or inducement whatever to offer users a third option of selective participation in its services.

Google's new Privacy Policy created a huge outcry across the world, despite a huge information campaign conducted to assuage users' fears. The policy was scrutinized by data protection authorities throughout the world (French data authority – CNIL on behalf of the European Union; U.S. Attorney General, the Privacy Commissioner of Canada and the Asia Pacific Privacy Authorities). Their privacy concerns (e.g. cross-services information gathering and possible consequences such as profiling, privacy concerns for Android users, ways of informing users and possibility of opt-out) are addressed in this paper. The emphasis is on the European standpoint as it seems to be the most articulated at the moment; this is highlighted by CNIL's detailed questionnaires on March 16 and March 22.

This paper also analyses Google's policy in the context of transparency and a data subject's right to be informed.

The paper offers the tentative conclusion that Google's Privacy Policy is in breach of the EU Data Protection Directive (Directive 95/46/EC). The paper finally

* Interdisciplinary Center for Security Reliability and Trust, University of Luxembourg, Luxembourg-Kirchberg, Luxembourg, alicja.gniewek@uni.lu

describes the possibility of massive abuse brought by the new policy. It attempts to show that personal profiling can bring with it such activities as hacking, identity theft and fishing expeditions conducted by law enforcement authorities. It can in turn impact upon freedom of expression.

KEYWORDS:
Cloud Computing, Data Protection, Privacy Policy, Transparency, EU Data Protection Law.

1. GOOGLE'S INFORMATION CAMPAIGN – MASSIVE SUCCESS OR FAILURE?

In today's IT world information has a measurable value. The magnitude of data and consequently the chaos of the Internet create the need for guidance. In the early 1990s the first Internet search engines were invented[1], and through special algorithms they allow people to look for anything they want on the Internet. There are a number of search engines in use nowadays, but Google's has achieved the biggest market share recently.[2] Every day millions and millions of people throughout the world utilize Google's search engine to look for information relating to different aspects of their personal and professional life. The total number of searches amounted to 1, 722, 071, 000, 000 in the year 2011, and this breaks down to 4, 717, 000, 000 searches per day[3]. Google retains information on both the objects searched for and the identities and characteristics of the searchers themselves (their interests, needs, personal situations, religious beliefs and sexual orientation[4]). The users' privacy could be violated by abusing the aggregated information. As the famous case of AOL has shown[5] – even anonymised data with numbers put in place of names can be decoded. This privacy problem has been intensified by the proliferation of vast number of

---

1 Wall, A. 2010, *History of search engines: from 1945 to Google today*, http://www.searchenginehistory.com [Accessed 1 Sep 2012].

2 Market share for 2012: Google-Global – 90,08%, Yahoo-Global – 5,53%, Baidu – 1,6%, Bing – 1,15%, Ask-Global – 0,46%, AOL – Global 0,02%, Excite-Global – 0,01%. NetMarketShare, *Internet Market Share Data*, http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4&qpcustomd=1&qpct=6&qptimeframe=Y [Accessed 2 Aug 2012].

3 Statistic Brain 2012, *Google Annual Search Statistics*, http://www.statisticbrain.com/google-searches/ [Accessed 2 Aug 2012].

4 Bodogh, Z. 2011, 'Privacy issues of the Internet search engines – in the light of EU Data Protection legislation', *Masaryk University Journal of Law and Technology*, Vol.5, No. 2, p.164.

5 Bodogh, Z. 2011, 'Privacy issues of the Internet search engines – in the light of EU Data Protection legislation', *Masaryk University Journal of Law and Technology,* Vol.5, No. 2, p.169.

other services, for example Gmail and YouTube in the case of Google and Yahoo! Mail etc. in the case of Yahoo!

On the 1st of March 2012 Google inaugurated its present Privacy Policy[6]. The company decided to establish a single global policy governing all of its services instead of a variety of policies for each and every service. Prior to the adoption of the new policy, Google regularly informed its users of its right to effect changes ('Privacy Policy may change from time to time"[7]). In 2000 Google informed[8] its users that in the event of any changes to its policies, they would be informed via the Privacy Policy Website. In 2004, Google further stated that most of the changes would be minor, but there might also be significant ones, and that any changes would be announced either or both on its standard website or through other unspecified means ("more prominent notice" [9]). In the same announcement, Google also provided an easily accessible archive of past versions of its Privacy Policy. One year later in 2005, Google made the following announcement: "We will not reduce your rights under this Policy without your explicit consent". It is also stated that users would be notified of any significant changes to its Privacy Policy by e-mail. This announcement has remained substantially unchanged up to the present day (the only change has been the withdrawal of the assurance that the vast majority of changes would be "minor").

The alteration introduced by Google in the first half of 2012[10] was preceded by an information campaign. Google has described it as "first [information campaign] on such a scale in the history [of Google]." [11] This statement results in a conclusion that the modification of the Privacy Policy is significant from the Company's viewpoint. Media were interested in the planned modification before and after its introduction. This interest was even more fuelled by the announcements made by alarmed public authorities. The efficiency and the final effect of the information campaign remains

---

[6] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[7] Google 2000, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/archive/20000814/ [Accessed 1 Jul 2012].

[8] *Ibidem.*

[9] Google 2004, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/archive/20040701/ [Accessed 1 Sep 2012].

[10] By the time of this publication there were two alterations made in 2012 - on the 1st of March 2012 and on the 27th of July 2012. The latter brought only "Google Fiber" into the category of products with separated privacy rules. This article refers to the first modification as to the one in question.

[11] Google 2012, 'Google to CNIL, 20 April 2012' *Letter*, https://docs.google.com/file/d/0B8syaai6SSfiSUhFMHVpMmhFUG8/edit?pli=1 [Accessed 1 Jun 2012].

a matter of argument. Google upholds that its information campaign was very extensive and sufficient enough in addressing both authenticated and non-authenticated users. It has also reached data protection authorities which were notified[12] before ordinary users. These pre-briefings were later criticized[13] as being done too late and without sufficient coverage of all respective bodies (e.g. Google informed only 18 data protection authorities in the European Union – DPAs). Google opposed[14] this by underlying general reluctance among DPAs to the proposed meetings and discussions. The company stated however that it recieved constructive feedback. There was no request for "pause" in the process of launching the new Privacy Policy[15] at this point.

An announcement preceding the modification of the Privacy Policy was first publicly released[16] on Google's official blog on the 24th of January 2012. Afterwards, in order to inform its users about the alteration, Google used e-mail communications (the company sent a message to each e-mail address known to them, including those connected with an e-mail address created for the Google Account), promotion on the website (on the website google.com and on the corresponding websites with country domains), "in product" notification, an icon on the Google websites, and finally an interstitial[17].

Google was asked[18] by the French data protection authority (CNIL) to provide the exact number of unique visitors on the Google Privacy Policy website. The data protection authority intended to assess the effectiveness of the information campaign. The company refused and stressed many means used for communication between Google and its users[19]. CNIL was not satisfied with this reply and again requested the number of users' visits

---

12 *Ibidem.*

13 CNIL 2012, 'CNIL to Google, N/Ref: IFP/BPS/CE1211115, 27 Feb 2012' *Letter*, http://www.cnil.fr/fileadmin/documents/en/Courrier_Google_CE121115_27-02-2012.pdf [Accessed 1 Jul 2012].

14 Google 2012,'Google to CNIL, 20 April 2012' *Letter*, https://docs.google.com/file/d/0B8syaai6SSfiSUhFMHVpMmhFUG8/edit?pli=1 [Accessed 1 Jun 2012].

15 *Ibidem.*

16 *Google 2012,* Updating our privacy policies and terms of service, *http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html [Accessed 5 Jul 2012].*

17 Google 2012,'Google to CNIL, 20 April 2012' *Letter*, https://docs.google.com/file/d/0B8syaai6SSfiSUhFMHVpMmhFUG8/edit?pli=1 [Accessed 1 Jun 2012].

18 CNIL 2012, 'CNIL to Google, N/Ref: IFP/BPS/CE121169,16 March 2012', *Letter*,http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf [Accessed 3 Jun 2012].

19 Google 2012,'Google to CNIL, 20 April 2012' *Letter*, https://docs.google.com/file/d/0B8syaai6SSfiSUhFMHVpMmhFUG8/edit?pli=1 [Accessed 1 Jun 2012].

on the Privacy Policy website in the period between the 24th of January 2012 and 1st of March 2012. They were surprised that Google had not measured the efficiency of the campaign[20]. The final refusal of Google was supported by the same argumentation as the previous one[21].

An informed consent done by a user should be the ultimate goal of each information campaign relating to privacy. The form of the consent itself is also important. Google was recently criticized for proposing a "take-or-leave-it" mechanism in this matter. According to the new rules, a user may either adhere to the new policy or stop using Google services. The latter involves changing his personal habits as well as considerable professional dealings of many users around the world, especially taking into account Google's big search market share in both the United States[22] and Europe[23]. People using Google services for professional activity and companies and public bodies are faced with a significant change that not only requires looking for a new service provider but also training their staff and related costs.

The processing of personal data as defined in Article 2b of the Data Protection Directive (Directive 95/46/EC) may occur only if there is at least one legal basis from Article 7 of the Data Protection Directive (Directive 95/46/EC) present. In the given circumstances two options could be discussed: a user gives consent to the processing of his data either by further using the Google services or because it is necessary for the performance of the contract. The latter is strictly interpreted by the data protection authorities,[24] and it seems that combining data across the services is not necessary for the performance of a contract that has in its core such services as Gmail communications or YouTube videos. The requirements for consent are set by the Data Protection Directive (Directive 95/46/EC) and repeated in the interpretation of Article 29 Working Party (WP29). Firstly, according to WP29,

---

[20] CNIL 2012, 'CNIL to Google, N/Ref: IFP/GLD/CE121236, 22 May 2012', *Letter,* http://www.cnil.fr/fileadmin/documents/en/Letter_CNIL_to_Google_22_May_2012.pdf [Accessed 10 July 2012].

[21] Google 2012,'Google to CNIL, 20 April 2012' *Letter*, https://docs.google.com/file/d/0B8syaai6SSfiSUhFMHVpMmhFUG8/edit?pli=1 [Accessed 1 Jun 2012].

[22] Pew Internet & American Life Project 2012, *Search Engine Use 2012,* http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf [Accessed 3 Jul 2012].

[23] Henderson, T. 2012, 'How I divorced Google. Leave Google, and save your privacy in 7 days (or at least get a start on it)', *ITWorld,* http://www.itworld.com/it-managementstrategy/259252/how-i-divorced-google?page=0,0 [Accessed 3 Jul 2012].

[24] Kuner, Ch. 2005, *European Data Protection Law*, Oxford University Press, Oxford, pp. 243-244.

the exercise of real choice exists if there are no "significant negative consequences" for users. It was also stressed in another opinion of WP29[25] that there cannot be any pressure on the user "be it social financial, psychological or other". Moreover, the consent according to WP29 "seems to imply a need for action" and cannot be passive, as the absence of any behaviour is not regarded as consent.[26] In the case of Google and the new Privacy Policy, the existence of an action is questionable. It could be alleged that the users were unexpectedly forced to make a choice that was not supported at that time by any official analysis of a data protection authority or statement of consequences of any other body. Without proper information and with the possibility of financial and psychological consequences – the choice of Google does not seem to be free and real.

2. EVOLUTION OF GOOGLE

Google is an example of an IT company that has vastly expanded its interests and has significantly evolved technologically. It started as a search engine which achieved massive success. The company's services could be described as relatively simple, intuitive and free of charge. Google has created such services as mail, maps, translator, specialized search engines (e.g. images, videos, news, and research publications), document readers and editors on this basis. The next step of Google's development was commercialization. After gaining experience with the free services, it proposed paid versions for commercial users. This concept corresponds to the Software as a Service (SaaS) Cloud Computing paradigm: the user pays only for the effectively used software. There are only two requirements: connection to the Internet and computing devices necessary to access the Cloud, which could be any modern personal computer or a smartphone.

Data centers are at the core of Google's infrastructure. Their purpose is to run processes on commodity servers and this is aimed at providing services. The Cloud Computing paradigm of multi-tenancy allows the company to optimize the usage of resources. A multi-tenant system processes the requests from many distinct users or organizations. The main benefit of that concept is the statistical multiplexing of clients' demands: servers are not

[25] Article 29 Working Party 2007, *Working Document on the processing of personal data relating to health in electronic health record (HER) WP 131*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf [Accessed 5 Aug 2012].

[26] Article 29 Working Party 2011, *Opinion 15/2011 on the definition of consent*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf [Accessed 4 Jun 2012].

dedicated to specific services, but each of them runs multiple processes. As a result, the varying demand for different services is distributed among servers, resulting in even utilization and mitigating consequences of bursts in usage.

At the same time, such techniques raise privacy and security concerns. In case of an attack on such a machine a hacker could obtain control over it and subsequently accesses data stored or processed. He may use the data directly or utilize them in order to continue the attack. Moreover, there are no technical barriers for the cloud provider to analyse not only the content of stored data but also its usage patterns. Using data mining could give insights which are unknown even to the data subjects. Such knowledge can be used to optimize the state of the cloud system (e.g. reducing data centers energy consumption), but also to extract sensitive information such as private data, behavioural patterns or trade secrets (e.g. given load balancing algorithms it could be used by another entity which uses Google services). The multi-tenancy grants access to even higher level of information: combined behavioural data of many users can lead to the creation of statistical models of the behaviour of the whole community of Google's users. While such information is not sensitive from the point of view of an individual, it can be used to get valuable information about whole societies. Finally, multi-tenant resource sharing technologies allow the execution of various processes on the same machine, e.g. Google File System (GFS)[27], BigTable[28], MapReduce[29] and application servers. Google has developed these technologies in order to process huge and distributed volumes of data.

The evolution of Google also brought many privacy questions and forced the international community to again ask the core questions about today's definition, meaning, and application of privacy. Some of Google's steps were really sensitive and important for users, for example the case of Street View and the intercepting of unauthorized data[30], Google Buzz and violations of privacy by default settings, and the scanning of Gmail ac-

[27] Ghemawat, S., Gobioff, H.,Leung, S. 2003, 'The Google file system', *Proc. of the 19th ACM symp. on Operating syst. principles (SOSP '03)*. ACM, New York, NY, USA, pp. 29-43.

[28] Dean, J.,Ghemawat, S. 2008, 'MapReduce: Simplified Data Processing on Large Clusters', *Commun. ACM*, vol. 51, pp. 107-113, Jan. 2008.

[29] Chang F. et al. 2008, 'Bigtable: A Distributed Storage System for Structured Data', *ACM Trans. Comput. Syst.*, vol. 26, art. 4.

[30] Sloot v. d., B.,Zuiderveen Borgesius, F. J. 2012, 'Google and Personal Data Protection', *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models in Information Technology and Law Series,* ed. Lopez-Tarruella, A., vol. 22 VIII, T.M.C. Asser Press.

counts. Some of these questions are still not resolved today. An ambiguous approach of Google to privacy and compliance was presented threateningly in the recent release of information that Google has not erased the data intercepted via its Street View scanning although the company was requested to do so.

The relationship between business and privacy was finally taken into account in the merger case of Google and DoubleClick. FTC failed to fully address the privacy issues[31]. In December 2007 the Google-DoubleClick merger was approved[32]. In March 2007, the European Commission also approved the merger, referring to privacy only by the statement that EU data protection laws will apply[33]. The difference between the rules governing competition and the rules governing privacy are clear. Although it seems that the approach to the privacy of Internet companies constitutes an important factor that should be assessed in further considerations on competition law, it was proved in the recent case of TripAdvisor and Google[34] that there is clearly a tight relationship between competition and privacy. The value of unrestricted access to the users' data is at stake.

---

[31] Interestingly enough Commissioner Harbour in his dissenting opinion raised core elements of relation between users' trust and company's behaviour: *"(…)the combined firm is urged to state clearly and unambiguously what kind of information it intends to gather, how it will collect and use that information, and what choices consumers will be able to exercise. Consumers deserve a clear explanation from Google/DoubleClick, so they can shape their Internet behavior and determine how much information they are willing to reveal. Clearly explaining the firm's information practices and the choices available to consumers will demonstrate Google/DoubleClick's good intentions, as well as the company's willingness to be held accountable for its commitments.* [7]*"To be available at:* Harbour, P.J. 2007, *In the matter of Google/DoubleClick, FTC File No. 071-0170 dissenting statement of commissioner Pamela Jones Harbour*, http://ftc.gov/os/caselist/0710170/071220harbour.pdf [Accessed 2 Jul 2012].

[32] Federal Trade Commission 2007, *Statement of Federal Trade Commission concerning Google/DoubleClick, FTC File No. 071-0170*, http://ftc.gov/os/caselist/0710170/071220statement.pdf [Accessed 6 Jul 2012].

[33] European Commission 2008, *Commission Decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement*, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf [Accessed 1 Jun 2012].

[34] Garside, J. 2012, 'TripAdvisor files competition complaint against Google', *The Guardian*, http://www.guardian.co.uk/technology/2012/apr/03/tripadvisor-files-complaint-against-google [Accessed 5 Aug 2012].

3. ELEMENTS OF THE CUREENT GOOGLE PRIVACY POLICY

3.1 LANGUAGE AND STRUCTURE OF THE GOOGLE PRIVACY POLICY

3.1.1 LANGUAGE OF THE GOOGLE PRIVACY POLICY

Alma Whitten[35] pointed out that the language of the new Privacy Policy is "plain"[36]. The Privacy Policy itself states that it was designed to be "as simple as possible". The text of the Privacy Policy itself is short – it has only ca. 2260 words. Additionally, the main Privacy Policy website includes a link to another website – "Key terms". The latter contains basic definitions of: personal information, Google Account, Cookie, Anonymous identifier, IP address, Server logs, Sensitive personal information, Non-personally identifiable information, and Pixel tag.

The cohesion of the language of the Privacy Policy raises objections. The object of the processing is not represented coherently throughout the text. Google uses various terms – mainly "information", but also more specifically – "personal information" and "personally identifiable information" and "non-personally identifiable information". In the "Key terms" there is no definition of "information" as such, but the company provides the description of "personal information" and "non-personally identifiable information." For that reason, in its questionnaire the French date authority invited Google to clarify the meaning of the abovementioned terms[37]. Google replied that the terms "personally identifiable information" and "personal information" are used interchangeably, and the meaning of "information" according to them is broader and refers to "information associated with anonymous identifiers". Moreover, Google pointed out a problem of different terminology used both within the European Union and beyond its borders. According to the company – its choice of terms is justified by their simplicity.

Google uses expressions of the possibility and the likelihood of certain actions in the Privacy Policy. They may leave a user with an impression of uncertainty. Google does not explicitly inform that the company conducts

---

[35] Director of Privacy, Product and Engineering of Google

[36] Whitten, A. 2012, 'Google's new Privacy Policy', *Google Official Blog*, http://googleblog.blogspot.com/2012/02/googles-new-privacy-policy.html [Accessed 5 Aug 2012].

[37] CNIL 2012, 'CNIL to Google, N/Ref: IFP/BPS/CE121169,16 March 2012', *Letter*,http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf [Accessed 3 Jun 2012].

some activities, but it states that it "may" [38] do so. The modal verb "may" is repeated in the text of the Privacy Policy 38 times. In 21 out of the 38 cases – "may" refers to the crucial activities of Google (e.g. "we may collect information"[39], "Google may associate"[40], "We may use the name" [41], "We may use your email address"[42], "We may combine personal information"[43], "We may reject request"[44]. According to the general study on the language of Google representatives done by Hoofnagle, – "(…) analysis shows that Google's privacy rhetoric generally lack substance. It most frequently uses hackneyed messaging that is optimized to affect consumer biases, encouraging them to assume that the company will do the right thing when in fact it has promised only good intentions"[45]).

3.1.2 STRUCTURE OF THE GOOGLE PRIVACY POLICY

Google transformed its privacy message from around 60 product-specific notices[46] into one single Privacy Policy. There is no separate privacy notice for each of the Google services except products such as Chrome and Chromose OS, Books, Wallet and Fiber.

The Privacy Policy website is accessible via the direct address or the "privacy" bookmark visible on each website used by Google's services. Google advises customers to contact the company directly in case of further questions that go beyond the Privacy Policy. Contact can be made via the "contact us" link that is located in the third paragraph of the Google Privacy Policy. Google FAQ (Frequently Asked Questions)[47] contains both a contact form and the direct address of Google in California for correspondence. Once a user decides to contact Google via the "contact us/contact form" link

[38] 'May', *Cambridge Dictionary Online 2012*, http://dictionary.cambridge.org/dictionary/british/may_1?q=may [Accessed 4 Aug 2012].

[39] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[40] *Ibidem.*

[41] *Ibidem.*

[42] *Ibidem.*

[43] *Ibidem.*

[44] *Ibidem.*

[45] Hoofnagle, Ch. J. 2009, 'Beyond Google and evil: How policy makers, journalists and consumers should talk differently about Google and privacy', *First Monday*, vol. 14, no. 4-6.

[46] Whitten, A. 2012, 'Google's new Privacy Policy', *Google Official Blog,* http://googleblog.blogspot.com/2012/02/googles-new-privacy-policy.html [Accessed 5 Aug 2012]./8

[47] Google 2012, *FAQ*, http://www.google.com/intl/en/policies/privacy/faq/ [Accessed 15 Aug 2012].

he is redirected to the "Privacy Troubleshooter"[48] website where he can either select a topic from the list or send an opinion or question to Google directly via the contact form. Moreover, in the privacy bookmark Google offers explanations in the form of "Advertising privacy FAQ", "Privacy principles", "Privacy tools" and blogs and videos dealing with the topic of privacy.

Article 29 Working Party proposed another structure of privacy policies informing individuals about their privacy online. In the Opinion 10/2004 on More Harmonized Information Provisions, WP29 suggested three main principles that should help in better informing data subjects:

- Language and layout easy to understand
- Multi-layered format of data subject notices
- Acceptance of short notices if only the whole multi-layered structure meets specific national requirements

The projected multi-layered format of the Privacy Policy will be discussed further here. It covers three layers of information. The first layer[49] informs the user about the identity of the data controller and the purposes of processing (except this information is already known to the user) as well as any additional information that must be provided beforehand to ensure fair processing. Finally, access to the second layer should be included. The second layer communicates[50]: name of the company, purposes of processing, recipients of data, communication between user and company, data transfer to third parties, the rights to access, to rectify and oppose, and finally the user's choices. Consequently, there must be also a point of contact for questions and information on in-company redress mechanisms and information on the nearest data protection agency. As to the format, it should be made available online and in hard copy upon written or phone request. The third layer – "the full notice,"[51] contains all national legal requirements and specific features. As such, it is a full privacy statement plus links to national contact information.

---

[48] Google 2012, *Privacy Troubleshooter*, http://support.google.com/bin/static.py?hl=en&hlrm=pl&ts=1291807&page=ts.cs [Accessed 4 Jul 2012].

[49] Article 29 Data Protection Working Party 2004, *Opinion 10/2004 on More Harmonised Information Provisions,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf [Accessed 3 Jun 2012].

[50] *Ibidem.*

[51] Article 29 Data Protection Working Party 2004, *Opinion 10/2004 on More Harmonised Information Provisions,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf [Accessed 3 Jun 2012].

The explained approach of WP29 could be an interesting solution for Google. It provides all of the necessary information in the simple form of layers that are connected with each other, giving a possibility for a user to decide how much information about privacy he wants to reach for. It could be browsed through according to users' needs without any unnecessary burden. The problem of vagueness could be solved by smart connections between the layers containing more and more precise and definite information. The current Google Privacy Policy is shaped as a single-layered notice that contains a wide array of issues. It could be better for users to have the first layer of Google policy with only several matters that could be unwound in the separate, connected layers. While providing some definitions of technical terms is generally supportive for users, such a Privacy Policy seems to need more definitions that are characterised not only by simplicity but also by their technical and legal precision. There is no obligation to preserve the Privacy Policy in the form of bare text. Illustrative comments, videos, blogs, graphs, and finally a great number of examples could possibly provide a great encyclopaedia of privacy used according to the user's needs. Practice shows that users do not read [52] privacy policies. In order to assure conscious consent nowadays, company should provide privacy information that is not only transparent and easy to read but also short and precise. Again, the problem of space can be easily resolved by using the layered structure. The last question is whether the company should care about the visual presentation of its Privacy Policy in order to attract customers.

3.2 SELECTED ELEMENTS OF THE GOOGLE PRIVACY POLICY

3.2.1 PURPOSE OF PROCESSING: IMPROVEMENT OF SERVICES

Google frequently assures in the text of its Privacy Policy that its main objectives are simplicity and the interest of the user, such as "(…) we can make those services even better (…)", "(…) to make sharing with others quicker and easier (…)", "(…) as simple as possible (…)", "Your privacy matters to Google (…)", "(…) provide better services to all of our users (…)", "(…) to

[52] *Inter alia*, McDonald, A.M., Cranor, L.F. 2008, 'The Cost of Reading Privacy Policies', *A Journal of Law and Policy for the Information Society*, vol. 4, is. 3; Delichatsios, S. A., Sonuyi, T. 2005, 'Get to Know Google… Because They Know You', *Ethics and Law on the Electronic Frontier*, 6.805.

improve your user experience and the overall quality of our services (…)", "(…) make it easier to share things with people you know (…)", "Our goal is to be clear (…)". The company aims at the development of better services and simpler, quicker and easier sharing of data. Development and improvement of Google services is going to be not only tailored for the users but also secure, because "(…) privacy matters to Google[53]"

Google expressed its devotion to the constant development of the user experience with Google services. It uses both business and technical measures in order to achieve this goal. According to Article 29 Working Party, the improvement of services is a ground often mentioned by search engines in order to justify using and storing personal data[54]. According to this study, "search queries do not need to be attributable to identified individuals in order for them to be used to improve search services"[55]. Furthermore, for the given purposes it is sufficient to differentiate search queries of non-authenticated users and not to combine them with personal data.[56] Google declares that it "collects information to provide better services to all of our users" (among others from search logs). In the study of WP29, it was stressed that "generally, search engine providers fail to provide a comprehensive overview of the different specified, explicit and legitimate purposes"[57]. This seems to be the case in the new Google Privacy Policy given that the purposes of processing are not explained in detail. Such an explanation could be helpful for an ordinary user to understand what exactly might happen to his/her personal data. Adding an explanation of specific purposes of processing for each service should be considered. It could be made in a form of small websites sub-linked to the main Privacy Policy for example. Such a form of notices would allow the user to have a transparent main Privacy Policy with important "footnotes" beneath.

---

[53] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 July 2012].

[54] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[55] *Ibidem.*

[56] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[57] *Ibidem.*

3.2.2 TYPES OF COLLECTED DATA.

Google uses different channels for obtaining information concerning its users. Users introduce their data while using Google services. Google tracks customers' characteristics (e.g. location and IP address) and their behaviour while they use its services. The Privacy Policy contains a list of different types of collected data – "This information includes: Device information (…), Log Information (…), Location information (…), Unique application numbers (…), Local storage (…), Cookies and anonymous identifiers (…)"[58]. The term "This information includes:" suggests that the provided list of data is not enumerative and Google could also collect other types of data. The lack of precise information – either a full list of collected data or a stronger underlining of the fact that Google can collect more – is likely to mislead users. Users are not able to precisely determine which data are processed in the end. Moreover, examples of different types of processed data could be useful in order to clarify and supplement the often "hermetic" language of computer science.

3.2.3 COMBINING DATA ACROSS DIFFERENT GOOGLE SERVICES.

Google admits that the company combines personal data required in the course of registration of the Google Account with other data obtained across its services –"We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account"[59]. Additionally, the company introduces an unclear functionality that replaces past names existing in different services with the current one – "so that you are represented consistently across all our services"[60]. Better recognition of users is in the best interest of the users themselves according to the company's statement. It provokes the question of the intensity of tracking conducted by Google. It is also interesting how Google plans to monitor, differentiate and control the past and the current names. The company intends to have its users identified, although there is a possibility that users would like to be anonymous with different names for different services without considerable effort.

---

[58] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[59] *Ibidem.*

[60] *Ibidem.*

The company admits to using cookies, pixel tags and other technologies which are not described in detail. Consequently, the user does not know exactly which technologies will be used in order to track their behaviour. There is no enumerative list of technologies used in this respect.

According to the cross-service exchange of information in the area of behavioural advertising, Google declares that it will not correlate sensitive categories with personal information –"we will not associate a cookie or anonymous identifier with sensitive categories such as those based on race, religion, sexual orientation or health"[61]. However, the company does not assure that it will not store these kinds of data. Additionally, Google declares that they are not combing DoubleClick cookie information with personally identifiable information unless there is a specific opt-in. "We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.[62]"

Article 29 Working Party explains that the cross-service data correlation can be done for authenticated users only after two conditions are fulfilled jointly – there is consent of a user which is adequately informed[63]. The meaning of adequate information given by Google to its users is a matter of dispute. Google declares that "It's been the most extensive user notification effort in Google's history – including promotions on our homepage, emails to our users, just-in-time notifications, and more(…)[64]". CNIL replies that there was no adequate information campaign addressed to all data protection authorities. Additionally, a survey conducted in the UK by Big Brother Watch and YouGov revealed that only 12% of Google users read the changed Privacy Policy. As many as 65% of people were not aware of when exactly the modifications would be implemented and 47% did not have any knowledge about the proposed changes[65]. These numbers show the relatively weak effect of the information campaign.

---

[61] *Ibidem.*

[62] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[63] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[64] Google 2012, 'Google to CNIL, 3 Feb 2012', *Letter,* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120203_google_reply_to_art29_en.pdf [Accessed 1 Jul 2012].

[65] Big Brother Watch 2012, *Nine in ten people have not read Google's new Pirvacy Policy*, http://www.bigbrotherwatch.org.uk/home/2012/02/ten-people-havent-read-googles.html#.T5EihtlIuAp [Accessed 6 Jun 2012].

The correlation can also be done in the case of non-authenticated users by means of an IP address or unique cookie that could be tracked in all services. It is against the principles of fair and legitimate processing[66] in the case of not informed users. Therefore WP29 suggests that search engines should clearly inform the users about the correlation and well obtain valid consent from them[67].

3.2.4 DATA CENTERS LOCATION

Data centers of Google are located in many countries around the world. Information on their precise location is not comprised in the text of the Privacy Policy. Data centers store and process the data of Google's users. The users are not informed about the current location of their data. The location of the data is not permanent. The packets of data could cross borders of any country where the data center is located. There is no obligation to locate the user's data in his country of residence. In the previous version of the Google Privacy Policy (20th of October 2011) there was an explicit reference to the data centers in the United States (as one of the possible locations), but in the current version it was deleted. The whole paragraph related to the data centers appeared for the first time in the Google Privacy Policy in 2005 (14th of October 2005).

The location of data centers and the related concept of dynamic allocation of data is dubious from the legal point of view, taking into account general territorial character of law. From the business perspective it brings new quality to computing as it offers fast and massive processing at low costs. Applicability of law is a matter of question. Appliance of the U.S. law is widely discussed in the European Union, especially because of the Patriot Act and respective privacy fears of the Cloud users[68]. Recently, "protectionist" moves have emerged on the national level, for example the French project Andromède and safe "made in Germany" Cloud. Such initiatives aim at creating an in-house cloud computing on a national level in order to protect users from 3rd parties attempts to access personal data. While encouraging

---

[66] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[67] *Ibidem.*

[68] Reding V 2012, *The future of data protection and transatlantic cooperation Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels, 6 December 2011, Speech/11/851*, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&format=HTML&aged=0&language=EN&guiLanguage=en [1 Jun 2012].

the growth of European Clouds, Commissioner Reding suggested that the free flow of data between countries around the world should be preserved[69].

3.2.5 ACCESS TO THE INFORMATION AND DATA RETENTION

The data retention information is not contained in the text of the Privacy Policy. Google's focus is on the access to the data and right to delete it at the user's request. Google explains that user has a possibility to access, update and delete data – "(…) we aim to provide you with access to your personal information. (…) 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.[70]" The last phrase, "legitimate business or legal purposes," seems to be utterly vague as there are no further definitions or clarifications regarding the two types of purposes in question.

The text of the Privacy Policy address is another situation in which Google is not obliged to act upon the request of the user. It is purely technical – "(…) 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 (…) extremely impractical (for instance, requests concerning information residing on backup tapes).[71]" The GFS design goals mentioned above do not include retention. It may be unjustified from the technical point of view for the company to remove user's data due to the arbitrary request of a user.

Even if the data are deleted, it is uncertain if they are deleted entirely. The backup systems and the residual copies are being kept due to the security reasons. There are no time limits set therein in order to provide for a definite retention period. "Where we can provide information access and correction, we will do so for free, 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."[72] In this statement, Google differentiates

---

[69] *Ibidem.*

[70] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[71] *Ibidem.*

[72] *Ibidem.*

between the storage on the active servers and storage in the backup systems. It implies that deletion made by the user is not ultimate since Google may store the data on the active servers for some time after the deletion request. Moreover, there is no clarification regarding the term "not immediately", and Google declares that it may not delete the information from the backup systems. This issue raises the following questions for the user:

- Does "information" in question mean users' data within the Google services?

- Does it mean that user's data will stay endlessly in some form in the Google storage system?

- Is there any possibility for Google to use data after the deletion request, and in case of a positive answer – for which purposes?

Article 29 Working Party maintains that retention periods should be proportionate to the specific purposes of the processing[73]. The Google Privacy Policy does not comprise such periods. Moreover, according to further studies of WP29 the retention period should be defined[74]. Such information seems to be necessary even if in the first layer of the policy such as the user's knowledge on access and deletion is decisive for their usage of services[75] (e.g. the user may not be willing to include their photos in the service in case they cannot ultimately delete these data). Data retention will not be discussed in this paper in detail due to the space limitations; however it should not be neglected by the Privacy Policy of any company that processes data.

3.2.6 INFORMATION SHARING

Google affirms that in principle it does not share its users' data with third parties. Nevertheless, the Privacy Policy indicates four circumstances in which this rule does not apply. Firstly – Google may share user's data with "companies, organizations or individuals"[76] with the user's consent. There is no indication as to the form of the consent. Additionally, Google intro-

---

[73] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[74] *Ibidem.*

[75] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[76] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

duces specific "opt-in consent"[77] for sharing sensitive personal information. The difference between simple "consent" and "opt-in consent" is not explained. Access to the data exercised by the domain administrators is the second exception. Next, Google shares users' data in the course of external processing – with "affiliates or other trusted businesses or persons"[78]. There is no enumerative list of these actors or any other indication as to their nature and the types and purposes of such processing. Last but not least, Google could be forced by law to share data with third parties. Google recognizes the circumstances in which sharing is necessary to comply with law, regulation, process or governmental request, enforcing the applicable Terms of Service, and in the case of fraud and security prevention and investigations and for technical reasons. Finally, there is a possibility to share user's data in order to "protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law"[79]. These conditions apply to "information" – there is no mention of "personally identifiable information". However, Google explicitly refers to "non-personally identifiable information" in the text of the Privacy Policy.

The more detailed and precise data about customers and users is, the better situation the company is in. This claim could be easily adopted by many business actors, including advertisers. According to Article 29 Working Party, search engines "(…) seek personalized advertising in order to increase their revenues. Current practices include taking into account history of past queries, user categorization and geographical criteria"[80]. The present processing of information about users may clearly surpass this definition, especially since Google are able to mix personal data from many services such as YouTube, Gmail, Google Buzz and Google Maps. WP29 reveals that "it is difficult to find a legitimate ground for this practice for users who have not specifically signed in based on specific information about the purpose of the processing. The Working Party has a clear preference for anonymised data[81]".

---

[77] *Ibidem.*

[78] *Ibidem.*

[79] *Ibidem.*

[80] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

[81] *Ibidem.*

3.2.7 NON-PERSONALLY IDENTIFIABLE INFORMATION SHARING

Google freely shares information that is non-personally identifiable. "Non-personally identifiable information" is defined as information "that is recorded about users so that it no longer reflects or references an individually identifiable user."[82] According to Google's "Key terms" site that is sub-linked to the Privacy Policy, Google "(…) may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites[83]". The boundaries of Google's right to gather and share non-personally identifiable information are not easy to determine. It remains an open question whether data aggregated from non-authenticated users combined across many different services is still non- personally identifiable information.

4. SELECTED OPINIONS ON GOOGLE PRIVACY POLICY

Whereas different concerns were raised according to the New Google Privacy Policy – there are some common denominators therein. The most interesting issues were raised in the European Union, the United States and Canada. This paper focuses on the analysis coming from the European Union as it is the most developed at the moment. It also indicates the most important elements of the others.

4.1 THE COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉ (CNIL)

The French data protection authority (Commission nationale de l'informatique et des libertés– CNIL) investigated the Google Privacy Policy on behalf of all EU Data Protection Authorities (DPAs)[84]. The examination was initiated by the Article 29 Working Party in February 2012. Interestingly enough, the CNIL representation of the EU DPAs proves the effectiveness of one DPA acting on behalf of others while being backed by all of the DPAs, as Commissioner Reding has underlined in her speech. This can lead

---

[82] Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

[83] *Ibidem.*

[84] Article 29 Data Protection Working Party 2012,'Article 29 Working Party to Google, just.c.3/2012/135480, 2 Feb 2012', *Letter,* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf [Accessed 4 Jun 2012].

to actively dealing with citizen's concerns[85] and can serve as an argument of having such a provision in the Draft Regulation on Data Protection.

Article 29 WP requested Google to suspend the introduction of its new Privacy Policy. This was justified by the need for investigation into the possible consequences of the new Privacy Policy. Google did not accord with this request,[86] underling its information campaign and respective pre-briefings offered to DPAs. Google presented itself as open to discussion and questions. The company stressed that the "misunderstandings" are caused by the wrong information being spread by competitors[87].

4.1.1 FIRST CORRESPONDENCE BETWEEN CNIL AND GOOGLE

The sufficiency of the information provided to data subjects and combining data across the services were two major concerns stressed by CNIL in its first letter to Google.

According to the preliminary analysis of CNIL – the new Google Privacy Policy does not meet the requirements of the Data Protection Directive (Directive 95/46/EC), especially in context of information provided to data subjects[88]. In its opinion, Google provides only general information, and therefore the average user is unable to distinguish the purposes of data processing, types of collected data, recipients or access rights. According to CNIL, Google should "supplement existing information with service and purpose specific information"[89] and design its Privacy Policy according to Opinion 10/2004 of Article 29 Working Party on More Harmonized Information[90]. Therefore, compliance with Articles 10 and 11 of the Data Protection Directive (Directive 95/46/EC) must be properly examined.

---

[85] Reding, V. 2012, *Strong and independent data protection authorities: the bedrock of the EU's data protection reform Spring Conference of European Data Protection Authorities Luxembourg 3 May 2012 SPEECH/12/316,* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/316&format=HTML&aged=0&language=EN&guiLanguage=en [Accessed 6 Jul 2012].

[86] Google 2012, 'Google to CNIL, 3 Feb 2012', *Letter*, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120203_google_reply_to_art29_en.pdf [Accessed 1 Jul 2012].

[87] *Ibidem.*

[88] CNIL 2012, 'CNIL to Google, N/Ref: IFP/BPS/CE1211115, 27 Feb 2012' *Letter*, http://www.cnil.fr/fileadmin/documents/en/Courrier_Google_CE121115_27-02-2012.pdf [Accessed 1 Jul 2012].

[89] *Ibidem.*

[90] *Ibidem*.

Even "trained privacy professionals"[91] find it hard to identify which data are processed by Google and what the purposes of such processing are. Moreover, it is not clear how cookies will be used in this respect and how user's consent is required by the e-Privacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2009/136/EC) will be expressed[92]. Finally, there are doubts according to the lawfulness, fairness and compliance with the Data Protection Directive (Directive 95/46/EC) of such processing, meaning Article 6 and 7 of the Data Protection Directive (Directive 95/46/EC).

4.1.2 SECOND CORRESPONDENCE BETWEEN CNIL AND GOOGLE: I QUESTIONNAIRE CNIL

On the 16th of March 2012, CNIL issued a detailed questionnaire posing questions regarding what in its view are the most relevant issues of the Google Privacy Policy.[93]. On behalf of all DPAs, CNIL asked for clarification of rules governing data sharing across Google services. It underlined possible difficulties in understanding the terms and conditions[94]. Ten groups of questions were posed[95] by CNIL: definitions, transition to the new Privacy Policy, services and collected data, purposes, data retention, rights and consent, Google terms of service versus Privacy Policy, cross-services data collection, information and additional remarks.

4.1.3 II QUESTIONNAIRE CNIL

CNIL was not entirely satisfied with the answers to the first questionnaire. According to CNIL, Google's replies are not precise, clear and comprehensive. Lack of clarification is of major concern to CNIL, as the user's position is much weaker than the position of the Data Protection Authority. On the 22nd of May 2012 CNIL issued a new questionnaire[96] referring to the first one in order to clarify the objectives of the previous questions.

---

[91] *Ibidem.*

[92] *Ibidem.*

[93] CNIL 2012, 'CNIL to Google, N/Ref: IFP/BPS/CE121169,16 March 2012', *Letter,*http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf [Accessed 3 Jun 2012].

[94] Ibidem.

[95] Ibidem.

[96] CNIL 2012, 'CNIL to Google, N/Ref: IFP/GLD/CE121236, 22 May 2012', *Letter,* http://www.cnil.fr/fileadmin/documents/en/Letter_CNIL_to_Google_22_May_2012.pdf [Accessed 10 July 2012].

4.2. PRIVACY COMMISSIONER OF CANADA

The Privacy Commissioner of Canada[97] focused on three main issues in its examination of the Google Privacy Policy: data retention, combining information across services, and the consequences for Android users.

The privacy authority observed that the expected specific and detailed information on data retention and disposal were not included in the Privacy Policy. This is unacceptable according to its opinion, as such information is crucial for the users. Firstly, Google did not publish any precise retention period for its services, and secondly deletion at the request of the user is not designed well[98].

It was underlined[99] that in its opinion the alterations introduced into the Google Privacy Policy apply only to the holders of Google Accounts. Clarification in this respect was requested. Moreover, the statement that Google "may replace past names associated with your Google Account so that you are represented consistently across all our services[100]" alarmed the Privacy Commissioner. The matter of combining existing and previous accounts in Google services is seen as not being explained clearly enough.

According to the Privacy Commissioner of Canada – in order to fully benefit from the use of Google products Android users must have a Google Account[101]. The user could only benefit from having such an account when he or she accepts the Privacy Policy. Consequently, the new Google Privacy Policy leaves no choice for Android users if they want to keep their devices, and therefore they will be unwillingly affected by the changes to the Google Privacy Policies.

4.3 NATIONAL ASSOCIATION OF ATTORNEY GENERAL (NAAG)

The National Association of Attorney General expressed concern over/with the modifications of Google's Privacy Policy[102] at the end of February 2012.

---

97 Google 2012, *Privacy Policy*, http://www.google.com/intl/en/policies/privacy/ [Accessed 5 Jul 2012].

98 *Ibidem.*

99 *Ibidem.*

100 *Ibidem.*

101 *Ibidem.*

102 National Association of Attorneys General 2012, *Attorneys General Express Concerns Over Google's Privacy Policy,* http://www.naag.org/attorneys-general-express-concerns-over-googles-privacy-policy-attorneys-general-express-concerns-over-googles-privacy-policy.php [Accessed 12 Jun 2012].

Thirty-six Attorney Generals asked Google to clarify several points of the policy, including consent, problems of Android-powered smartphone users and related cybercrime[103]. The assessment of the new Google Privacy Policy is important as it is likely to affect individuals, businesses and government.

NAAG focused among other things on the absence of opt-out and opt-in for the new cross-service sharing of the data. According to the new policy, the processing of data occurs without the affirmative consent of the user, who makes an informed choice to have his data shared across different services of Google[104]. The company has not fitted its user with the real opt-out possibility. Such an option would allow users to continue to use Google's services under the previous privacy conditions. On the contrary, Google did not propose any third option if users do not agree with the Privacy Policy. It is not a real and honest opt-out according to NAAG's argumentation due to the great number of users relying on Google's services. There is also a great chance of danger of lock-in for the businesses that confided in Google services. Affected parties will have to examine the privacy consequences, (including "many federal, state, and local government agencies") of the new Privacy Policy. Finally, it was suggested[105] that the change raises so many consequences that an opt-in procedure for users is better than the current quasi opt-out possibility[106].

The interests of the Android-powered smartphone users (ca. 50% of smartphone market) are also at stake. It seems that their opt-out could only be done by way of abandoning the phone. According to the Attorneys, this invades the statement of Google that they will not reduce users' rights when modifying its Privacy Policy. Moreover, no pre-purchased notice for Android users was underlined[107].

Finally, the Attorney Generals have raised the issue of cybercrime. The new Privacy Policy might increase the possibility of attacks from hackers and identity thieves on the new Google database[108].

---

[103] National Association of Attorneys General 2012, 'NAAG to Google, 22 Feb 2012' *Letter*, http://www.naag.org/assets/files/pdf/signons/20120222.Google%20Privacy%20Policy%20Final.pdf [Accessed 12 Jun 2012].

[104] *Ibidem.*

[105] *Ibidem.*

[106] Abbott, G. 2012, *Google Privacy Policy remains a cause for concern, https://www.oag.state.tx.us/agency/weeklyag/2012/0412google.pdf* [Accessed 12 Sep 2012].

[107] *Ibidem.*

[108] *Ibidem.*

4.4 ASIA PACIFIC PRIVACY AUTHORITIES (APPA).

Asia Pacific Privacy Authorities (APPA) constitute a forum for privacy authorities in the Asia Pacific Region that discuss matters such as personal data privacy, privacy legislation amendments, privacy and security[109]. At the end of February 2012, the APPA Technology Working Group (TWG) on the behalf of APPA[110] made several inquiries about the Google Privacy Policy[111]. TWG recognized Google's commitment to simplicity and intelligibility in designing the new privacy rules and noted the existence of the intensive information campaign. At the same time, combining personal data from across different services and the lack of possibly important details remain the main concerns raised by the organisation[112].

APPA inquired about the user's ability to segregate between different online identities within Google's services. Minorities and risk groups were of special concern in this respect. Google replied[113] that users are still able to hold multiple accounts with multiple identities and are able to safely move data between them thanks to data liberation tools. In Google's opinion, the integration of its services and sharing data across them are in line with the needs and requests of its users. It aims at the creation of a more intuitive, easier and faster user experience. The only exception mentioned is the one-way sharing in the case of Google Web History and YouTube (Google could share with YouTube and YouTube could not share with Google)[114]. APPA followed the conversation between Google and the French data protection authority (CNIL). Therefore, in its second letter to Google[115] – they inquired about data correlation across accounts in order to avoid abuse and preserve

---

[109] *Asia Pacific Privacy Authorities,* http://www.privacy.gov.au/aboutus/international/appa [Accesssed 20 Sep 2012].

[110] Following privacy authorities are signatories to this letter: Office of the Australian Information Commissioner, Australia; Office of the Information and Privacy Commissioner, British Columbia, Canada; Office of the Privacy Commissioner, Canada; Office of the Privacy Commissioner for Personal Data, Hong Kong; Korea Internet & Security Agency, Korea; Federal Institute for Access to Information and Data Protection, Mexico; Office of the New South Wales Privacy Commissioner, Australia; Office of the Privacy Commissioner, New Zealand; Office of the Northern Territory Information Commissioner, Australia; Office of the Information Commissioner, Queensland, Australia; Office of the Victorian Privacy Commissioner, Australia.

[111] APPA 2012, 'Changes to Google's Privacy Policy, APPA to Google,28 Feb 2012, http://www.privacy.gov.au/materials/types/other/view/7167 [Accessed 15 July 2012].

[112] *Ibidem.*

[113] Google 2012, 'Re: Changes to Google's Privacy Policy, 29 Feb 2012', *Letter, http://www.privacy.gov.au/materials/types/other/view/7168* [Accessed 20 Sept 2012].

[114] *Ibidem.*

[115] APPA 2012, 'Letter to Google re CNIL response, APPA to Google,18 May 2012', http://www.privacy.gov.au/materials/types/other/view/7171 [Accessed 20 Sep 2012].

security. The second question related to the storage of associated data of different account holders logged in the same browser session.

Google has not fully answered[116] the APPA's concerns about the effect on new and existing users. New privacy rules are likely to affect new users in the opinion of APPA. However, the organisation is not sure about the effect on existing users. Google declared[117] that the new privacy rules are equally applicable to all of its users, both signed and not-signed. The alteration is not affecting the existing privacy setting and status of the data currently kept privately.

Moreover, APPA states that privacy tools allowing more anonymous usage of Google services are not readily accessible by users. Google did not answer[118] the problem of readability. Instead, the company has listed the examples of the respective tools (no need to sign for some services, edition and turning off the search history, switching Gmail chat to off the record, using Incognito mode on Chrome and controlling ads via Ads Preference Manager).

Asia Pacific Privacy Authorities were also concerned about the lack of important and specific information on time frameworks for the deletion of user's data and the collecting and processing of sensitive information. Google claims [119]to make good faith efforts to provide users with the possibility to access and delete their data. Although it is determined by the architecture of its archive system and therefore deletion at the user's request is made in reasonable time and not immediately, Google has not touched the matter of specific retention periods. In the second letter issued by APPA, it stressed that its opinions are in line of those of the Privacy Commissioner of Canada: clear information on data retention and relevant timelines for data deletion should be included in the public policies[120].

Finally, APPA raised the question of the effect on Android users. Google's reply[121] focused on the equal applicability for all users, both desktop and mobile (Android). Moreover, in Google's opinion Android

---

[116] Google 2012, 'Re: Changes to Google's Privacy Policy, 29 Feb 2012', *Letter, http://www.privacy.gov.au/materials/types/other/view/7168* [Accessed 20 Sept 2012].

[117] *Ibidem.*

[118] *Ibidem.*

[119] *Ibidem.*

[120] APPA 2012, 'Letter to Google re CNIL response, APPA to Google,18 May 2012', http://www.privacy.gov.au/materials/types/other/view/7171 [Accessed 20 Sep 2012].

[121] Google 2012, 'Re: Changes to Google's Privacy Policy, 29 Feb 2012', *Letter, http://www.privacy.gov.au/materials/types/other/view/7168* [Accessed 20 Sept 2012].

users' experience is not deteriorated due to the fact that users still have access to "nearly all functionalities" and they also have many options to control their privacy via respective available privacy tools.

5. CONCLUSIONS

Google took a significant step towards the creation of a simple and user-friendly Privacy Policy. This tendency should be praised as long as in the end it does not bring less information to the user. Unfortunately, the proposed framework has several shortcomings and imperfections.

The language of the Privacy Policy is general and relatively simple. The technical and legal terms do not appear in excess. At the same time, it is very unclear and incomplete in answering the specific issues. The content of the policy fails to address data retention periods. Combining user's data across Google's services is not explained in a sufficiently clear way. Sections dealing with the methods and purposes of data processing lack the basic information needed to determine the possible consequences for the user. Finally, constructing consent on the principle of "take-it-or-leave-it" without leaving any backdoor for the users remains unsatisfying. Consequently, the user is not sufficiently informed about the processing and storage of his data. Accordingly the existence of his informed consent is called into question. Without this information, the user is not able to predict the consequences of his behavior and control his actions.

Combining information obtained across different services leads to the creation of databases[122]. The amount and diversity of the data contained in the databases may induce massive abuses, such as hacking, identity theft and "fishing expeditions"[123]. Storing large amounts of personal data could possibly constitute an incentive[124] for public bodies to exercise their right to request the access to stored data[125] via a valid legal order.

---

[122] Tene, O. 2008, 'What Google knows: Privacy and Internet Search Engines', *Utah Law Review*, No.4, p.1435; Battelle, J. 'The database of intentions', *John Battelle's Searchblog*, http://battelle-media.com/archives/2003/11/the_database_of_intentions.php [Accessed 15 Aug 2012].

[123] Gutwirth, S., De Hert, P. 2008, 'Regulating Profiling in a Democratic Constitutional State', *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Hildebrandt, M., Gutwirth, S., Springer Science + Business Media B. V. 2008.

[124] Tene, O. 2008, 'What Google knows: Privacy and Internet Search Engines', *Utah Law Review*, No.4,p.1482.

[125] Article 29 Data Protection Working Party 2008, *Opinion 1/2008 on data protection issues related to search engines,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [Accessed 12 Jun 2012].

The privacy of the user may be compromised by the access of third parties to the databases. The users could be tracked very precisely due to the information contained therein, even if he does not directly put any personal data into Google services. The latter could bring about serious consequences, even in the area of freedom of speech.