Google and Personal Data Protection

Bart van der Sloot[*]
Frederik Zuiderveen Borgesius[**]

Working Paper. Please, do only refer to the published version:
B. v.d. Sloot & F. J. Zuiderveen Borgesius, Google and Personal Data Protection, p. 75-111, in A. Lopez-Tarruella (Ed.), Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models. Series: Information Technology and Law Series, Vol. 22 VIII, T.M.C. Asser Press (Springer) 2012.

Abstract. This chapter discusses the interplay between the European personal data protection regime and two specific Google services, Interest Based Advertising and Google Street View. The chapter assesses first the applicability of the Data Protection Directive, then jurisdictional issues, the principles relating to data quality, whether there is a legitimate purpose for data processing, and lastly the transparency principle in connection with the rights of the data subject. The conclusion is that not all aspects of the services are easy to reconcile with the Directive's requirements.

"Google's mission is to organize the world's information and make it universally accessible and useful."
(About Google, corporate information)

"Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed (…)" (Recital 28 of the Data Protection Directive)

[*] *LL.M. MPhil. Researcher at the Institute for Information Law, University of Amsterdam, the Netherlands, specialized in privacy* b.vandersloot@uva.nl
[**] *LL.M. PhD Researcher at the Institute for Information Law, Institute for Information Law, University of Amsterdam, the Netherlands* F.J.ZuiderveenBorgesius@uva.nl

4.1. Introduction

4.1.1 Google

The stated aim of Google, one of the biggest, most important and most interesting companies of this age, is to "organize the world's information and make it universally accessible and useful."[1] This chapter discusses two Google services that have sparked much debate, Google's behavioural advertising program called "Interest Based Advertising" and Google Street View.[2] Can the services be reconciled with the requirements of the European Data Protection Directive?[3] The remainder of this section introduces the two services. In the second section, five aspects of the Directive are discussed, largely following the structure of the Directive. The sub sections focus on: the applicability of the Directive, the jurisdiction, the principles relating to data quality, the legitimate purpose and lastly the transparency principle in connection with the rights of the data subject. For each aspect its application to Interest Based Advertising and Google Street View is discussed after a general introduction. Several aspects of the two services are not easy to reconcile with the requirements of the Directive, which was not written with the Internet in mind.[4]

4.1.2 Behavioural advertising

Behavioural advertising entails the tracking of online behaviour of Internet users in order to build a profile of these users to target them with customized advertising.[5] In a highly simplified example, an Internet user that often visits websites with information about cars and football might be profiled as a male sports enthusiast. If this Internet user books a flight to Amsterdam on a website, advertising for tickets for a game of the local football club Ajax might be shown. Many Internet users are not aware to what extent their online behaviour is being tracked.[6]

Google obtains almost all its income from advertising.[7] For years Google concentrated mainly on small text ads next to search results, related to the search queries of users. It seemed that Google was not eager to enter the business of behavioural advertising.[8] In 2007 however, Google paid 3.1 billion dollars for DoubleClick, which was a leading company in the field of

---

[1] See Google's information Our Philosophy at www.google.com/corporate. Accessed 31 August 2011.

[2] See Google, Interest-based advertising: How it works, at http://www.google.com/ads/preferences/html/about.html, and Google, Street View: Explore the world at street level, available at http://www.maps.google.com/help/maps/streetview. Accessed 31 August 2011.

[3] 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 (OJ L 281/31, 23 November 1995).

[4] See about the application of the Directive on the Internet: ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*", para 86.

[5] This description is loosely based on the definition used by the Article 29 Working Party (Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising (WP 171)*. 22 June 2010, p 3).

[6] McDonald 2010, chapter 5; Van Eijk et al. (2011).

[7] According to the annual report of Google, 97 % of Google's revenue in 2009 came from advertising (See Google *2009 annual report*, p 37, available at http://investor.google.com/pdf/2009_google_annual_report.pdf. Accessed 31 August 2011). See about the introduction of advertising to Google's business: Battelle 2005, chapter 6.

[8] See about Google's shifting approach to behavioural advertising: Hoofnagle 2009.

behavioural advertising for over fifteen years.[9] DoubleClick acts as an intermediary between website holders and advertisers, and places advertisements on websites for advertisers. These advertisements are often targeted on the basis of the online behaviour of Internet users. Among other tracking techniques, DoubleClick uses so-called cookies to monitor people's online behaviour. A cookie is a small text file that a website operator (or a third party such as DoubleClick serving content on that website) can store on a computer or a smart phone of an Internet user to recognize that equipment during subsequent visits. This way, a computer can be recognized when it visits another website on which DoubleClick serves advertising. As a result, DoubleClick can follow the online behaviour of an Internet user over all sites on which it serves advertising.

After the acquisition of DoubleClick, Google announced in March 2009 that it would start "making ads more interesting", and it launched its behavioural advertising program, called "Interest Based Advertising".[10] In order to build a profile of Internet users, Google tracks the browsing behaviour of Internet users over all the websites that are part of the Google Display Network, a collection of websites where Google serves advertising. As Google explains, this network "offers text, image, rich media, and video advertising on Google properties, YouTube, and millions of web, domain, video, gaming, and mobile partner sites"[11] and "reaches over 70% of unique Internet users around the world" from over 100 countries.[12] Internet users that do not visit any websites owned by Google are also being tracked. If somebody visits a website within the Google Display Network or a website where Google offers content such as an embedded YouTube video, a cookie or other tracking device might be stored on his computer.

Google would have plenty of opportunities to enrich behavioural profiles with other data.[13] Google's databases might include data regarding with whom you communicate, what you buy, what you write, what you read, where you are, where you will go, and of course what you search for.[14] If somebody provides Google with a name and address when registering for a service, Google could tie this information to the profile.[15] Furthermore, like many online email providers Google automatically scans the contents of email messages, for example to filter out spam. Google also targets advertising in Gmail based on current and earlier email messages: "For example, if you've recently received a lot of messages about photography or cameras, a deal from

---

[9] Google Investor Relations, Google to acquire DoubleClick. Combination will significantly expand opportunities for advertisers, agencies and publishers and improve users' online experience. 13 April 2007, available at http://investor.google.com/releases/2007/0413.html. Accessed 31 August 2011.

[10] Wojcicki S, Making ads more interesting. The Official Google Blog. 11 March 2009, http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html. Accessed 31 August 2011.

[11] Google Adwords, Yankee Candle case study, available at http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//adwords/displaynetwork/pdfs/GDN_Case_Study_YankeeCandle.pdf. Accessed 31 August 2011.

[12] Google AdWords, What are the benefits of the Display Network?, available at https://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=57174. Accessed 31 August 2011.

[13] Krishnamurthy and Wills 2009b

[14] See *inter alia* Google Chat (www.google.com/talk), Gmail (www.gmail.com), Google Voice (www.google.com/voice), Google checkout (http://checkout.google.com), Blogger (www.blogger.com) and Google Docs (www.docs.google.com), Google Books (www.books.google.com), Google Latitude (http://www.google.com/latitude), and Google Calendar (www.google.com/calendar). Accessed 31 August 2011.

[15] For some services Google requires registration with correct name and address information (See Google Terms of Service, available at www.google.com/accounts/TOS. Accessed 31 August 2011.).

a local camera store might be interesting."[16] Google could enrich profiles with data gathered like this. Research has shown that Google could even enrich profiles with information that users submit to social networks that are not related to Google.[17]

However, Google states that it does not tie a name to behavioural profiles: "Throughout this process, Google does not know [the Internet user's] name or any other personal information about her."[18] Furthermore, Google says that it "does not attach particular ads to individual messages or to users' accounts"[19] and that data collected for behavioural advertising are "intentionally kept separate from your Google Account".[20] Hence, Google does not add data that it could gather in for example a Gmail account to a behavioural profile.[21] It is difficult to deduce from the information Google provides to what extent it ties search queries to behavioural profiles.[22]

4.1.3 Google Street View

Why need a room with a view when the world with a view is within hand's reach? The concept of Google Street View is dazzlingly simple, as is the case with most good ideas. Take the roadmap of the world and allow people to zoom in, so that they may walk down Broadway, stop at Abbey Road's zebra crossing and drive down Route 66 in one day. All it takes to achieve this dream is a car and a circulating camera attached to it, or more specifically, several cars with several cameras attached to them.[23] Such techniques are of common use for smaller applications, such as virtual tour guides in famous museums.[24] The idea for Street View is perhaps more dazzling in bluntness than in originality, allowing for a virtual tour around the world. Still, Google has habituated projects larger than life as a company ethic, making the world's information available (Google Books, YouTube), easily accessible (search engine), understandable (Google translation), and visible (Google Street View, Google Earth).[25] Obstacles are of course inherent with projects

---

[16] Gmail. Ads in Gmail and your personal data. http://mail.google.com/support/bin/answer.py?answer=6603. Accessed 31 August 2011.

[17] Krishnamurthy and Wills 2009a

[18] Google Ads Preferences, Interest-based advertising: How it works, available at www.google.com/ads/preferences/html/about.html. Accessed 31 August 2011.

[19] More on Gmail and privacy, available at http://mail.google.com/mail/help/intl/en_GB/more.html. Accessed 31 August 2011.

[20] Google Accounts: Is this everything?, available at www.google.fr/support/accounts/bin/answer.py?hl=en&answer=162743. Accessed 31 August 2011.

[21] It has to be noted that Google's adherence to its own privacy policies cannot easily be checked.

[22] "The technical way that we're doing this is by associating the relevant query words in the referral URL with the existing advertising cookie on the user's browser." (Illowsky R, Better contextual matching. The Inside AdSense Blog. 10 February 2010, available at http://adsense.blogspot.com/2010/02/better-contextual-matching.html. Accessed 31 August 2011.) The search history that is connected to a Google account is not added to a profile however: "Your ads preferences are not linked to your Google search history, Gmail, or other Google Account information in any way. Your ads preferences, including your custom list of interest and demographic categories, are only associated with an advertising cookie that's stored in your browser." Google Ads Preferences. Frequently Asked Questions. www.google.com/ads/preferences/html/faq.html. Accessed 31 August 2011.

[23] Anguelov et al. 2010

[24] See for example: Louvre, Another Way to Visit the Louvre..., available at www.louvre.fr/llv/musee/visite_virtuelle.jsp?bmLocale=en. Accessed 31 August 2011.

[25] YouTube, www.youtube.com; Google Translate, www.translate.google.com; Google Earth, www.earth.google.com; Google Labs Mars, www.google.com/mars. See also Google Mobile. Google Sky Map (beta), www.google.com/mobile/skymap. All accessed 31 August 2011.

larger than life, specifically legal problems, since law has a tendency to preserve rather than to change.

First some basic facts are provided. Street View was launched in May 2007 and allows users 360° horizontal and 290° vertical panoramic street level views.[26] In this sense, it is different from Google Earth, which makes it possible to zoom in on the earth from a bird's view perspective. With Street View, one sees the world through the eyes of the virtual person Pegman. Street View allows for zooming in on specific details, for the identification of a rare flower or the face of a man leaving a strip club.[27] One may also click on a direction in the street and encourage Pegman to take a nice walk. Street View is active in every continent and although the 'Western' countries appear to be on the top of Google's wish list, in time, the whole world may be engulfed by it.[28] Biker tracks and ski slopes are covered by bikes and snow mobiles.[29]

Google's Street View cars have intercepted Internet traffic, including some email messages and passwords, transmitted via Wi-Fi networks, when driving around in neighbourhoods. After investigations by German Data Protection Authorities, Google acknowledged this problem. In a number of countries, investigations have been initiated to determine whether or not Google is violating privacy law, and many regulators concluded that it did.[30] Although it might be somewhat exaggerated to call Google's collection of Wi-Fi data "the largest privacy breach in history across Western democracies", this phenomenon is problematic.[31] The interception of Wi-Fi data is not discussed here *in extenso*.

4.2. Data Protection Directive

There are several major legal instruments on privacy related matters in the European Union (EU).[32] Firstly article 8 of the European Convention on Human Rights and article 7 of the Charter of Fundamental Rights of the European Union (EU Charter) provide that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8 of the EU Charter provides a separate fundamental right to data protection:

> "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

---

[26] Williams M, Google maps. Behind the scenes, available at www.google.com/intl/en_us/help/maps/streetview/behind-the-scenes.html. Accessed 31 August 2011.

[27] Schroeder S, Top 15 Google Street View sightings. Mashable. 31 May 2007, available at http://mashable.com/2007/05/31/top-15-google-street-view-sightings. Accessed 31 August 2011.

[28] Google maps, Where are our vehicles currently driving?, available at http://maps.google.com/help/maps/streetview/learn/where-is-street-view.html. Accessed 31 August 2011.

[29] Google Maps, Cars, Trikes & More, available at http://maps.google.com/help/maps/streetview/technology/cars-trikes.html. Accessed 31 August 2011.

[30] See for an overview of national investigations of Google Street View: Electronic Privacy Information Center, Investigations of Google Street View, available at www.epic.org/privacy/streetview. Accessed 31 August 2011. See for the legal framework applicable to geolocation services: Article 29 Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185)*. 16 May 2011.

[31] Australian Minister of Communications Conroy. Senate. Environment, communications and the arts legislation committee, Budget Estimates, p 159, available at www.aph.gov.au/hansard/senate/commttee/S13005.pdf. Accessed 31 August 2011.

[32] For easy of reading, this chapter uses the phrases "EU" and "Community", also when the European Economic Area is meant.

> Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority."

This chapter focuses on the Data Protection Directive (Directive), which is the general instrument regulating the fair and lawful data processing of personal data. This chapter does not go into detail about specific implementations in Member States, but focuses instead on the Directive. Not all provisions of the Directive are discussed. The Directive contains an exemption for purposes of journalism, in particular in the audiovisual field, to reconcile the fundamental rights of individuals with the right to receive and impart information.[33] Although this may be relevant for Google, an in-depth discussion of this exemption falls outside the scope of this chapter. The right to freedom of expression is not discussed extensively in this chapter either.[34] Rights with regard to the commercial exploitation of one's portrait are not discussed in this chapter. The chapter does not discuss the e-Privacy Directive, which regulates data protection in the telecommunications sector and contains specific rules regarding the use of cookies and similar devices.[35]

When discussing the application of the Data Protection Directive, the opinions of the Article 29 Working Party are taken into account. The Working Party is an advisory body to the European Commission on data protection matters. It publishes opinions on all matters relating to the protection of persons with regard to the processing of personal data in the EU. The opinions of the Working Party are not legally binding. Nevertheless they are influential, since the Working Party consists of representatives of the data protection authorities of the Member States, and usually takes decisions by consensus.[36]

4.2.1 Applicability of the Data Protection Directive

4.2.1.1 Data Protection Directive

The Data Protection Directive protects the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.[37] The applicability of the Directive is triggered when "personal data" are "processed" under the authority of the "controller" of the personal data.[38] Personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or

---

[33] Article 9 and recital 37 of the Data Protection Directive.
[34] See about freedom of expression and the Data protection Directive: ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*", para 90; ECJ 16 December 2008, Case C-73/07, "*Satamedia*", para 56 and 62.
[35] Directive 2002/58 of 12 July 2002 concerning the processing off personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC.
[36] Article 29 and 30 of the Data Protection Directive; Poullet & Gutwirth 2008.
[37] Article 1.1 of the Data Protection Directive.
[38] Article 2(d) of the Data Protection Directive.

social identity".[39] The Working Party has elaborated on four elements of the definition: "any information", "relating to", "an identified or identifiable" and "natural person".[40] The information in question might relate either to objective or subjective information and might be kept in any form to be relevant for the Directive. Information may relate to a person either qua "content", such as medical records, qua "purpose", if it is used to evaluate or influence personal behaviour, or qua "result", if the consequence is that a person might be treated or looked upon differently.[41] Personal data may either be directly identifiable, such as a name, or indirectly, such as a telephone number.[42] To determine whether a person is identifiable, all the means likely reasonably to be used either by the controller or by any other person to identify a person should be taken into account.[43]

The concept of data processing is defined very broadly as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[44] In short, almost everything that can be done with personal data falls within this definition.

The Directive makes a distinction with regard to the actors processing the personal data. First there is the so called "data controller", which is defined as anybody who alone or jointly with others determines the purposes and means of the processing of personal data. On him lie all the obligations under the Directive. A party that processes personal data on behalf of the controller is called the processor and has limited obligations under the Directive.[45]

The Directive distinguishes between non-sensitive data and sensitive data. The latter are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health and sex life. There is a stricter regime with regard to the processing of sensitive data than there is with regard to non-sensitive data.[46]

4.2.1.2 Behavioural Advertising

The first question that needs to be answered is whether personal data are processed for the behavioural advertising program. Google says that it "does not know Mary's name or any other personal information about her. Google simply recognizes the number stored in Mary's browser, and shows ads related to the interest and inferred demographic categories associated with her cookie."[47] Perhaps Google assumes that because it does not collect a "name or any other personal information", it does not collect "personal data" as defined in the Directive, and that thus the Directive does not apply. Google defines "personal information" as "information that you provide to us which personally identifies you, such as your name, email address or billing

[39] Article 2(a) of the Data Protection Directive.
[40] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data (WP 136)*. 20 June 2007
[41] *Idem*, p 10.
[42] *Idem*, p 12-13.
[43] Recital 26 of the Data Protection Directive.
[44] Article 2(b) of the Data Protection Directive.
[45] Article 2(e) of the Data Protection Directive.
[46] Article 8.1 of the Data Protection Directive. This chapter uses the phrase 'sensitive data', while the Directive uses 'special categories of personal data'.
[47] Google Ads Preferences, Interest-based advertising: How it works, available at www.google.com/ads/preferences/html/about.html. Accessed 31 August 2011.

information, or other data which can be reasonably linked to such information *by Google*" (emphasis added).[48] This definition is narrower than the Directive's definition of "personal data".[49] Google says that it does not "collect or serve ads based on personally identifying information without your permission."[50]

However, it is not decisive whether Google adds a name to a profile or not, as the Directive regards data that *can* lead to the identification of a person as personal data.[51] All the means that can reasonably be used by the controller *or any other person* to identify a person are relevant to determine whether a person is identifiable,[52] and it is often possible to tie "anonymous" information to a name.[53] According to the Working Party, behavioural advertising usually entails the processing of personal data, as a cookie can be used to "single out" one individual within a group.[54] After all, the profiles are built with the intention to target advertising to a specific (albeit nameless) Internet user. The purpose of behavioural advertising is influencing behaviour, as Google and advertisers hope that the targeted Internet users will respond to advertising. The discussion about cookie-based profiles resembles the ongoing discussion about IP addresses. The Working Party is of the opinion that IP addresses usually are personal data.[55] Many, including Google, do not agree: "IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings."[56] The matter is contentious, but many judges and data protection authorities in Europe tend to agree with the Working Party and consider IP addresses to be personal data.[57] It seems safe to assume that profiles tied to cookies or IP addresses should be regarded as personal data in most cases.

According to Google, it "will not associate sensitive interest categories with the anonymous ID (such as those based on race, religion, sexual orientation, health, or sensitive financial categories) and will not use these categories when showing you interest-based ads."[58] Google's description of sensitive interest categories resembles the Directive's definition of sensitive personal data, but Google does not mention trade union membership or political opinions. For its behavioural advertising program, Google can associate one's cookie with more

---

[48] Google Privacy Center. Privacy FAQ, available at www.google.com/intl/en/privacy/faq.html. Accessed 31 August 2011.

[49] See also: Lawford J, Lo J (2010) Consumer Privacy Consultations – Comments of PIAC. Public Interest Advocacy Centre (Canada). 15 March 2010. www.piac.ca/files/piac_comments_onlinetrackingconsultation.pdf. Accessed 31 August 2011.

[50] Google Privacy Center, Advertising and Privacy, available at www.google.com/privacy/ads. Accessed 31 August 2011.

[51] Bygrave 2002, p 318; Korff 2010, p 53; Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising (WP 171)*. 22 June 2010, p 9; *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, p 12-21.

[52] Recital 26 of the Data Protection Directive. Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, p 14.

[53] Ohm 2009; Toubiana & Nissenbaum 2011.

[54] Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising (WP 171)*. 22 June 2010, para 3.2.2.

[55] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, para 4.1.2.

[56] Whitten A, Are IP addresses personal? Google Public Policy Blog. 22 February 2008, available at http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html. Accessed 31 August 2011.

[57] Kuner et al. 2009; Kuner et al. 2010. The Advocate General of the ECJ is also of the opinion IP addresses are personal data (AG Opinion 14 April 2011, Case C-70/10, "*Scarlet/Sabam"*, para 75-78).

[58] Google Privacy Center. Privacy Policy for Google Ads and the Google Display Network. 29 September 2010, available at www.google.com/privacy/ads/privacy-policy.html. Accessed 31 August 2011.

than 1000 categories.[59] Although some might say that certain categories are sensitive, such as the category "parenting", with sub category "adoption", there are no categories that squarely fall within the Directive's definition of sensitive data.[60] Nevertheless, adding the category "unions & labor movement" to a profile could be considered processing of personal data regarding political opinion. Someone's interest in the "labor movement" can imply a certain political opinion.

Furthermore, much depends on the question on which sites Google tracks browsing behaviour. Does Google process data concerning religion if it tracks daily visits to a website with kosher recipes?[61] However, when compared to other players in this field, Google stays away reasonably well from data that are considered sensitive in the Directive. Many other companies that engage in behavioural advertising are less restrained and target advertising based on categories such as "U.S. Hispanics",[62] "democrats", "Methodists",[63] or "cardiovascular general health".[64] Still, as the category "sensitive data" must not be interpreted narrowly, it could be argued that Google processes sensitive data.[65]

The collection and analysis of personal data of Internet users is a process that falls within the definition of processing of personal data in the Directive.[66] Google is the controller as it determines the goal of the processing, targeted advertising, and the means by which the data are processed, such as determining the data mining techniques. In short, the Directive is applicable.

4.2.1.3 Google Street View

Techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, fall under the scope of the Directive.[67] Hence, photographs with people that are processed for Google Street View fall under the scope of the Directive. Although the processing of personal data, photographs showing people, is not the goal of Street View, it is inherent to an online mapping service.[68] When Google registers and stores photographs with directly identifiable information, such as an individual's face, it processes personal data. However, Google erases most directly identifiable information.

---

[59] Krafcik J, Reach your audience with interest categories. Google Inside AdWords. 23 June 2011, available at http://adwords.blogspot.com/2011/06/reach-your-audience-with-interest.html. Accessed 31 August 2011.

[60] There is some debate about the question of whether the Directive lists categories of sensitive data exhaustively or not (Bygrave 2002, p 344).

[61] See e.g. Allrecepies.com, working with DoubleClick cookies (Privacy policy 2 February 2011), http://allrecipes.com//Help/aboutus/Privacy.aspx. Accessed 31 August 2011.

[62] Batanga Network Inc, About us, available at www.batanganetwork.com/about-us. Accessed 31 August 2011.

[63] Graham R, Laredo Group, Getting Started with Behavioral Targeting (promotional video), available at www.youtube.com/watch?v=rqpd3O239qI. Accessed 31 August 2011.

[64] Yahoo! Privacy, All Standard Categories, available at http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/asc/details.html. Accessed 31 August 2011.

[65] The European Court of Justice has ruled that "the expression 'data concerning health' (…) must be given a wide interpretation". In this light, the category 'sensitive data' must not be interpreted narrowly (ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*").

[66] Article 2 (b) and 3.1 of the Data Protection Directive.

[67] Recital 14 of the Data Protection Directive.

[68] Commission for the Protection of Privacy Belgium (2010) recommendation on mobile mapping, 05/2010, 15 December 2010, available at www.privacycommission.be/en/static/pdf/recommendation-05-2010.pdf para 20.

> "We have developed cutting-edge face and license plate blurring technology that is applied to all Street View images. This means that if one of our images contains an identifiable face (for example, that of a passer-by on the pavement) or an identifiable license plate, our technology will blur it automatically, meaning that the individual or the vehicle cannot be identified. If our detectors missed something, you can easily let us know."[69]

Photographs of people make them identifiable, not only with regard to their faces but also with regard to their exceptional height, clothes, hair colour, physical handicaps or any other characteristics.[70] Photographs of people with a blurred face can constitute indirectly identifiable information, for example when they are entering their own home. Different data put together (neighbourhood, colour of a car and a man seen knocking on a door) might paint a detailed picture (for example a man secretly visiting his ex-girlfriend's house) and can also constitute indirectly identifiable information.[71] The Swiss Data Protection Commissioner has stated: "In outlying districts, where there are far fewer people on the streets, the simple blurring of faces is no longer sufficient to conceal identities."[72] Hence, the elements of "identified" or "identifiable" are often satisfied with regard to the photographs shown on Google Street View. Furthermore, the information relates to a "natural person" since it relates to the people walking, driving or standing in the streets. Thus, not all data protection authorities fully agree with the statement on the private blog of Peter Fleischer, Google's Global Privacy Counsel.[73] He does not think a person should be regarded as identifiable if the face is not visible.

> "Basically, Street View is going to try not to capture "identifiable faces or identifiable license plates" in its versions in places where the privacy laws probably wouldn't allow them (absent consent from the data subjects, which is logistically impossible), in other words, in places like Canada and much of Europe. And for most people, that pretty much solves the issue. If you can't identify a person's face, then that person is not an "identifiable" human being in privacy law terms. If you can't identify a license plate number, then that car is not something that can be linked to an identifiable human being in privacy law terms. (…)
>
> Some privacy advocates raise the question of how to circumscribe the limits of "identifiability". Can a person be considered to be identifiable, even if you cannot see their face? In pragmatic terms, and in privacy law terms, I think not. The fact is that a person may be identifiable to someone who already knows them, on the basis of their

[69] Google Maps, Privacy, available at http://maps.google.co.uk/intl/en_uk/help/maps/streetview/privacy.html. Accessed 31 August 2011.
[70] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, example 19.
[71] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, p 13.
[72] Federal Data Protection and Information Commissioner, Street View: FDPIC takes Google to the Federal Administrative Court, available at www.edoeb.admin.ch/dokumentation/00438/00465/01676/01683/index.html?lang=en. Accessed 31 August 2011.
[73] The statements on this blog should not be attributed to Google: "Since I work as Google's Global Privacy Counsel, I need to point out that these ruminations are mine, not Google's. Please don't attribute them to Google, because they're just my views, and many people at Google may hold different views on the same topics." http://peterfleischer.blogspot.com. Accessed 31 August 2011.

clothes (e.g., wearing a red coat), plus context (in front of a particular building), but they wouldn't be "identifiable" to anyone in general. (…)"[74]

However, the Directive states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[75] It is correct that most people with blurred faces will not be identifiable in most cases by most of the people. Still, some people might be identifiable, due to their unique qualities, such as celebrity status or remarkable body features. Moreover, many people with blurred faces will be identifiable by some of their close ones.[76] To refer to the famous quote attributed to Abraham Lincoln: "you cannot identify all the people all the time, but you can identify some of the people all the time and all of the people some of the time."[77]

Finally, the photographs shown on Street View may include sensitive data, such as data referring to race (with regard to the colour of the skin), religion (when walking out of a mosque), or sexual preferences (when walking out of a gay-bar).[78] For example, in a case between Google and the Federal Data Protection and Information Commissioner in Switzerland, the Federal Administrative Court ruled that in photographs of for example hospitals or prisons, not only faces but also features such as skin colour and clothing have to be blurred.[79]

In its notification to the Dutch Data Protection Authority, Google confirms processing sensitive data for the original unblurred photographs for its Street View service, both with regard to race and ethnicity and with regard to health related information. According to the notification, Google processes the photographs (personal data) to use them in anonymized form for Street View.[80] It is not certain, but it seems that Google only regards the photographs as personal data before the faces are blurred.[81]

The personal data are processed by Google since it collects, records, organizes, stores, adapts and alters data. As far as the blurred photographs contain personal data, Google discloses personal data to the public.[82] Google is the controller as it determines the goal and the means of the data processing, since it determines the techniques for processing and publication. In sum, Google processes personal data for Street View. In principle, the Directive applies.

---

[74] Fleischer P, Can you "identify" the person walking down the street? Peter Fleischer: Privacy...? 23 October 2007, available at http://peterfleischer.blogspot.com/2007/10/can-you-identify-person-walking-down.html. Accessed 31 August 2011.

[75] Recital 26 of the Data Protection Directive.

[76] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, p 21.

[77] It is doubtful whether Lincoln ever said this (Parker D B, A New Look at "You Can Fool All of the People". For The People, A Newsletter of the Abraham Lincoln Association, available at http://abrahamlincolnassociation.org/Newsletters/7-3.pdf. Accessed 31 August 2011.

[78] Cf. Commission for the Protection of Privacy Belgium (2010) recommendation on mobile mapping, 05/2010, 15 December 2010, available at www.privacycommission.be/en/static/pdf/recommendation-05-2010.pdf, para 6.

[79] Federal Administrative Court Switzerland 20 March 2011, Case A-7040/2009, *"Eidgenössischer Datenschutz- und Öffentlichkeitsbeauf-tragter EDÖB vs. Google Inc. And Google Switzerland GmbH"*, Computer Law Review International 3/2011, p. 87-89.

[80] Notification of Google Street View to the Dutch Data Protection Authority, available at www.cbpweb.nl/asp/ORDetail.asp?moid=808084898f&refer=true&theme=purple. Accessed 31 August 2011.

[81] See about anonymous data: Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). 20 June 2007, p 18-21.

[82] See also ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*" para 24-27.

4.2.2 Jurisdiction

4.2.2.1 Data Protection Directive

This section discusses whether the Directive applies to Google, an American company.[83] The national provisions of each Member State apply to the processing of personal data in three circumstances. Firstly, the national provisions based on the Directive apply when processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. When the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.[84] Thus, the first circumstance under which the Directive applies is fulfilled when two criteria are met: "an establishment of the controller on the territory of the Member State" and "processing is carried out in the context of the activities." According to the European Court of Justice, an establishment requires "the permanent presence of both the human and technical resources necessary for the provision of [the] services".[85] This may be taken as a guideline for interpretation, says the Working Party. An establishment does not need to have a legal personality. With regard to the second criterion, relevant factors are the degree of involvement of the establishment(s) in the activities in the context of which personal data are processed, the nature of the activities of the establishments and whether an activity involves data processing or not. According to the Working Party, "the decisive element to qualify an establishment under the Directive is the effective and real exercise of activities in the context of which personal data are processed."[86] When applying the criteria, the goal of the Directive, an adequate protection of personal data, has to be taken into account.[87]

Secondly, the national provisions based on the Directive apply when the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law. An example where this criterion might be satisfied is the case of a foreign embassy.[88] This criterion is not relevant in the case of Google.

The final circumstance in which the national provisions based on the Directive apply, is when the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of a Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[89] This last circumstance consists of four elements: "the controller is not established on Community territory", "and for purposes of processing personal data makes use of equipment, automated or otherwise situated on the territory of the Member State", "unless used only for purposes of transit through Community territory" and "must designate a representative established on the Member State's territory".[90] The criterion that "the controller is not established on Community territory" refers to the first circumstance, in which the processing is carried out in the context of the activities of an establishment of the controller on the territory

---

[83] This section is largely based on Article 29 Working Party, *Opinion 8/2010 on applicable law (WP 179)*. 16 December 2010. The thorny question of which national law applies falls outside the scope of this chapter.
[84] Article 4.1(a) of the Data Protection Directive.
[85] ECJ 4 July 1985, Case C-168/84, "*Berkholz*".
[86] Article 29 Working Party, *Opinion 8/2010 on applicable law (WP 179)*. 16 December 2010, p 11.
[87] *Idem*, p 14.
[88] Article 4.1(b) of the Data Protection Directive; Article 29 Working Party, *Opinion 8/2010 on applicable law (WP 179)*. 16 December 2010, p 18, example nr. 6.
[89] Article 4.1(c) of the Data Protection Directive.
[90] Article 29 Working Party, *Opinion 8/2010 on applicable law (WP 179)*. 16 December 2010, p 18-25.

of the Member State. The third circumstance thus only applies if the first one does not. For the second criterion, the controller needs to make use of the equipment on the territory of a Member State. The third criterion, "unless used only for purposes of transit through Community territory", refers to pure transmission services.[91] The final element is the obligation to designate a representative established on the Member State's territory, which is responsible for the activities of the controller throughout the Community's territory.[92]

4.2.2.2 Behavioural advertising

As Google is an American company, a relevant question is whether the Directive applies at all to its behavioural advertising program. Is the processing carried out in the context of an establishment of Google on the territory of a Member State? Google has several offices in Europe. In an opinion regarding search engines, the Working Party has mentioned some factors to take into account when deciding if an establishment plays a relevant role in the data processing. For example, a relevant factor is whether a search engine provider complies with requests from the courts of a Member State. Another relevant factor is whether a search engine provider has an office in a Member State from where it sells advertising targeted to the Member State's inhabitants.[93] In many Member States such factors may apply to Google.

The third circumstance is also applicable. Google has several data centres in Member States, so it makes use of equipment on Community territory. Furthermore, the Working Party has said several times that the Directive is applicable if companies store information on the computer of an Internet user which is located in a Member State, for example when companies use cookies, web bugs or Javascript.[94] "The use of cookies and similar software devices by an online service provider can also be seen as the use of equipment in the Member State's territory, thus invoking that Member State's data protection law. (…) [T]he user's PC can be viewed as equipment in the sense of [the Data Protection Directive]."[95] In short: because Google places a cookie on computers of Internet users within the EU, the Directive applies. According to Google however, "concluding that a non-EEA controller is subject to the laws of every EEA member state as a result of the existence of a file in the terminal equipment of its EEA-based users seems very far fetched and beyond the aims of the Data Protection Directive."[96] Nevertheless, the Working Party is clearly of the opinion that the Directive applies to Google's behavioural advertising service.[97]

---

[91] *Idem*, p 23.

[92] This is however without prejudice to legal actions against the controller himself. This was made clear, for example, in the controversial case of "*Italy v. Google*", before the *Tribunale Ordinario di Milano*, 24 February 2010, De Leon & Vivi Down/Google, available at http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf. Accessed 31 August 2011.

[93] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 9 -12.

[94] Article 29 Working Party, *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 (WP56)*, 30 may 2002, p 10-11, case A and B.

[95] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, para 4.1.2.

[96] Google, Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines, 8 September 2008, p. 13, available at www.scribd.com/doc/5625427/google-ogb-article29-response. Accessed 31 August 2011.

[97] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 9-12; Article 29 Working Party, Letter to CEO of Google, 26 May 2010, available at

4.2.2.3 Google Street View

Does Google Street View fall under the scope of the Directive? As is the case with the behavioural advertising program, the first circumstance may often be applicable to Google: the processing is carried out in the context of the activities of an establishment of Google in a Member State. The third circumstance under which the Directive could apply is also applicable. Google makes use of equipment, situated on the territory of the Member State, namely cars, camera equipment and processing tools, for the purpose of processing data. The equipment is not solely used to transfer data through Community territory. The Working Party wrote a Street View specific example in its opinion with regard to this requirement.

> "A company located in New Zealand uses cars globally, including in EU Member States, to collect information on Wi-Fi access points (including information about private terminal equipment of individuals) in order to provide a geo-location service to its clients. Such activity involves in many cases the processing of personal data. The application of the Data Protection Directive will be triggered in two ways:
>
> - First, the cars collecting Wi-Fi information while circulating on the streets can be considered as equipment (…);
> - Second, while providing the geo-location service to individuals, the controller will also use the mobile device of the individual (through dedicated software installed in the device) as equipment to provide actual information on the location of the device and of its user. Both the collection of information with a view to provide the service, and the provision of the geo-location service itself, will have to comply with the provisions of the Directive."[98]

In short, the Directive is applicable on Street View, even though Google is an American company.

4.2.3. Principles Relating to Data Quality

4.2.3.1. Data Protection Directive

The Directive lays down several rules under the heading "Principles relating to data quality".[99] The rather open norm that personal data must be processed "fairly and lawfully" is the overarching requirement of the Directive.[100] "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[101] Data processing must abide by the purpose limitation principle, which stipulates that personal data must be "collected for specified, explicit and legitimate purposes and

---

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf. Accessed 31 August 2011.

[98] Article 29 Working Party, *Opinion 8/2010 on applicable law (WP 179)*. 16 December 2010, p 21.

[99] Article 6 of the Data Protection Directive.

[100] Article 6.1(a) of the Data Protection Directive.

[101] Article 8 of the Charter of Fundamental Rights of the European Union.

not further processed in a way incompatible with those purposes".[102] Not all Member States interpret "incompatible purpose" in the same way.[103] The Directive also requires that data should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified, having regard to the purposes for which they were collected or for which they are further processed.[104]

Data minimization is a core principle of the Directive. Although the principle is not laid down explicitly in the text, several requirements in the Directive together express the data minimization principle.[105] Firstly, personal data shall only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive in relation to the specific purpose for which they are collected or further processed.[106] Secondly, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the specific purpose for which the data were collected or for which they are further processed.[107] Thirdly, the word "necessary" in for example the phrase "data may be processed only if (…) processing is necessary for the performance of a contract" implies that the amount of processed data should be kept to a minimum as well.[108] Collecting data because they might prove useful in the future would be in breach of both the purpose limitation principle and the data minimization principle. Finally, according to the European Court of Justice, the provisions of the Directive "must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures".[109] Hence, the European Convention on Human Rights and related case-law of the European Court of Human Rights should be considered when applying the Directive. As the proportionality principle takes a central position in this case-law, all data processing must comply with this principle.[110] A controller should always assess whether it is possible to achieve the purpose with less data.

4.2.3.2 Behavioural Advertising

To establish whether the data processing for behavioural advertising is legitimate, the first question is whether Google has a specified and explicit purpose. Google writes:

> "How we use the DoubleClick cookie information. We use the advertising cookie information collected on AdSense partner sites and certain Google sites to: (…) Enable the following ad serving features: (…) Interest-Based Advertising: Allows advertisers (including Google) to serve ads to users on AdSense partner sites and certain Google services based on online activity and interests associated with the DoubleClick cookie and to serve subsequent ads to you after you leave that advertiser's website."[111]

---

[102] Article 6.1(b) of the Data Protection Directive.
[103] Kuner 2007, p 100
[104] Article 6.1(d) of the Data Protection Directive.
[105] Cf. Bygrave 2002 , pp 341-348
[106] Article 6.1(c) of the Data Protection Directive.
[107] Article 6.1(d) of the Data Protection Directive.
[108] Article 7.1(b) of the Data Protection Directive. See also Bygrave 2002 p 341
[109] ECJ 20 May 2003, Cases C-465/00, C-138/01 and C-139/01 "*Österreichischer Rundfunk*", para 68. See also ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*" para 87 and 90.
[110] ECJ 29 January 2008, Case C-275/06, "*Promusicae*", para 68–70.
[111] Google Privacy Center, Privacy Policy for Google Ads and the Google Display Network, 29 September 2010, available at www.google.com/privacy/ads/privacy-policy.html. Accessed 31 August 2011. See also Google's main

According to the Working party however, "the offering of personalized advertising" is not a sufficiently specified purpose, especially when a company also mentions other purposes for the same data.[112] As Google lists more purposes than just behavioural advertising, data protection authorities might not regard the purpose as sufficiently specified and explicit.

With regards to the accuracy of data, there is an inherent problem of profiling. For example, not everybody who lives in a poor town is a credit risk. An Internet user that visits websites about adoption or cars might be doing research for somebody else. Although sophisticated data mining software might be able to ignore certain false signals, wrongly inferred interests could be added to a behavioural profile. Google mitigates this problem by allowing users to edit their profile.[113]

The question of how Google's behavioural advertising program should be judged in the light of the data minimization principle is difficult to answer, as it is not completely clear which data Google adds to a behavioural profile. An analysis of almost 400,000 unique domains by Gomez et al. showed that Google would be able to track browsing behaviour on 88% of the tested domains.[114] Many websites have installed Google Analytics for example. However, this does not mean that Google enriches behavioural profiles with all these data. For Google Analytics, "[a] different cookie is used for each website, and visitors are not tracked across multiple sites."[115] Google's privacy policies preclude Google from adding a name or data from a Google account to a behavioural profile.[116] But, when an Internet user registers for a Google service (such as Gmail), Google reserves the right to combine that information with information it gathers from other sources.[117]

One of the most sensitive databases Google holds is the database with search queries. As Google stated in a court case: "There are ways in which a search query alone may reveal personally identifying information."[118] Google targets advertising based upon earlier searches for

---

Privacy Policy: "We use cookies to improve (…) ad selection, and tracking user trends, such as how people search. Google also uses cookies in its advertising services to help advertisers and publishers serve and manage ads across the web and on Google services." (Available at www.google.com/privacy/privacy-policy.html. Accessed 31 August 2011.)

[112] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 16.

[113] See para 2.5.2.

[114] Gomez et al. 2009 p 27

[115] http://www.google.com/privacy/ads. Accessed 31 August 2011. Accessed 31 August 2011. See also Google Ads Preferences, Interest-based advertising: How it works, available at www.google.com/ads/preferences/html/about.html. Accessed 31 August 2011.

[116] Google's Knol service (an online encyclopedia) is an exception. "Similar to other web services, Google records information such as account activity (e.g., storage usage, number of log-ins, actions taken), data displayed or clicked in the Knol interface (including UI elements, settings, and other information), and other log information (e.g., browser type, IP address, date and time of access, cookie ID, referrer URL). If you are logged in we may associate that information with your account." (Emphasis added). http://knol.google.com/k/privacy-policy. Accessed 31 August 2011. See Toubiana V, A follow up on Google policies. Unsearcher. 15 June 2011, available at http://unsearcher.org/a-follow-up-on-google-policies. Accessed 31 August 2011.

[117] Google Privacy Center, Privacy Policy. "We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services." www.google.com/privacy/privacy-policy.html. Accessed 31 August 2011.

[118] Declaration of Matt Cutts in "*Gonzales v. Google*", 234 F.R.D. 674 (N.D. Cal. 2006) p 9, available at http://docs.justia.com/cases/federal/district-courts/california/candce/5:2006mc80006/175448/14/0.pdf. Accessed 31 August 2011.

"a short period of time (a few hours)".[119] It is difficult to deduce how much data are added to behavioural advertising profiles for this feature. It is obvious that Google tracks the surfing behaviour of Internet users over a large number of websites and that these data are added to the behavioural profile. Furthermore, many data are gathered and added to a behavioural profile when one watches YouTube videos, as becomes clear from the following sentences from YouTube's privacy policy.

> "YouTube is owned by Google and YouTube and Google share the same cookie technology in determining user interests."
> "As you watch videos, or take actions (such as uploading) YouTube stores an advertising cookie in your browser to understand the types of videos you watch."
> "Additionally, YouTube uses information based on the type of pages you visit on websites that are members of the Google content network."[120]

The statement that YouTube stores a cookie to understand what kind of videos an Internet user watches is somewhat confusing, when read together with Google's statements that it never ties a registered profile to a cookie-based behavioural profile. It is impossible to upload videos on YouTube without a registered profile. Google stores a cookie on the computer of an Internet user when he uploads a video to YouTube (this Internet user is logged into a Google service by definition). Perhaps the foregoing means that Google immediately separates data from the registered YouTube profile from data about which videos one watches or uploads. Since March 2010, Google also offers advertisers the chance to "retarget" Internet users. Google explains it as follows:

> "Here's an example of how it works. Let's say you're a basketball team with tickets that you want to sell. You can put a piece of code on the tickets page of your website, which will let you later show relevant ticket ads (such as last minute discounts) to everyone who has visited that page, as they subsequently browse sites in the Google Content Network. In addition to your own site, you can also remarket to users who visited your YouTube brand channel or clicked your YouTube homepage ad."[121]

In short, a retargeted advertisement "follows" a user around, for example after a user did not finish an online purchase. It is unclear what amount of data is added to the behavioural profile for this retargeting feature.

The requirement that personal data should not be kept longer than necessary for the specific purpose for which the data were collected or for which they are further processed is a rather open norm. In an opinion about search engines, the Working Party elaborated on how long search logs can be kept, and said that a longer retention period than six months could not

---

[119] Illowsky R, Better contextual matching. The Inside AdSense Blog. 10 February 2010, available at http://adsense.blogspot.com/2010/02/better-contextual-matching.html. Accessed 31 August 2011.
Google Ads Preferences. Frequently Asked Questions. www.google.com/ads/preferences/html/faq.html. Accessed 31 August 2011.

[120] YouTube Advertising and You, available at www.youtube.com/t/interest_based_ads. Accessed 31 August 2011. The Google Content Network is the old name for the Google Display Network.

[121] Weinberg A, Now available: Reach the right audience through remarketing. Google Inside Adwords. 25 March 2010, available at http://adwords.blogspot.com/2010/03/now-available-reach-right-audience.html. Accessed 31 August 2011.

easily be justified.[122] However, Google's privacy policies do not make clear how long a behavioural profile is kept. Most of Google's cookies expire in about 2 years, but some of them expire in 2038.[123] Furthermore, a cookie can be refreshed whenever an Internet user passes one of the millions of websites within Google's reach. According to Google however, a profile is lost when a user deletes the Google cookies or switches over to another browser.[124]

Some tentative conclusions can be drawn about which data Google adds to the behavioural profiles. Google's privacy policies preclude Google from adding a name or a registered profile to a cookie-based behavioural profile. But, Google does add the surfing behaviour over Google services and millions of websites to the profile, and enriches profiles with YouTube viewing data. Making an educated guess about the lifespan of behavioural profiles is difficult. Hence, Google may not comply with the data minimization principle. The Working Party does not regard the purpose of the personal data processed for the cookie-based profiles as sufficiently specified and explicit.

4.2.3.3. Google Street View

With regard to Google Street View, personal data are gathered and processed for a specified and explicit purpose, namely, for the functioning of the Street View service, a cartography service that lets the public explore the world.[125] However, since the photographs of people with blurred faces are out in the open, all kinds of parties can use the personal data in Street View for their own purposes.[126] Personal data may not be further processed in a way that is incompatible with the original purpose and Google is responsible for publishing the data on the Internet. As Google can neither check nor control for which purposes third parties might use the photographs published on Street View, questions regarding the purpose limitation principle may arise.[127]

To understand whether Google lives up to its requirements with regard to the data minimization principle, the exact purposes for processing have to be established. In Google's notification to the Dutch Data Protection Authority, the purpose is described as taking panoramic photographs of public roads by means of camera cars, with the purpose of integrating these photographs in anonymized form into Google's Street View service.[128]

---

[122] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 19. Toubiana & Nissenbaum doubt whether the search logs are sufficiently anonymized (Toubiana & Nissenbaum 2011).

[123] The cookies that Google Scholar stored on the computer of one of the authors of this chapter have an expiry date in 2038.

[124] Google Ads Preferences. Frequently Asked Questions, available at http://www.google.com/ads/preferences/html/faq.html. Accessed 31 August 2011.

[125] Information Commissioner's Office, *Google Inc.'s Notification for Street View*. Registration number Z2451429, available at www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=4923359. Accessed 31 August 2011.

[126] See Rundle 2011 et al; Burdon 2010, para III. See also Mayer-Schönberger, who mentions the possibility of websites asking the public to report crimes seen on Street View: "law enforcement entertainment". (Wiser G, Google plans to launch Street View in Germany by end of year, Deutsche Welle, 10 August 2010, available at www.dw-world.de/dw/article/0,,5887193,00.html. Accessed 31 August 2011).

[127] Cf. Kotschy 2010, p 52. Cf. the Article 29 Working Party in the context of social networks: "Personal data published on social network sites can be used by third parties for a wide variety of purposes, including commercial purposes, and may pose major risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm." (Article 29 Working Party, *Opinion 5/2009 on online social networking (WP163)*, 12 June 2009, p 4).

[128] *Notification of Google Street View to the Dutch Data Protection Authority*, available at www.cbpweb.nl/asp/ORDetail.asp?moid=808084898f&refer=true&theme=purple. Accessed 31 August 2011. The

Hence, the question is whether it is necessary for Google to process personal data. Although the processing of personal data is a side effect of Street View, this question must be answered positively, since the Directive defines personal data very broadly.[129] Personal details, clothing and cars may indirectly lead to personal identification. Google has done a reasonable job to secure that the most direct and sensitive information is blurred, both with regard to faces and licence plates.

> "We have developed cutting-edge face and license plate blurring technology that is applied to all Street View images. This means that if one of our images contains an identifiable face (for example that of a passer-by on the sidewalk) or an identifiable license plate, our technology will automatically blur it out, meaning that the individual or the vehicle cannot be identified."[130]

There may be an issue with regard to the requirement to stop processing data when it is no longer necessary for the purposes for which the data were collected or for which they are further processed. This regards the unblurred images, faces and licence plates. Google keeps the unblurred photographs for up to one year, for testing applications that are used for the anonymization process and to "to build better maps products".[131] Members of the Working Party have asked Google to limit the period it keeps the unblurred photographs to six months.[132] Here, no definite answer to the question whether a shorter retention period would be possible can be given, since to a large extent the technological possibilities determine what is necessary and what is not. This information is however not publicly available.

Finally, Street View has published some incorrectly taken or processed photographs, which might come into conflict with the requirement of data accuracy. A further problem might be that some photographs may be outdated. **"**Our images show only what our vehicles were able to see on the day that they drove past the location. Afterwards, it takes at least a few months to process the collected images before they appear online. This means that images that you look at on Street View could be anywhere from a few months to a few years old."[133] But these are minor points. In brief, although there might be questions regarding the purpose limitation principle and the data minimization principle, Street View complies with most of the principles relating to data quality.

---

notification to the Information Commissioner's Office in the United Kingdom refers to the purpose 'cartography' (Information Commissioner's Office, *Google Inc.'s Notification for Street View, available at www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=4923359*. Accessed 31 August 2011).

[129] Commission for the Protection of Privacy Belgium (2010) recommendation on mobile mapping, 05/2010, 15 December 2010, available at www.privacycommission.be/en/static/pdf/recommendation-05-2010.pdf, para 20. Accessed 31 August 2011.

[130] Google Maps Privacy. http://maps.google.com/intl/en_us/help/maps/streetview/privacy.html. Accessed 31 August 2011.

[131] *Notification of Google Street View to the Dutch Data Protection Authority*, available at http://www.cbpweb.nl/asp/ORDetail.asp?moid=808084898f&refer=true&theme=purple. Accessed 31 August 2011; Fleischer P, Navigating Europe's Streets, Google European Public Policy Blog, 7 October 2009, available at http://googlepolicyeurope.blogspot.com/2009/10/navigating-europes-streets.html. Accessed 31 August 2011.

[132] EDRI, Article 29: Reduce The Storing Period Of Google Street View's Images. 10 March 2010, available at www.edri.org/edrigram/number8.5/article-29-wp-google-street-view. Accessed 31 August 2011.

[133] Google Maps Privacy. http://maps.google.com/intl/en_us/help/maps/streetview/privacy.html. Accessed 31 August 2011.

4.2.4. Legitimate Purpose and Purpose limitation

4.2.4.1. Data Protection Directive

The Directive requires that personal data are processed on a legitimate basis as laid down by law and offers six possibilities to comply with this requirement. Firstly, a data processor may process personal data if "the data subject has unambiguously given his consent".[134] Consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[135] Consent can be given implicitly, but according to the Working Party, doing nothing can almost never be construed as unambiguous consent.[136] Consent should be freely given, so consent given under pressure is not valid. As consent also has to be specific, consent "to use personal data for commercial purposes" is not acceptable for example.[137] Finally consent has to be informed.[138]

Secondly data processing is allowed when it is necessary for the performance of a contract. This is for example the case when one pays with a credit card: certain personal data have to be processed. Thirdly, processing is allowed if it is necessary for compliance with a legal obligation to which the controller is subject. Fourthly, processing is allowed if it is necessary in order to protect the vital interests of the data subject. Fifthly, processing is allowed if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.[139]

Finally, under the so called "balancing provision", data processing is allowed when the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (…)".[140] When balancing the interests of the controller and the data subject, it has to be taken into account that the right to privacy and data protection are fundamental rights. As the proportionality principle guides the interpretation of the Directive, relevant questions are whether the processing of data is proportional to the specified purpose and whether there is another way of pursuing the purpose. The balancing provision is notoriously vague, and not all legislators and data protection authorities interpret it in the same way.[141]

The Directive provides for a separate regime for the processing of sensitive data, such as data revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership and data concerning health or sex life. In principle, the processing of such sensitive data is prohibited. This prohibition can only be lifted if certain specified conditions are met, which can be summarized as follows. Firstly, it can be lifted if the data subject has given his "explicit consent" to the processing of those data, except where the laws of the Member State provide that

---

134 Article 7(a) of the Data Protection Directive
135 Article 2(h) of the Data Protection Directive
136 Article 29 Working Party, *Opinion 15/2011 on the definition of consent (WP 187).* 13 July 2011, p. 12. *1/2008 on data protection issues related to search engines (WP148).* 4 April 2008, p 17.
137 *Landgericht* Bonn, LG Bonn, Urteil vom 31.10.2006, Az. 11 O 66/06.
138 See about transparency and information duties: para 2.5.
139 Article 7(b), 7(c), 7(d) and 7(e) of the Data Protection Directive.
140 Article 7(f) of the Data Protection Directive.
141 See Korff 2010, p 72.

the prohibition may not be lifted by the data subject's giving his consent.[142] Secondly, processing of sensitive data is allowed if it is necessary to comply with employment law. Thirdly, processing is allowed if it is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving his consent. Fourthly, processing is allowed if it is carried out in the course of the legitimate activities of a non-profit-seeking body with for example a political or religious aim. Lastly, processing is allowed if it relates to data which are manifestly made public by the data subject.[143]

4.2.4.2 Behavioural Advertising

Like every controller, Google needs a legitimate basis for the use of personal data. There are no legal obligations for which the processing of personal data is necessary, and Google's behavioural advertising program does not serve the public interest or a vital interest of the data subject. Furthermore, Google cannot invoke a contractual relationship. Although search engine providers have suggested that the use of their service implies a contract on the basis of which they can process personal data for targeted advertising, the Working Party does not accept this reasoning.[144] Hence, in this case there are only two possible grounds to legitimize data processing: the balancing provision or unambiguous consent.

The balancing provision allows processing if it is necessary for the purposes of the legitimate interests pursued by the controller, unless the fundamental rights of the data subject should prevail. If behavioural advertising were not allowed, Google could still serve contextual advertising in many cases. Because the tracking of online behaviour can paint a highly detailed picture of an Internet user, which is often regarded as an invasion of privacy, the interests of the data subject should probably prevail.[145] According to the Working Party, "Covert surveillance of people's behaviour, certainly private behaviour such as visiting websites, is not in accordance with the principles of fair and legitimate processing of the Data Protection Directive."[146]

This means that in most circumstances the only possible ground to legitimize the processing of personal data for behavioural advertising is the "unambiguous consent" of the data subject.[147] Google's terms of service say: "You can accept the Terms by: (…) actually using the Services",[148] but such a 'browse wrap' license does not constitute unambiguous consent.[149] Merely

---

142 Article 8.2(a) of the Data Protection Directive. Some Member States require extra safeguards in their national laws, even when specific consent is obtained (European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, p 12).

143 Article 8 of the Data Protection Directive.

144 Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 17.

145 *Idem*, para 5.2. See also Article 29 Working Party, *The future of privacy (WP168)*. 1 December 2009, pp 16 - 17. The English Information Commissioner's Office seems to have a less stringent view (ICO (2010) *Personal information online code of practice*. July 2010, available at http://www.gov.gg/ccm/cms-service/download/asset/?asset_id=13634136. Accessed 31 August 2011.

146 Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines (WP148)*. 4 April 2008, p 23; See further about the requirements for valid consent: Article 29 Working Party, *Opinion 15/2011 on the definition of consent (WP187)*. 13 July 2011.

147 Traung 2010, p 220; Koëter 2009, p 111

148 According to article 7.2 of Google's Terms of Service, accepting the terms of Service means that "You agree to the use of your data in accordance with Google's privacy policies." www.google.com/accounts/TOS. Accessed 31 August 2011.

149 See also ECJ 9 November 2010, Case C92/09 and C-93/09 "*Volker und Markus Schecke GbR*", para 63, and Opinion Advocate General, para 91.

using a Google service does not constitute a freely given, specific and informed decision to allow Google to collect personal data. Moreover, even visiting one of the millions of websites where Google serves content such as advertisements, can result in receiving a cookie and being profiled. It is not plausible that prior unambiguous consent is always obtained in such cases. Furthermore, it is possible that Google is processing sensitive personal data, such as data regarding political opinions. The mere fact that somebody uses the Internet does not entail he has manifestly made public his sensitive data. Therefore, in the case of behavioural advertising, the only relevant exception to the prohibition to process sensitive data appears to be the "explicit consent" of the Internet user. However, like most other companies that engage in behavioural advertising, Google does not obtain prior consent. Offering a possibility to opt out is not sufficient to obtain consent.[150] In October 2010, the Working Party sent a letter to several advertising network providers (possibly including Google), inviting them to come up with solutions for more transparency and suitable mechanisms for consent.[151] To conclude: in most cases Google needs the unambiguous consent of Internet users to legitimize data processing for behavioural advertising. Therefore Google may not have a legitimate basis for the processing of personal data for its behavioural advertising program.

4.2.4.3 Google Street View

Can Google rely on one of the grounds to legitimize data processing for Street View? There are neither contractual nor legal obligations for which the processing of personal data is necessary and Google does not serve the vital interests of the data subject. Google processes both ordinary and sensitive personal data for its Street View service. In principle the data subject's consent may be a legitimate ground for both the processing of ordinary and sensitive personal data. While data subjects have not consented explicitly to their data being processed, they might have done so implicitly. According to the American "reasonable expectation of privacy" doctrine, one may not reasonably expect full privacy when walking on the street. "Street View contains imagery that is no different from what you might see driving or walking down the street."[152] Google also writes:

> "In the US, there's a long and noble tradition of "public spaces," where people don't have the same expectations of privacy as they do in their homes. This tradition helps protect journalists, for example. So we have been careful to only collect images that anyone could see walking down a public street. However we've always said that Street View will respect local laws wherever it is available and we recognize that other countries strike a different balance between the concept of "public spaces" and individuals' right to privacy in those public spaces. In other parts of the world local laws and customs are more protective of

[150] Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising (WP 171)*. 22 June 2010, p 15. The new e-Privacy Directive (amended in 2009) only allows the use of tracking cookies on condition that the Internet user has given his prior consent, having been provided with clear and comprehensive information. Although Member States had to implement the rule in May 2011, it is not clear yet how this rule will be applied in practice.

[151] Letter from the Article 29 Working Party addressed to the Ad Network Providers, 29 October 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_10_29_letter_Ad_network_and_annex_en.tif. Accessed 31 August 2011.

[152] Google Maps Privacy. http://maps.google.com/intl/en_us/help/maps/streetview/privacy.html. Accessed 31 August 2011.

> individuals' right to privacy in public spaces, and therefore they have a more limited concept of the right to take and publish photographs of people in public places."[153]

Indeed, in Europe the "reasonable expectation of privacy" doctrine is less influential; in certain circumstances one has a right to privacy in public.[154] Furthermore, according to the European Court of Justice, "a general derogation from the application of the directive in respect of published information would largely deprive the directive of its effect."[155] In principle the Directive applies when photographs that contain personal data are published on the Internet, also when they are taken in public.[156]

To invoke the consent of the data subject as the ground for data processing, it must either be unambiguous when it relates to ordinary personal data or explicit when it relates to sensitive data. An opt-out system that consists of blurring one's face if Google failed to blur it is not enough to construe unambiguous consent. The requirement for a legitimate purpose must be fulfilled before the data processing starts, not afterwards. The concept of implicit consent when walking in public or with regard to a less reasonable expectation of privacy in the public domain might also relate to another legitimate ground under the Directive for the processing of sensitive data, namely that personal data have been manifestly made public by the data subject. Although some people may have manifestly made public their (sensitive) personal data, it is unlikely that all people on the street have done so. Kotschy writes in another context: "'Making information public' requires a deliberate act by the data subject, disclosing the data to the public. Video-surveillance can therefore not be justified by the fact that the data subjects 'showed themselves in public.'"[157]

Google might try to invoke the argument that its service is necessary for the performance of a task carried out in the public interest. Street View has indeed enriched the public life and might be said to be of such importance that it serves the public interest. However, this does probably not fulfil the requirements for a successful invocation of this legitimisation of the processing of personal data. This ground is primarily invoked by governmental organisations which serve the public interest. It may either relate to governmental organisations performing a public task or to private companies that fulfil privatized governmental tasks.[158] Neither is however the case with regard to Street View.

Finally the balancing provision allows data processing of non-sensitive personal data when it is necessary for the legitimate interests of the controller, unless these interests are overridden by the interests of the data subjects with regard to data protection and privacy. Google has a legitimate interest in processing personal data, but the question is whether the fundamental rights of the data subjects should override this interest. To answer this question, there must be a balancing of the two interests of these parties. This weighing of interests must be done on a case-by-case basis, and all circumstances should be taken into account.[159] A fundamental right of the data controller would be an example of a legitimate interest that could override the fundamental rights of the data subject.[160] In general, fundamental rights carry greater

---

[153] Fleischer P, Street View and Privacy. Google Lat Long Blog. 24 September 2007, available at http://google-latlong.blogspot.com/2007/09/street-view-and-privacy.html. Accessed 31 August 2011.
[154] ECtHR, 24 June 2004, application no. 59320/00, Caroline Von Hannover v. Germany, para 50.
[155] ECJ 16 December 2008, Case C-73/07, "*Satamedia*", para 48 – 49.
[156] See ECJ 6 November 2003, Case C-101/01, "*Bodil Lindqvist*", para 24 – 27.
[157] Kotschy 2010, p 62
[158] Kuner 2007, p 244
[159] See Kotschy 2010, p 58; Kuner 2007, p 244
[160] ECJ 6 November 2003, Case C-101/01 (Bodil Lindqvist) para 90; Kotschy 2010, p 58

weight than the interest for profit, which is Google's main interest. Therefore, it seems not evident that Google can rely on the balancing provision in the case of Street View. This conclusion appears to be in line with the fact that some national authorities asked Google to implement extra measures to ensure the privacy of the data subjects, such as prior opt-out options for houses, information distribution via media and more effective blurring methods.[161] These conditions may be set on the ground of a number of the Directive's requirements, but may also affect the outcome of the balancing act.

4.2.5 Transparency Principle and the Rights of the Data Subject

4.2.5.1 Data Protection Directive

Data processing should take place in a transparent manner. This is one of the key principles of data protection regulation.[162] In order for data processing to be fair the data subject has to be aware data concerning him are being processed. The controller should at least provide information regarding his identity and the purposes of the processing. More information should be given when this is necessary to guarantee fair processing, having regard to the specific circumstances in which the data are collected. Some examples of this type of information are the recipients or categories of recipients of the data, the existence of the right of access and the right to rectify data. The information needs to be clear and precise. The Directive provides for an exemption from the information duty where the provision of information "proves impossible or would involve a disproportionate effort". In such cases Member States must provide appropriate safeguards.[163]

On the Internet, information is usually provided in privacy policies that are posted (behind a link) on websites. The Working Party emphasizes that overly long privacy policies full of legalese do not provide information in a sufficiently clear manner and that is not acceptable if they are difficult to find on a website. Therefore, the Working Party calls for privacy statements written in "simple, unambiguous and direct language."[164] Indeed, there is abundant empirical research that shows that the current practice of posting privacy policies on websites largely fails to inform Internet users.[165]

---

[161] See for example: Czech Office for Personal Data Protection, Annual Report 2010, p. 29-30, and Press Release 23 May 2011 (available at www.uoou.cz/files/rep_2010.pdf and www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=792&lang=en, accessed 31 August 2011); Federal Administrative Court Switzerland 20 March 2011, Case A-7040/2009, *"Eidgenössischer Datenschutz- und Öffentlichkeitsbeauf-tragter EDÖB vs. Google Inc. And Google Switzerland GmbH"*, Computer Law Review International 3/2011, p. 87-89; Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Keine weiteren Veröffentlichungen von Bildern in Google Street View, Press release 11 April 2011, available at http://www.datenschutz-hamburg.de/news/detail/article/dies-ist-ein-pressebeitrag2-copy-3.html?tx_ttnews%5Bswords%5D=street%20view&tx_ttnews%5BbackPid%5D=129&cHash=1f64e5b4aebdf6d2d73d4107ca61491d. Accessed 31 August 2011; Türk A (2011) How many German households have opted-out of Street View?, Google European Public Policy Blog, 21 October 2010, http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html. Accessed 31 August 2011.

[162] Gutwirth & De Hert 2006.

[163] Article 11 of the Data Protection Directive.

[164] Article 29 Working Party, *Opinion 10/2004 on More Harmonised Information Provisions (WP100)*. 25 November 2004, para V.

[165] McDonald 2010, chapter 5, with further references. See also Van Eijk et al. 2011.

Transparency is not only an obligation a controller must fulfil, it is also one of the rights the Directive grants the data subject. These rights are presented in somewhat summarized form below. Firstly, the data subject has the right to receive confirmation from the controller as to whether or not his data are being processed; information regarding the purposes of the processing; the categories of data concerned; and the recipients or categories of recipients to whom the data are disclosed. Secondly the data subject has the right to obtain communication, in an intelligible form, of the data undergoing processing and of any available information as to their source. Thirdly the data subject has the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.[166] Fourthly, a data subject has a general right to object on compelling legitimate grounds to the processing of his data.[167] The Directive requires Member States to grant this right at least when data are processed by a public authority or in the public interest, or when the processing is based on the balancing provision.[168] Where there is a justified objection, the processing may no longer involve those data. Fifthly, a data subject has a specific right to object to the use of his personal data for direct marketing.[169] Lastly, every person has the right not to be subjected to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[170]

4.2.5.2 Behavioural Advertising

How should Google's behavioural advertising program be judged in the light of the transparency principle? Google provides more transparency than other companies that engage in behavioural advertising. Google did not launch its behavioural advertising program quietly, but announced it in a blog post.[171] Furthermore, Google releases videos on YouTube, explaining clearly how cookies are used and how behavioural advertising works (how Google makes advertising "more interesting").[172] In addition, Google presented a tool called the Ads Preferences Manager, "which lets you view, delete, or add interest categories associated with your browser so that you can receive ads that are more interesting to you."[173] Google also adds icons in advertisements based on behavioural targeting on which users can click to access their profile.[174]

There are also negative aspects in the light of the transparency principle. Google's privacy policies do not fully explain which data are added to a behavioural profile and to what extent one's online behaviour is monitored. Although Google's privacy statements are not typical

---

166 Article 12(a) and 12(b) of the Data Protection Directive.
167 Article 14(a) of the Data Protection Directive.
168 Article 7 (a) and 7(b) of the Data Protection Directive.
169 Article 14(a) and 14(b) of the Data Protection Directive.
170 Article 12(a) and 15 of the Data Protection Directive.
171 Wojcicki S, Making ads more interesting. The Official Google Blog. 11 March 2009, available at http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html. Accessed 31 August 2011.
172 Google Privacy: Interest-based advertising. 2 March 2009, available at www.youtube.com/watch?v=aUkm_gKgdQc. Accessed 31 August 2011.
173 Wojcicki S, Making ads more interesting. The Official Google Blog. 11 March 2009, available at http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html. Accessed 31 August 2011.
174 Shieh L, New In-Ads Notice Label and Icon, Google Inside Adwords, 21 March 2011, available at http://adwords.blogspot.com/2011/03/new-in-ads-notice-label-and-icon.html. Accessed 31 August 2011.

legalese and not overly long, some questions remain about the data flows.[175] "Advertising and publishing customers may use web beacons in conjunction with the DoubleClick cookie to collect information about your visit to the website and exposure to a particular advertisement."[176] "We provide [personal] information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf."[177] Such phrases may confuse some readers. Which companies are deemed "other trusted businesses"? How many "affiliated companies" are there? Many companies reserve the right to change their privacy policies, and Google is no exception:

> "Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes)."[178]

Which changes would be "significant" is not clear. According to Google's terms of service: "The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you."[179]

Although the Ads Preferences Manager is a step in the right direction, Internet users cannot see all data that are actually tied to their profile. The Ads Preferences Manager merely shows the interests that Google infers after monitoring the user's online behaviour. As Van Hoboken notes: "To some extent, the control and transparency is merely a façade, behind which a (for the end-user) opaque sophisticated data processing architecture is doing the real work."[180] For example, one cannot access information about the retargeting information. Likewise it is impossible to find out on what basis Google infers interests. Furthermore, ample research shows that most Internet users are not or only vaguely aware to what extent their online behaviour is tracked. The average Internet user does not understand how cookies work, and is not acquainted with the data flows behind behavioural advertising.[181] Such users might never see Google's Ads Preferences Manager or the possibilities to opt out. An opt-in system would be a more transparent way of starting to track the online behaviour of an Internet user. The onus would be on Google to convince Internet users that the advantages of behavioural advertising ("ads that are relevant") outweigh possible disadvantages.[182]

In terms of the rights of the data subject, Google complies to a large extent with the requirements. The Ads Preferences Manager presents information in a user-friendly way and offers the possibility to rectify or erase categories Google has associated with a cookie. However,

---

[175] See also: Yang M, Trimming Our Privacy Policies. The Official Google Blog. 3 September 2010, available at http://googleblog.blogspot.com/2010/09/trimming-our-privacy-policies.html. Accessed 31 August 2011.

[176] Google Privacy Center. Privacy Policy for Google Ads and the Google Display Network. 29 September 2010. www.google.com/privacy/ads/privacy-policy.html. Accessed 31 August 2011.

[177] *Idem.*

[178] Google Privacy Center. Privacy Policy. 3 October 2010, available at http://www.google.com/privacy/privacy-policy.html. Accessed 31 August 2011.

[179] Article 17.2 of the Google Terms of Service. www.google.com/accounts/TOS. Accessed 31 August 2011.

[180] Van Hoboken J, Google Rolls Out Behavorial Targeting. 19 March 2009, available at http://www.jorisvanhoboken.nl/?p=262. Accessed 31 August 2011.

[181] McDonald 2010, chapter 5. See also Van Eijk et al. 2011.

[182] The e-Privacy Directive provides for a separate transparency regime. Article 5.3 only allows the use of cookies and similar devices "on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with [the Data Protection Directive], inter alia about the purposes of the processing."

as there are much more data stored than one can see in the Ads Preferences Manager, this may not be sufficient to comply with the right to access. For example, it is questionable whether Google provides sufficient information "as to their source" of one's data, as it is not completely clear which data are used to compile the behavioural profiles. Although it would be an interesting experiment, we have not tested if Google provides an overview of the personal data it processes for the behavioural profile upon request. Some practical issues might arise when doing such a request, as no name is tied to the profile, but a request to have access to all personal data tied to cookie "2vesgazbej45va555xsenyvs"[183] would be conceivable.

Google offers a user-friendly way to opt out of behavioural advertising. A common problem with such opt-out systems is that if a user clears his cookies, the opt-out cookie is deleted as well and the tracking starts again. Google also offers a plug-in for browsers to make an opt-out permanent.[184] According to Google, it will not only stop showing targeted advertisements after an opt-out, but it will also stop "collect[ing] interest category information".[185] In this respect Google offers users a broader opportunity to protect their data than many other behavioural advertising companies, which merely promise to stop showing targeted advertisements after an opt-out.[186] Although more transparency would make the rights of the data subject more meaningful, Google complies with a data subject's right to object.

Finally, every person has the right not to be subjected to an automated decision that produces legal effects concerning him or significantly affects him. This rule may seem relevant for some behavioural advertising practices. For example, banks might not advertise credit cards to people whose profile suggests that they live in a poor town. The targeting could limit the choices that are presented to a person. However, as such targeting does not constitute a decision that "significantly affects" a data subject, the prohibition does not apply.[187] In conclusion, Google's behavioural advertising program largely complies with the rights of the data subject, but it could do better with regards to the transparency principle.

4.2.5.3 Google Street View

Does Google Street View comply with the transparency principle? In an opinion regarding video surveillance, the Working Party said: "Data subjects should be informed in line with Article 10 and 11 of the Directive. They should be aware of the fact that video surveillance is in operation (…); they should be informed in a detailed manner as to the places monitored."[188] Street View does not concern continuous filming, so it is not fully comparable with video surveillance.[189] Still,

---

[183] This is one of the cookies that Google placed on the computer of one of the authors.

[184] Wojcicki S, Making ads more interesting. The Official Google Blog. 11 March 2009, available at http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html Accessed 31 August 2011.
; Harvey S, Moonka R, Keep your opt-outs, Google Public Policy Blog, 24 January 2011, available at http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html. Accessed 31 August 2011.

[185] Google Privacy Center, Advertising and Privacy, available at www.google.com/privacy/ads. Accessed 31 August 2011.

[186] Komanduri et al. (2011). See for example the opt-out page of the Internet Advertising Bureau, available at www.youronlinechoices.com/uk/your-ad-choices. Accessed 31 August 2011.

[187] González Fuster G et al. 2010, p 115

[188] Article 29 Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP89)*, 11 February 2004, p 22.

[189] See also: Information Commissioner's Office (2009) Letter regarding Privacy International's complaint about Google Street View, 30 March 2009,

it is questionable whether the data subject is adequately informed about data processing. Many people do not know that they are on Street View. Google does publish on a website where it will be photographing in a certain period.

> "This information shows a sample of the areas in which our cars are currently operating. We try to make sure the information is accurate and kept up to date, but because of factors outside our control (weather, road closures, etc), it is always possible that our cars may not be operating, or be operating in areas that are not listed. In these circumstances, we'll try to update the list as soon as we can. Please also be aware that where the list specifies a particular city, this may include smaller cities and towns that are within driving distance."[190]

The user may click on a country and see in which areas Google is planning to photograph in the near future. However, a possibility for individuals to check Google Street View to see whether they might be or have been photographed may not suffice to comply with the Directive's transparency requirements. People cannot be expected check Street View to see whether they will be or have been photographed either in their residential or working area, or in unusual places where they go to only once a month, a year or a lifetime. Moreover, the data specified on the website is not very specific. It may be possible to provide more information without a disproportionate effort. Several data protection authorities required Google to inform the public about photographing through the press as well.[191] Google grants data subjects the right to erasure of their personal data:

> "If our detectors missed something, you can easily let us know. We provide easily accessible tools allowing users to request further blurring of any image that features the user, their family, their car or their home. In addition to the automatic blurring of faces and license plates, we will blur the entire car, house, or person when a user makes this request for additional blurring. Users can also request the removal of images that feature inappropriate content (for example: nudity or violence)."[192]

To conclude, Google respects most of the data subject's rights, but there is room for improvement with regards to the transparency principle.

4.3. Conclusion

This chapter assessed the interplay of the European data protection regime and two services: Google's behavioural advertising program and Google Street View. The chapter focused on five aspects of the Data Protection Directive: the applicability of the Directive, the jurisdiction, the principles relating to data quality, the legitimate purpose and lastly the transparency principle in connection with the rights of the data subject.

---

www.ico.gov.uk/upload/documents/library/data_protection/notices/response_to_pi_complaint_v1.pdf. Accessed 31 August 2011.

[190] Google Maps, Where is Street View available?, available at www.google.com/intl/en_us/help/maps/streetview/where-is-street-view.html. Accessed 31 August 2011.

[191] Article 11.2 of the Data Protection Directive. See section 4.2.4.3.

[192] Google Maps Privacy. http://maps.google.com/intl/en_us/help/maps/streetview/privacy.html. Accessed 31 August 2011.

The applicability of the Directive is triggered when "personal data" are "processed" under the authority of the "controller" of the personal data. Both "processing" and "personal data" are broadly defined in the Directive. Personal data is any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly. Profiles without a name tied to them and photographs of people with a blurred face on Street View can also constitute personal data. Accordingly, Google processes personal data for both services. In the case of Street View, and possibly in the case of behavioural advertising, Google also processes sensitive data, such as data revealing racial origin, political opinions, religious beliefs, trade-union membership and data concerning health and sex life. As Google determines the purposes and means of the processing it is the data controller. Therefore, the first threshold is met for both services.

Secondly there is the jurisdictional threshold. The Directive applies, among other situations, when the controller is not established on Community territory and uses equipment situated on Community territory for data processing. For both services Google uses equipment on Community territory, by using cars for Street View, and – according to the Working Party – by placing cookies on computers for behavioural advertising. Hence, the Directive applies to both services. This chapter made an assessment with regard to three requirements: the principles relating to data quality, the legitimate ground for the processing, and finally the transparency principle in connection with the rights of the data subjects.

Firstly, the principles relating to data quality require that personal data be processed fairly and lawfully. Data must be collected for specified and explicit purposes and not further processed in a way incompatible with those purposes. Data must be accurate and not excessive in relation to the purposes for which they are processed, and retained no longer than is necessary for those purposes. Assessing Google's compliance with the data quality principle is not easy because not all aspects of its data processing practices are transparent. Google is more restrained than other companies that engage in behavioural advertising. Although Google does not add all information at its disposal to behavioural profiles, it does add large amounts of data, such as data regarding surfing behaviour and YouTube viewing data. Furthermore, Google may not have a sufficiently specified purpose for this data processing. With regard to Street View, personal data are processed for a specified and explicit purpose. Street View largely complies with the principles relating to data quality.

Secondly, personal data may only be processed on the basis of a legitimate basis laid down by law. There are neither contractual nor legal obligations for which the processing is necessary and Google does not serve the vital interests of the data subject or the public interest with the services. As a result, there are only two possible grounds to legitimise data processing: the unambiguous consent of the individual and the so-called balancing provision. The Directive prohibits processing of sensitive data unless certain requirements are satisfied. In Google's case the most relevant exception to this prohibition is the individual's explicit consent. Google does not obtain prior consent for either of the two services. Offering a possibility to opt out of a service is not sufficient for unambiguous or explicit consent. This would leave the balancing provision as the only possible legitimate ground for data processing. This provision allows data processing when it is necessary for the legitimate interests of the controller, unless the interests of the data subjects for data protection and privacy should prevail. Google has an interest in processing personal data, but this interest should be weighed against the fundamental rights of the data subjects. The Working Party does not accept the balancing provision as a ground for the processing of personal data for behavioural advertising. For Street View, the balancing act is somewhat more complex. Some data protection authorities only accept the balancing provision

as a legitimate ground if Google takes additional measures to ensure that the privacy of the data subjects is adequately protected.

Thirdly and finally, this chapter has assessed whether Google lives up to its duties under the transparency principle and its duty to respect the rights of the data subject. In order for data processing to be fair the data subject has to be aware that data concerning him are being processed. The controller must provide clear, precise and comprehensive information. Furthermore, the data subject has several rights, such as the right to be informed, to consult the data, to request corrections and to object to processing in certain circumstances. With regard to its behavioural advertising program, Google respects most of the rights of the data subject. Google offers access to part of a profile and offers several user-friendly possibilities to opt out. In this respect Google is a forerunner in comparison with other companies. However, Google could do better in terms of transparency. Questions remain about how much personal data are stored, for how long the data are retained, and how the data are used. In the case of Street View, Google respects the rights of the data subject. People can request Google to blur their houses or their vehicles. Again, Google could do better in terms of transparency. In conclusion, not all aspects of the two services are easy to reconcile with the Directive's requirements. The Directive is under review at the moment, and issues such as jurisdiction, the definition of personal data, the requirements for consent and the application of the balancing provision may need clarification.

* * *

References

Anguelov D et al. (2010) Google Street View: Capturing the World at Street Level. IEEE Computer Society, Computer. June 2010 (Vol. 43, No. 6) pp 32-38.

Battelle J (2005) The Search. How Google and its rivals rewrote the rules of business and transformed our culture. Penguin Group, New York.

Burdon M (2010) Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws. University of Illinois Journal of Law Technology & Policy. No. 1, 2010.

Bygrave L (2002) Data protection law: approaching its rationale, logic and limits. Kluwer Law International, The Hague.

Gomez J et al. (2009) Know Privacy, Final Report. UC Berkeley, School of Information. 1 June 2009, available at http://www.knowprivacy.org.

González Fuster G et al. (2010) From Unsolicited Communications to Unsolicited Adjustments. Redefining a Key Mechanism for Privacy Protection. In: Gutwirth, S et al. (eds) Data Protection in a Profiled World. Springer, Dordrecht, pp 105-117.

Gutwirth S & De Hert P (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes E, Duff A & Gutwirth S (eds) Privacy and the criminal law. Intersentia, Antwerp, pp 61-104.

Gutwirth S & Poullet Y (2008), The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'? In: Asinari V P & Palazzi P (eds) Défis du droit à la protection de la vie privée .Challenges of privacy and data protection law - Challenges of privacy and data protection law. Bruylant, Brussels, pp 570 – 610.

Hoofnagle C J (2009) Beyond Google and evil: how policy makers, journalists and consumers should talk differently about Google and privacy. First Monday, Volume 14, Number 4. 6 April 2009, available at http://www.firstmonday.org.

Koëter J (2009) Behavioral targeting en privacy: een juridische verkenning van internet gedragsmarketing. Tijdschrift voor internetrecht 2009-4.

Komanduri S et al. (2011) AdChoices? Compliance with Online Behavioral
Advertising Notice and Choice Requirements. CMU-Cylab-11-005, 30 March 2011, available at http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf.

Korff D (2010) Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Working Paper 2.0. 20 January 2010, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

Kotschy W (2010) Directive 95/46/EC – Data Protection Directive. In: Büllesbach A et al. (eds.) Concise European IT Law, Kluwer Law International, Alphen aan den Rijn.

Krishnamurthy B, Wills C (2009) On the leakage of personally identifiable information via online social networks. WOSN '09: the second workshop on online social networks, 2009, available at http://www2.research.att.com/~bala/papers.

Krishnamurthy B, Wills C (2009) Privacy diffusion on the web: a longitudinal perspective. Proceedings of the 18th international conference on world wide web, available at http://www2.research.att.com/~bala/papers.

Kuner C (2007) European data protection law: corporate compliance and regulation. Oxford University Press, Oxford.

Kuner C et al. (2009) Study on online copyright enforcement and data protection in selected Member States, available at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf.

Kuner C et al. (2010) Study on online copyright enforcement and data protection in selected Member States (Netherlands, Poland, UK), available at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf.

McDonald A M (2010) Footprints near the surf: individual privacy decisions in online contexts (diss.) Paper 7, available at http://repository.cmu.edu/dissertations/7.

Ohm P (2009) Broken promises of privacy: responding to the surprising failure of anonymization. University of Colorado Law Legal Studies Research 2009 (Article No. 09-12), 13 August 2009.

Rundle A G et al. (2011) Using Google Street View to audit neighborhood environments. American Journal of Preventive Medicine. Volume 40, Issue 1, January 2011, pp 94-100.

Toubiana V & Nissenbaum H (2011) An Analysis of Google Logs Retention Policies. Journal of Privacy and Confidentiality. Volume 3, Issue 1, Article 2, 2011.

Traung P (2010) EU Law on Spyware, Web Bugs, Cookies, etc., Revisited: Article 5 of the Directive on Privacy and Electronic Communications. Business Law Review 31 pp 216–228.

Van Eijk N.A.N.M. et al. (2011) A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland (Dilemmas with the implementation of the Cookie law in the Netherlands), TNO-report no. 35473, 28 February 2011, available at http://www.ivir.nl/publicaties/vaneijk/A_bite_too_big.pdf.

* * *