THE ROLE OF INTERNET SEARCH ENGINE PROVIDERS IN THE LIGHT OF THE EUROPEAN DATA PROTECTION LEGISLATION

A Study on the Judgment of the Court of Justice of the European Union on

Google Spain and Google Inc. v. Agencia Española de Protección de Datos (AEPD)

and Mario Costeja González

C-131/12

Master's Thesis

Anette Luomala

Legal Informatics

Faculty of Law

University of Lapland

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: The Role of Internet Search Engine Service Providers in the Light of the European Data Protection Legislation, A Study on the Judgment of the Court of Justice of the European Union on Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12

Tekijä: Anette Luomala

Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka

Työn laji: Pro Gradu X Laudaturtyö__ Lisensiaatintyö__ Kirjallinen työ__

Sivumäärä: XI + 87

Vuosi: 2014, syksy

Tiivistelmä. Tutkielman tarkoituksena on tutkia Internetin hakukoneen roolia EU:n tietosuojalainsäädännön valossa. Vertailukohtana käytän EU-tuomioistuimen tuomiota asiassa C-131/12. Tutkielmassani päädyn lopputulokseen, että Internetin hakukoneet käsittelevät henkilötietoja EU:n tietosuojadirektiivin tarkoittamassa merkityksessä. Hakukoneen voidaan myös katsoa olevan rekisterinpitäjä suhteessa sen käsittelemiin käyttäjätietoihin, kuten henkilön hakuhistoriaan sekä hakukoneen hakutuloksissa ilmeneviin henkilötietoihin, sillä se päättää henkilötietojen käsittelyn tarkoituksen ja keinot. Tutkielmassani ehdotan kuitenkin, että lähdesivustolla tulisi olla vastuu henkilötiedoista, jotka näkyvät hakukoneen hakutuloksissa, kun tietyt edellytykset täyttyvät. Avaintekijät tässä suhteessa ovat rekisteröidyn suostumus sekä poistokoodien käyttäminen lähdesivustolla. Hakukonetta voitaisiin käyttää ennemminkin apuna virheellisten tai vanhentuneiden tietojen paikantamiseen ja täten vastuun kohdentamiseen. Tutkielmassani pohdin myös lyhyesti yksilön ”oikeutta tulla unohdetuksi” sekä vaihtoehtoja sen tehokkaaseen täytäntöönpanoon käytännössä.

Avainsanat/asiasanat

Euroopan unioni, perusoikeus, yksityisyys, henkilötieto, hakukone, henkilötieto,

rekisterinpitäjä, oikeus tulla unohdetuksi, lähdesivu, Internet

Suostumus tutkielman luovuttamiseen kirjastossa käytettäväksi.

Suostun tutkielmani luovuttamiseen Rovaniemen hovioikeuden käytettäväksi X

Suostun tutkielmani luovuttamiseen Lapin maakuntakirjastossa käytettäväksi X

University of Lapland, Faculty of Law

Title of the Thesis: The Role of Internet Search Engine Service Providers in the Light of the European Data Protection Legislation, A Study on the Judgment of the Court of Justice of the European Union on Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12

Writer: Anette Luomala

Branch of Law: Legal Informatics

Type of the thesis: Master's Thesis

Amount of pages: XI + 87

Year: 2014, Autumn Semester

Summary. The aim of the thesis is to research the role of an internet search engine provider in the light of the European data protection legislation. As a benchmark in my thesis I use the judgment of the EU Court of Justice in the case C-131/12. The conclusion of the thesis is firstly, that the search engine provider processes personal data in the meaning of the EU Data Protection Directive. Secondly, the search engine provider can be considered to be a data controller in respect of the user data it processes such as person's search queries. Furthermore, the search engine provider is considered to be a data controller in relation to the personal data in its search results (content data). This is because the search engine provider solely decides the purposes and means of the processing of personal data.

In the thesis I suggest, however, that the source web page, which originally publishes the personal data, should be liable for the incorrect or irrelevant personal data in the search engine's search results when certain conditions are fulfilled. The key factors here are the consent of the data subject and the use of the exclusion codes. In my opinion, the search engines could be used as help when locating the incorrect or irrelevant personal data from the Internet. The thesis discusses also shortly about the individual's right to be forgotten and represents options for the effective implementation of the said right.

Key words
European Union, fundamental right, privacy, personal data, search engine, data controller, right to be forgotten, source web page, Internet

I consent that my thesis is placed at the disposal of the Library of the University of Lapland.

I consent that my thesis is placed at the disposal of the library of Lapland Province X
I consent that my thesis is placed at the disposal of the Rovaniemi Court of Appeal X

CONTENTS

BIBLIOGRAPHY

A) LITERATURE

Aarnio (1997)

Aarnio, Aulis: Oikeussäännösten systematisointi ja tulkinta. Teoksessa: Häyhä, Juha (toim.), Minun metodini. WSOY, Porvoo, 1997.

Beverley-Smith (2002)

Beverly-Smith, Huw: The commercial appropriation of personality, Cambridge University Press, New York, 2002.

Bygrave (2002)

Bygrave, Lee A.: Data Protection Law – Approaching Its Logic and Limits. Klüwer Law International, Hague, 2002.

Habermas (1998)

Habermas, Jürgen: Faktizität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtstaats, Frankfurt am Main, Suhrkamp, 1998.

Halavais (2009)

Halavais, Alexander: Search Engine Society – Digital Media and Society series. Polity Press MPG Books, Ltd, Bodmin, Cornwall, UK, 2009.

Heil (1997)

Heil, Helmut: Key Notes by the Federal Data Protection Commissioner. In Kilian (ed.): Beiträge zur juristische Informatik, Band 22, EC Data Protection Directive, Interpretation / Application / Transposition Working Conference, S. Toeche-Mittler Verlag, Darmstadt, 1997.

Helopuro – Perttula – Ristola (2009)

Helopuro, Sanna; Perttula, Juha; Ristola, Juhapekka: Sähköisen viestinnän tietosuoja, 2nd edition, Talentum Media Oy, Kariston Kirjapaino Oy, Helsinki, 2009.

Herrmann (2007)

Herrmann, Debra S.: Complete Guide to Security and Privacy Metrics, Measuring Regulatory Compliance, Operational Resilience, and ROI. Auerbach Publications, 2007

Hofstadter & Horowitz (1964)

Hofstadter, Samuel H. And Horowitz, George. The Right of Privacy. Central Book Company, Inc., New York, 1964

Husa (1998)

Husa, Jaakko: Johdatus oikeusvertailuun. Lakimiesliiton kustannus, Helsinki, 1998.

Innanen & Saarimäki (2009)

Innanen, Antti; Saarimäki Jarkko: Internet-oikeus. Edita Publishing Oy, Edita Prima Oy, Helsinki, 2009.

Järvinen (2002)

Järvinen, Petteri: Tietoturva & Yksityisyys. SanomaWSOY-konserni, Porvoo 2002

Järvinen (2010)

Järvinen, Petteri: Yksityisyys – turvaa digitaalinen kotirauhasi, WSOYpro OY, Docendo, Jyväskylä, 2010

Järvinen (2014)

Järvinen, Petteri: NSA – Näin meitä seurataan. Jyväskylä, Docendo, 2014

Kemppinen (2011)

Kemppinen, Jukka: Informaatio-oikeuden alkeet. Tietosanoma Oy, AS Pakett, Tallinna, 2011.

Kilian (1997)

Kilian, Wolfgang: Introduction into the EC Data Protection Directive, in Kilian (ed.): Beiträge zur juristische Informatik, Band 22, EC Data Protection Directive, Interpretation / Application / Transposition Working Conference, S. Toeche-Mittler Verlag, Darmstadt, 1997.

Konstari (1992)

Konstari, Timo: Henkilörekisterilaki, Säännökset ja käytäntö. Lakimiesliiton kustannus, Helsinki, 1992.

Korhonen (2003)

Korhonen, Rauno: Perusrekisterit ja henkilötietojen suoja, Informaatio-oikeudellinen tutkimus yksityisyyden suojasta yhteiskunnan perusrekisteritietojen käsittelyssä, Lapin yliopistopaino, Rovaniemi 2003.

Korhonen (2014)

Korhonen, Rauno: Sähköinen asiointi ja viestintä, in Tuominen, Tomi (ed.): Oikeus tänään. 2nd Edition. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 62. Rovaniemi, 2014.

Kuner (2007)

Kuner, Christopher: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, 2007.

Kuner (2013)

Kuner, Christopher: Transborder Data Flows and Data Privacy Law. University Oxford Press Inc., New York, 2013.

Lloyd (2011)

Lloyd, Ian J.: Information Technology Law, 6th Edition, Oxford University Press Inc, New York, 2011.

Mahkonen (1997)

Mahkonen, Sami: Oikeus yksityisyyteen, WSOY Lakitieto Oy, Porvoo, 1997

Millard (2013)

Millard, Christopher (ed.) Cloud Computing Law. Oxford University Press, New York, 2013

Neuvonen (2014)

Neuvonen, Riku: Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus, Helsingin Kamari Oy, Helsinki, 2014.

Ojanen (2009)

Ojanen, Tuomas: Johdatus perus- ja ihmisoikeusjuridiikkaan. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja, Yliopistopaino, Helsinki, 2009.

Pitkänen – Tiilikka – Warma (2013)

Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija: Henkilötietojen suoja. Talentum, Helsinki, 2013

Pöysti (1999)

Pöysti, Tuomas: Tehokkuus, informaatio ja eurooppalainen oikeusalue, Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja, Hakapaino Oy, Helsinki, 1999.

Saarenpää (1997)

Saarenpää, Ahti: Data Protection in Finland. In Kilian, Wolfgang (ed.) Beiträge zur juristichen Informatik, Band 22, EC Data Protection Directive: Interpretation / Application / Transposition, Working Conference. S. Toeche-Mittler Verlag, Darmstad, 1997.

Saarenpää 1 (2012)

Saarenpää, Ahti: Oikeusinformatiikkaa, in Tammilehto Timo (ed.): Oikeusjärjestys, Osa 1, 8. täydennetty painos, Lapin yliopiston oikeustieteellisiä julkaisuja sarja C 59, Bookwell Oy, Rovaniemi 2012.

Saarenpää 2 (2012)

Saarenpää, Ahti: Henkilö- ja persoonallisuusoikeus, in Tammilehto Timo (ed.): Oikeusjärjestys, Osa 1, 8. täydennetty painos, Lapin yliopiston oikeustieteellisiä julkaisuja sarja C 59, Bookwell Oy, Rovaniemi 2012.

Saraviita (2005)

Saraviita, Ilkka: Suomalainen perusoikeusjärjestelmä. Talentum Media Oy, Gummerus Kirjapaino Oy, Jyväskylä, 2005.

Seipel (1977)

Seipel, Peter: Computing law, Perspectives on a New Legal Discipline. LiberFörlag Stockholm, LiberTryg Stockholm, 1977.

Seipel (1990)

Seipel, Peter: Juristen och datorn, Introduktion till rättsinformatiken, tredje upplagan (1990), Norstedts Förlag AB. Tryck: Studentlitteratur, Lund 1990. Stockholm, 1982.

Solove & Schwartz (2013)

Solove, Daniel J. and Schwartz, Paul M.: Privacy Law Fundamentals. Second edition, An IAPP Publication, 2013.

Van Dijk (2012)

Van Dijk, Jan: The Network Society, 3rd Edition, SAGE Publications Ltd, MPG Books Group, Bodmin, Cornwall, 2012

Vanto (2011)

Vanto, Jarno J.: Henkilötietolaki käytännössä, WSOYPro Oy, Helsinki, 2011

Warren & Brandeis (1890)

Warren, Samuel D. & Brandeis, Louis D: Right to Privacy. In Hofstadter, Samuel H. And Horowitz, George: The Right of Privacy. Central Book Company, Inc., New York, 1964. Originally published in the Harvard Law Review Vol. IV. No.5, 15th December, 1890.

B) OFFICIAL MATERIAL

European Union

eEurope Action Plans
http://europa.eu/legislation_summaries/information_society/strategies/l24226_en.htm

eGovernment Action Plan i2010
http://europa.eu/legislation_summaries/information_society/strategies/l24226j_en.htm

Europe 2020 Strategy
http://ec.europa.eu/europe2020/index_en.htm

Council of Europe

T-PD-BUR(2010)09 (I) FINAL (Conseil de l'Europe, 5 November 2010) (8) Report en the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_09%20FINAL.pdf

Article 29 Data Protection Working Party

WP12 Article 29 Data Protection Working Party, "Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive, Adopted by the Working Party on 24 July 1998

WP20 Article 29 Data Protection Working Party, WP20, Opinion No 3/1999 on Public sector information and the protection of personal data, Adopted on 3 May 1999, Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public sector information: a key resource for Europe" COM (1998) 585

WP29 Press Release Issued by the Article 29 Data Protection Working Party European DPAs meet with search engines on the "right to be forgotten"**,** Brussels, 25 July 2014

WP37 Article 29 Data Protection Working Party, 5063/00/EN/FINALWP 37, Working Document, Privacy on the Internet - An integrated EU Approach to On-line Data Protection- Adopted on 21st November 2000

WP136 Article 29 Data Protection Working Party, 01248/07/EN/WP136, Opinion 4/2007 on the concept of personal data

WP148 Article 29 Data Protection Working Party, 00737/EN/WP148, Opinion 1/2008 on data protection issues related to search engines

WP169 Article 29 Data Protection Working Party, 00264/10/EN/WP169, Opinion 1/2010 on the concepts of "controller" and "processor"

WP225 Article 29 Data Protection Working Party, 14/ENWP225, Guidelines on the implementation of the Court of Justice of the European Union judgment on Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12

Article 29 Data Protection Working Party, Press Release, 26.11.2014, Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten"

European Commission

COM(2012) 11 final 2012/0011 (COD)

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012

European Commission, Press Release Database, Memo, 12.3.2014, Progress on EU data protection reform now irreversible following European Parliament vote available at http://europa.eu/rapid/press-release_MEMO-14-186_fi.htm

European Parliament

Albrecht report:

Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht

OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

http://www.oecd.org/Internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD Guidelines, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79

http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

OECD Work on Privacy

http://www.oecd.org/sti/ieconomy/privacy.htm

OECD Members and Partners

http://www.oecd.org/about/membersandpartners/

UNITED NATIONS

Home page of the United Nations http://www.un.org

The Universal Declaration of Human Rights http://www.un.org/en/documents/udhr/

FINLAND

Government Bills

HE 49/1986	Government Bill for the Parliament Concerning the Enactment of the Personal File Act and Related Acts.
HE 309/1993	Government Bill for the Parliament Concerning the Amendment of the Finnish Constitution
HE 96/1998	Government Bill for the Parliament Concerning the Personal Data Act and Related Acts.
HE 194/2001	Government Bill for the Parliament Concerning the Acts for Information Society Services an Related Acts.

Opinions of the Committee for Constitutional Law

PeVL 54/2002 vp

PeVL60/2001 vp, p. 2/I, PeVM 14/2002 vp, p. 3/II

PeVL 25/1998 vp.

SWEDEN

Ministry of Justice

Personal data protection – Information on the personal data Act, 4th end (2006),

available at http://www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf

C) CASES AND ADMINISTRATIVE RULINGS AND RECOMMENDATIONS

EUROPEAN COURT OF JUSTICE

C-274/99 P Bernand Connolly

Judgment of the Court, In Case C-274/99 P, Bernard Connolly appeal against the judgment of the Court of First Instance of the European Communities (First Chamber) of 19 May 1999 in Joined Cases T-34/96 and T-163/96 Connolly v Commission [1999] ECR-SC I-A-87 and II-463, seeking to have that judgment set aside, the other party to the proceedings being: Commission of the European Communities

C-101/01 Bodil Lindqvist

Judgment of the Court, 6 November 2003, In case C-101/01 Bodil Lindqvist

C-6/64 Costa v E.N.E.L.

Judgment of the Court of 15 July 1964. Flaminio Costa v E.N.E.L. In the case C-6-64

C-293/12 and C-594/12 Digital Rights Ireland Ltd

Judgment of the Court (Grand Chamber), 8 April 2014, In Joined Cases C‑293/12 and C‑594/12, Digital Rights Ireland Ltd (C‑293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C‑594/12), Michael Seitlinger, Christof Tschohl and others.

Court of Justice of the European Union, PRESS RELEASE No 54/14, Luxembourg, 8 April 2014 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

C-131/12 Google Spain v. AEPD, Costeja Gonzáles

Judgment of the Court (Grand Chamber), 14th May 2014, In Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzáles

Reference for a preliminary ruling from the Audiencia Nacional (Spain) lodged on 9 March 2012 – Google Spain, S.L., Google Inc. v Agencia Española de Protección de Datos, Mario Costeja Gonzáles

Opinion of Advocate General Jääskinen, 25 June 2013, Case 131-12, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzáles

C-324/09 L'Oréal

Judgement of the Court (Grand Chamber), 12 July 2011, In Case C-324/09, L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v. eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi,

C-73/07 Satakunnan Markkinapörssi ja Satamedia

Judgment of the Court, (Grand Chamber), 16 December 2008, in the case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy,

C-92/09 and C-93/09 Volker und Markus Schecke ja Eifert

Judgment of the Court (Grand Chamber), 9 November 2010, in joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v. Land Hessen, joined party: Bundesanstalt für Landwirtschaft und Ernährung,

C-465/00 Österreichischer Rundfunk and others

Judgment of the Court, 20 May 2003, in the case C-465/00, Rechnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark,

Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk,

OTHER COURTS AND RULINGS OF AUTHORITIES

Belgium

Belgian Privacy Commission: Decision on 9th December 2008 in the case SWIFT

European Court of Human Rights

Times Newpapers Ltd. V. UK, on 10th March 2009

Finland

Data Protection Board: Dnro 2/932/2009 (1.2.2010)
http://www.finlex.fi/fi/viranomaiset/ftie/2010/20100001?search%5Btype%5D=pika&search%5Bpika%5D=2%2F932%2F2009

Finnish Data Protection Board 1/2006 available at:

http://www.finlex.fi/fi/viranomaiset/ftie/2006/20060001

The Finnish Administrative Supreme Court
KHO 27.9.2013/3084 Drnro: 1025/2/12

Germany

Solange I, BVerfGE 37, 271 2 BvL 52/71, 29 May 1974, Germany, Bundesverfassungsgericht

USA

Boyd v. United States, 116 U.S. 616 (1886), a decision by the United States Supreme Court

D) UNOFFICIAL ONLINE MATERIAL

Google

Privacy Policy	http://www.google.fi/intl/fi/policies/privacy/
About Google	http://www.google.fi/intl/fi/about/
Products of Google	http://www.google.fi/intl/fi/about/products/
Google location data	http://www.google.fi/intl/en/policies/technologies/location-data/
Google Cookies	http://www.google.fi/intl/en/policies/technologies/cookies/

Kuner, 2014 Kuner, Christopher: The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges, Version 1.0/September 2014, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496060

Mayclim, 2006 Mayclim, T.: Growing number of job searches disrupted by digital dirt, 2006 available at http://www.execunet.com/m_releases_content.cfm?id=3349

Saarenpää, 2000 Saarenpää, Ahti: Verkkoyhteiskunnan oikeutta: johdatusta aiheeseen, Article, 2000, available at https://helda.helsinki.fi/bitstream/handle/10224/3699/verkko-oikeutta.pdf?sequence=1

E) INTERVIEWS

Discussion with the Finnish Data Protection Ombudsman Reijo Aarnio, on 8th October, 2014, 9-10 am.

ABBREVIATIONS

AEPD	Agencia Española de Protección de Datos
CHARTER	Charter of Fundamental Rights of the European Union (2000/C 364/01)
COE CONVENTION	Convention EST 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the content of those instruments embody the basic principles of other legal instruments
DIRECTIVE	Directive (EC) 95/46/EY 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 [1995] OJ L281/31. It was adopted on 24 October 1995
DPA	Data Protection Authority
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EEC	European Economic Community
EU	European Union
FRA	Försvarets radioanstalt, Sweden's National Defence Radio Establishment
GPS	Global Positioning System
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISP	Internet Service Provider
NSA	US National Security Agency
OECD	Organization for Economic Cooperation and Development
REGULATION	The Upcoming EU Data Protection Regulation
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
URL	Uniform Resource Identifier
WP29	Article 29 Data Protection Working Party

1. Introduction

Data protection and privacy are the hot topics of this decade. The interest in the data protection arose at latest after the disclosures of Edward Snowden in 2013 which related to the US' National Security Agency. After the Snowden-disclosures also ordinary people got concerned about their personal data: who has access to them, are they transferred to third parties, who shall protect them and be responsible for them?

This thesis is written in a period of time in which, on the one hand, data protection laws are in a revolution and on the other hand, rapid technological developments, changes in the information society and in the behavior of digitally networked individuals can be seen. European Union is legislating its new Data Protection Regulation and the companies are getting ready for changes in the data protection framework. At the same time new inventions are brought to market such as wearable devices and other smart devices which collect huge amounts of personal data. People, especially youngsters, are interested in new technology and are willing to give part of their privacy to companies in a form of personal data in order to use cool technology and services.

Due to enormous amount of data in the digital networks it has become very hard to locate it. This problem creates markets to search engines which provide individuals one kind of an "information society service" helping individuals to find information from the Internet. The role of the search engines has, however, been problematic in a legal perspective. The aim of my thesis is to research the role of Internet search engine providers in the light of the data protection legislation in the EU. As an example of a search engine I use Google throughout my thesis. In addition, the recent judgment in the case C-131/12 '*Google Spain v. AEPD*[1] *and Mario Costeja Gonzáles'* is used as a benchmark for my findings. The judgment C-131/12 has a great significance for data protection law, EU fundamental rights law, and the Internet[2]. It is known as a case granting individuals a 'right to be forgotten'. Right to be forgotten is an important right and on that part, the judgment is significant. However, the case also provides other interesting issues to be researched such as territorial and material scopes of the EU Data Protection.

[1] Agencia Española de Protección de Datos, the national data protection authority of Spain.
[2] Kuner, 2014, 1

In my thesis I will first introduce the branch of law, *legal informatics,* on which my thesis is based on. The legal foundation for my research problem is represented in the third chapter. In the chapter 4, I will research the concept and history of privacy and study individual's right to privacy on a human- and fundamental rights level. Because search engines play an important part in the thesis, they will be represented together with the search engine related regulation in the chapter 5. Then, in the chapters 6 to 8 I research the important data protection related concepts, *data processing, personal data, data processor and data controller,* which have a significant meaning in my thesis when it comes to the final conclusion. Finally, in the ninth chapter I will put my findings on the concepts together and research the role and responsibilities of search engine providers as well as the role and responsibilities of source web pages. Further, the importance of effective implementation of individuals' right to data protection is included in the ninth chapter.

1.1 Research Problem

The research problem in my thesis is the following: What is the legal role of search engine providers in the light of European Data Protection framework? Search engines collect and process huge amounts of data. Data is collected from the Internet users who use search services in order to locate the information they need. Search engine services are used in people's everyday life and this makes defining the role and therefore the responsibilities of search engines important. I want to elaborate that search engines have a dual role when it comes to defining their legal role. On the one hand search engines process user data, which is data collected from the users. On the other hand search engines provide users with search results, content data, which may include persons' names, addresses and other personal data. In my thesis I want to define a role for a search engine provider in the both situations.

1.2 Approach, Theoretical Framework and Method

My *approach* to the research problem is from the viewpoint of a search engine user when it comes to privacy and further to the protection of personal data. However, in order to execute appropriate and sufficient data protection in connection with search engine services it is

necessary to find out the responsibilities of search engines in situations where they provide search services to Internet users. Therefore I will research the roles and responsibilities of the main actors represented in the EU data protection legislation: data controller and data processor. However due to the limited numbers of pages I only can define the roles of those actors, there is no space for researching their obligations. Therefore, the obligations of data processor and controller are mentioned only on a general level.

In my thesis the *theoretical framework* consists mainly of human and fundamental rights. As a background for my thesis I have researched the concept and history of privacy. This theme, individual's right to privacy and private life and further individual's right to data protection, is a red thread throughout my thesis. I have not forgotten the importance of the opposite human and fundamental rights to privacy, such as freedom of expression which includes the rights to hold opinions and to receive and impact information and ideas without interference by public authority and regardless of frontiers. However, due to the limited number of pages I have not had a possibility to research freedom of expression as deeply as I have researched individual's right to privacy and therefore freedom of expression is represented only on a general level to highlight that the right to privacy is not absolute. The theoretical framework also includes viewpoints from other branches of law such as EU law and data protection related regulation both on the EU level and on national level. The emphasis is in the legislation on the EU level; national laws, such as Finnish laws, are represented to give interesting examples and comparison to EU legislation.

The *method* of my thesis is legal dogmatic, meaning the jurisprudence which goals have traditionally been the interpretation of the legal rules (practical scope) as well as the systematization of provisions of law (theoretical scope). They both have their own methods but are in interaction with each other.[3] Theoretical jurisprudence tries to open possibilities for questions which arise in connection with the practical jurisprudence.[4] My thesis is based on the concepts used in the data protection framework such as *personal data, data processing, and data controller*. Therefore, the foundation of my thesis is very theoretical. The theoretical basis is, however, in interaction with more practical approach: in my thesis I research how the concepts work in reality in relation to the activities of search engine

[3] Aarnio, 36-37
[4] Aarnio, 53

providers. As an example I use the recent judgment, C-131/12, given by the European Court of Justice. By comparing the theory with practice I want to find out how the concepts included in data protection laws can fit the dynamic, complicated and sometimes contradictory interests in the society[5], such as the legal role of search engine providers.

2. Legal Informatics

Legal informatics[6] is a quite new field of law with historical roots to legal philosophy and legal theory[7]. It was born around the same era when a computer was invented and automatic data processing came into existence in the end of 1940s and beginning of 1950s. First, the concentration was in "computers and law" but later telecommunication as well as data processing related theories and methods received more attention. This development led to the term *legal informatics*.[8]

The research in the field of legal informatics concentrates on the relationships of law and information[9] as well as justice and information technology in their versatile forms. It discusses 'old' legal questions by combining traditional theories with new viewpoints[10]. Therefore it can be said that legal informatics goes along with the changing society by researching new information related phenomena. As a branch of law, legal informatics can be described as interdisciplinary field of law with international dimensions.[11]

Research in the area of legal informatics has been strong for example in Sweden in the 1970s. The first doctoral thesis in the area of legal informatics was written in 1977 by Peter Seipel (Computing Law, 1977).[12] According to Seipel, the main areas of legal informatics

[5] Aarnio, 38
[6] Seipel, 1990, 24: Different language versions: danska: retsinformatik, norska: rettsinformatikk, tyska: Rechtsinformatik, finska: oikeusinformatiikka, franska: droit et informatique, italienska: informatics e diritto. English has a problem with "informatics" and has used "computers and law or "law and information technology".
[7] Saarenpää, 2012 (1), 426
[8] Seipel, 1990, 23-24
Saarenpää 1986, 317-318 and Seipel 1990, 31-35: Legal informatics (Rechtsinformatik) as a term stems from Germany, where Wilhelm Steinmüller together with his group of researchers started to use it in 1970.
[9] Information can be defined as data which has been communicated and understood. See the Chapter 7.
[10] Seipel, 1990, 48
[11] Saarenpää, 2012 (1), 415, 426
[12] Korhonen, 2003, 18-20.

concentrate on questions relating to automatic data processing, computers and software, and communication through information networks.[13] Legal informatics is divided in general and special sectors. The general sector researches rights of human beings in the constantly transforming society, whereas the specific sector consists of legal data processing, study of legal information, information law and information technology law.[14]

Information has become a crucial resource together with capital, raw materials and energy[15]. We have come a long way starting from hunting- and agriculture societies through industrial and service societies till information society.[16] The fast development of the Western societies has been consistent from the 1990s and we have lived in the information society for a while already. However, a more advanced level of information society has not yet been reached. The change would require quality of data as well as selective processing of data.[17] The recent judgment of European Court of Justice in the case "Google Spain" gave human beings the right to be forgotten, meaning the right of Internet users to correct and delete their personal data from web pages of the Internet and more precisely from the search results provided by the search engine.[18] This judgment is a step forward to achieve more qualified level of data processing.

In addition to information society, there are other ways to present the current society we are living in: network society and legal network society. Those concepts illustrate the fact that significant functions of today's society are connected with each other through various networks in a digital environment crossing geographical borders[19].

The first settlers of law and informatics was *Lee Loevinger* who represented a new field of science, jurimetrics, in his article Jurimetrics – The Next Step Forward, 1949. (Korhonen, 2003, 18-20).

[13] Seipel, 1990, 16

[14] Saarenpää 2012 (1), 430-554. Legal Informatics as a branch of law is taught and studied in the University of Lapland.

[15] Seipel, 1990, 31

[16] Seipel, 1990, 31 and Saarenpää 2012 (1), 415

[17] Korhonen, 2003, 3-5

[18] C-131/12

[19] **Transborder data flows**. Due to economic growth and efficiency, the amount of international transfers of personal data has increased exponentially and had a positive impact around the world. Such occurrence, however, evokes risks for individuals at the same time. In the 1970s the term 'transborder data flows' was typically understood to refer to point-to-point data transfers meaning, for example, responding to requests of customers or exchanging internal company administrative information. Today, many transborder data flows involve multiple partners communicating through networks in a distributed fashions such as search engines and cloud computing. The term *'transborder data flows'* is not defined in the current EU data protection legislation and neither is it included in the Commission's proposal for EU's new data protection framework. However, the OECD Guidelines as well as the Convention 108 of the Council of Europe both refer to transborder data flows. (Kuner, 2013, 2, 4, 11). Even though the regulation on transborder data flow is

The difference between *information society* and *network society* can be described as follows: an information society concentrates on the changing substance of activities and processes in the society. The main emphasis is in the content meaning the use, production and exchange of the information which has become crucial in the information society. Network society, instead, gives attention for the changing organizational forms and infrastructure of the societies.[20] In my thesis I use the term 'information society' because the emphasis of the thesis is more in the activities related to the information than in the infrastructure of the networked society. However, I agree that when discussing about the infrastructure, the term 'network society' could be used instead of the concept of 'information society'.

> **Network society.** Social networks are as old as human kind[21] but the term "network society "reflects the needs of the current society: in addition to traditional infrastructure and ways of communication we are currently depended on the networks of electronic communication. Such dependence goes for the society at large. The significant role of online communication networks can be seen for example in politics and power[22] and in the economics. Furthermore, networks effect on the social life of individuals and the culture in the society.[23] The 21st century can therefore be called the age of networks. [24]
>
> The most important structural characteristic of the network society is called *convergence.* It means the integration of telecommunications, data communications and mass communications in a single medium.[25] Also Professor Ahti Saarenpää has written about the convergence meaning the integration of medium, technology and economical actions to a single medium of open networks.[26] Saarenpää also thinks that the term 'information society' could be replaced with the term 'network society' because the infrastructure of networks has significantly changed during the past years and the use of networks has become a daily action in different levels of society. The developing infrastructure of the network society must also be followed by a contemporary legislation (term '*legal network society'*).[27]
>
> Currently, the networks serve society at every level and connect those levels[28]. This means connecting individuals, organizations and other groups. In the network society those units are linked with each other through various online

important and interesting, but due to the limited number of pages I have no possibility to research this theme more deeply.

[20] Van Dijk, 22-23
[21] Van Dijk, 48
[22] Van Dijk, 98-101 (Networks as a tool for democracy by e-participation, see Van Dijk, 104, 111)
[23] Van Dijk, 171, 210
[24] Van Dijk, 1-2
[25] Van Dijk, 7-8
[26] Korhonen, 2014, 28. See also Saarenpää 2012(1)
[27] Saarenpää, 2000, 4-6
[28] Van Dijk, 48

networks such as Internet.[29] Network society is sometimes compared with a *mass society* meaning an infrastructure of groups, organizations and communities (masses) organizing individuals.

The challenge in the current network society is the huge amount of information in the networks. In order to manage those enormous amounts of data intermediaries such as search engines are needed to organize and locate the information.[30] In fact, the largest part of the Internet and online networking audience goes to a few big players such as Facebook and Google.[31]

Living in a network society creates also some problems. First of all there is a risk to individuals' privacy. Privacy legislation and regulation are at a low level of development and effectiveness: constitutions are very broad whereas privacy laws are often very specific.[32] In the EU the effectiveness of privacy legislation is uncertain, which can also be seen in the implementation of the right to be forgotten confirmed by the ECJ's judgment C-131/12.

Secondly, the question who rules the Internet still remains open. There are attempts by governments to rule the Internet by legislation but the problem is that the laws cannot keep pace with technological and economic level. Also communities and corporations try to rule the Internet with self-regulation and market control whereas software designers compete against other rulers by placing technological control over the Internet.[33] Thirdly, the network society is quite vulnerable. It is prone to hacker attacks, network centric warfare and cyber wars.[34] This problem is serious since most of our daily actions are carried out in the networks.

Fourthly, the use of networks creates economic issues as well as issues related to intellectual property rights. Information has become the most important economic product in the modern society and some people think that it should be submitted to the principles of the market economy like any other good. However, opposite opinions exist.[35] Finally, technology is important for the development of the network society. Current technical trends in the network society are for example mobile and wireless technology[36] as well as *cloud computing*[37]. Companies such as Microsoft, Google and Amazon offer cloud computing services on demand[38].

---

[29] Van Dijk, 24, 45
[30] Van Dijk, 39
[31] Van Dijk, 41
[32] Van Dijk, 130-131
[33] Van Dijk, 140-151
[34] Van Dijk, 98-101
[35] Van Dijk, 157
[36] Van Dijk, 54-58
[37] Cloud computing means services provided in the "cloud" meaning that all the data needed for the application/service is stored on a centralized database and Internet service users can have an online access to them. Therefore data does not have to be stored on a user's own computer. Systems like cloud computing create new kinds of legal problems such as the ownership of information in clouds, as well as the responsibilities and rights of actors using and providing cloud services.
[38] Van Dijk, 58

Due to the digital environment and complex relations in networks, the network society needs guidelines and development of the "information and communication technology" (ICT). In the European Union this need of has been answered by providing eEurope action plans (2002 and 2005) which have been completed by the eGovernment Action Plan i2010. In 2009 a new Europe 2020 Strategy started which is a ten-year incremental strategy to develop EU[39]. In addition, the environmental and economic effects of information technology are important to take into account, and that is why the concept of Green Information Society has raised its head.[40] All in all, as can be seen from the initiatives described above, it seems that Peter Seipel's question "Does legal informatics have a future?[41]" has an answer at latest now, almost three decades later: we are in a need of constant research of data processing technologies and their relationship with changing network societies.

3. Legal Foundation

3.1 Data Protection Directive

The major legal instrument for data protection in the European Union is the EU Data Protection Directive 95/46/EY (hereinafter "the Directive") [42]. It was enacted in 1995 for two main purposes: to allow free flow of data within the Europe and to minimize the divergence of data protection laws in the Member States. The latter purpose was set up to achieve a minimum level of data protection in all Member States. The first goal matches with EU principles relating to free movement of goods, persons, services and capital. The Directive tries to find a balance between those two purposes.[43] The objectives of the Directive support

[39] Korhonen 2014, 29-30.
eEurope Action Plans available at:
http://europa.eu/legislation_summaries/information_society/strategies/l24226_en.htm
eGovernment Action Plan i2010 available at:
http://europa.eu/legislation_summaries/information_society/strategies/l24226j_en.htm
Europe 2020 available at: http://ec.europa.eu/europe2020/index_en.htm
[40] Saarenpää, 2012(1), 418
[41] Seipel, 1977, 377
[42] Directive (EC) 95/46/EY 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 [1995] OJ L281/31. It was adopted on 24 October 1995 and Member States had 3 years time to implement it.
[43] Kilian, 1-2

EU's aim to create a field of legal informatics into the EU by developing European information markets.[44] The Directive aims to protect individuals and at the same time ensure that legitimate interests of data controllers are addressed.[45]

The Directive is an extension of Article 8 of the ECHR (European Convention on Human Rights) which guarantees every person a *right to respect for private and family life.*[46]. In addition, the Directive is greatly influenced by the OECD Guidelines and the Coe Convention (see below), and the content of those instruments embody the basic principles of other legal instruments.[47] Noteworthy is that some differences exist between the mentioned three instruments and therefore, in conflicts of laws, the Directive should always be applied in the first place.[48]

> **The OECD (*Organization for Economic Cooperation and Development*) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines" or "Guidelines"),** enacted in 1980, have had a tremendous impact on the legislation process of the Directive. OECD was established in 1960 and it began its work in the area of protection of privacy already in 1969. This work included, for example, analyzing of digital information, public administration, transborder data flows, and policy implication.[49] The Guidelines were adopted due to the concerns arising from the increased use of personal data. Also, some risks to global economies existed resulting from restrictions of the flow of data across borders.[50]
>
> OECD has currently 34 member countries from various regions including many EU member states, Canada and the USA, Australia, Korea, Chile and Mexico[51]. Even though the Guidelines are not legally binding the member states and can be considered as *soft law*[52], they have been highly influential on the content and enactment of data protection legislation also in non-European jurisdiction.[53] The Guidelines have, for example, acted as a model for privacy principles of APEC (Asia-Pacific Economic Cooperation) Privacy Framework. In addition, many recommendations as well as provisions are built on OECD's Fair Information Privacy Principles which were the first internationally agreed privacy principles.[54]

[44] Pöysti, 355
[45] WP136, 4-5
[46] Herrmann, 234
[47] Bygrave, 2002, 31-32
[48] Korhonen, 2003, 126
[49] Lloyd, 27 and Konstari, 17
[50] OECD Guidelines 1980, see also Saarenpää, 2012 (2), 328
[51] OECD webpage, Members and Partners available at http://www.oecd.org/about/membersandpartners/
[52] Konstari, 30-33
[53] Bygrave, 2002, 32-33
[54] Pitkänen – Tiilikka – Warma, 14

Despite the technology-neutral nature of the Guidelines, the changed usage of personal data has created a need to update the Guidelines. New Guidelines[55] were adopted in 2013 and they include two new themes: (1) risk management approach when implementing the privacy protection regulation in practice, and (2) greater efforts to address global dimension of privacy through improved interoperability. In addition, several new concepts were introduced.[56]

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("CoE Convention")*, Council of Europe Convention on Privacy, ETS No. 108 (1981)*. The CoE Convention is a sole international treaty on the field of data protection[57]. The CoE Convention shares very same kind of privacy principles as the OECD Guidelines and it can be seen as a second remarkable legal instrument in addition to OECD Guidelines. The CoE Convention has a legally binding role in the international law and Finland has been part of the Convention since 1992.[58] The CoE Convention clearly reflects similar values and principles that are written into the ECHR. However, some differences exist. Firstly, the CoE Convention does not create direct rights for human beings to appeal to national courts. Secondly, the ECHR regulates mainly vertical relationships between individuals and authorities, whereas the CoE Convention regulates also the horizontal relationships between private persons.[59]

United Nations' Guidelines Concerning Computerized Personal Data Files, 14.12.1990 *(*hereinafter UN Guidelines). The UN Guidelines are an instrument to encourage UN Member States without data protection legislation to take steps to enact such legislation. Furthermore, another goal of the Guidelines is to encourage governmental and non-governmental international organizations to process personal data responsibly.[60] The principles laid down in the Guidelines cover lawfulness and fairness of processing, and regulation on transborder data flows. They include also requirements that data must be processed only for specified purposes and they must be accurate.[61] The UN Guidelines are more general compared to the CoE Convention and they haven't had that many effects in practice due to the non-legally binding status.[62]

The scope of the Directive is defined in Article 3. In short, Directive applies to wholly or partly automatic processing of personal data which form, or is intended to form, part of a

[55] Available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[56]OECD work on privacy, available at http://www.oecd.org/sti/ieconomy/privacy.htm
New concepts: Countries need to have *national privacy strategies* and *privacy management programs.* Also, a *data security breach notification* must be given to authorities and individuals when necessary.
[57] Bygrave, 2002, 30-32
[58] Korhonen 2003, 125
[59] Konstari, 16-17
[60] Bygrave, 2002, 33
[61] Solove & Schwarz, 168
[62] Konstari, 34 and Bygrave, 2002, 33

filing system. Further in my thesis I define what is meant by 'processing' and by 'personal data'.[63] There are certain areas of data processing that are excluded from the scope of the Directive (Art 3(2)). These areas are processing relating to national defense, security and criminal law as well as data processing by a natural person for his/her purely personal needs.

The Directive had to be implemented in the Member States[64] and it gave Member States flexible measures to improve national data protection taking into account the Member States' differing degrees of capability and willingness to integrate.[65] The Directive is, on the one hand, minimum directive because it allows the Member States to invoke more-detailed rules. On the other hand, the Directive is also a maximum directive granting the individuals rights which cannot be restricted more than already restricted in the Directive.[66] Because of the nature of the Directive the Member States' data protection laws differ from each other in structure, content and approach. Member States' national legislation may contain also data protection regulation in other laws such as in labor law. In addition, some Member States might have separate provisions for data processing made by public entities whereas some Member States do not distinguish between public and private entities.[67]

> **The Finnish Personal Data Act.** The first Finnish data protection act, Personal File Act (471/1987) came into force in Finland in 1988 and some parts of it came into force in 1989. The Personal File Act was struck down by a Personal Data Act which came into force in 1999. The Personal Data Act (523/1999) was a result of the implementation of the Directive[68] and it provides the foundation and principles for processing of personal data. The scope of the Personal Data Act reflects the scope of the Directive.
> Right to data protection is also ensured in Section 10 of the Finnish Constitution (731/1999)[69]. Section 10 of the Constitution states that protection of personal data must be further protected by law. The aim of Personal Data Act is to fulfill the requirements of the Constitution and safeguard the protection of fundamental rights of individuals in respect of the protection of their personal data[70]. Personal Data Act is a general act which has to be applied if there are no specific laws applicable. Such laws are, for example, the Act on Protection of Privacy in Electronic Communications (516/2004) and the Act on Protection of Privacy in Working Life (759/2004). Such special laws have to be applied over the Personal Data Act but the

[63] See about data processing in the chapter 6 and about personal data processing in the chapter 7.2
[64] Bygrave, 2002, 31: Countries (Norway, Liechtenstein and Iceland) that are part of the European Economic Area (EEA) but not part of the EU were bound to implement the Directive because the Directive was incorporated into the Agreement on the EEA on 25.6 1999. Also the new EU Regulation proposal is written with the EEA relevance.
[65] Heil, 39-40
[66] Saarenpää, 2012 (2), 329 and Herrmann, 236
[67] Kuner, 2007, 33
[68] Vanto, 17
[69] See the chapter 4.4 Privacy as a Fundamental Right.
[70] Pitkänen-Tiilikka-Warma, 28

Personal Data Act can complete the sometimes lacking or narrow contents of special laws. [71]

The Directive was legislated in the early 1990s and it was made technology-neutral. The legislators couldn't, however, even think about the fast development of data processing in the Internet and the huge amount of collected and shared data in the networks. New challenges in the data protection field as well as increased privacy risks demand an updated data protection legislation in the EU. European Commission has answered to this need to ensure stronger and more consistent privacy framework by giving its proposal for new EU Data Protection Regulation in 2012.[72]

3.2 New EU Data Protection Regulation

The Commission of the European Union has given its proposal for new EU Regulation in the field of data protection on 25th of January 2012. The legal basis for the Regulation is Article 16 of the Treaty on the Functioning of the European Union (TFEU) which provides everyone the right to the protection of their personal data. In addition, the paragraph 2 of Article 16 of the TFEU, which was added to the article by the Lisbon Treaty, provides the legal basis for the European Parliament and the Council to lay down rules to ensure protection of personal data.

The current data protection framework still includes the same aims and principles as it had two decades ago. However, the framework has not been sufficient to prevent the legal uncertainty in the field of data protection, and the risks related to the activities in the network environment. In addition, the incoherence of the implementation and enforcement of the data protection provisions in the Member States has resulted in the problem that the Member States are unable to sufficiently enforce the individuals' fundamental right to privacy[73]. All these reasons require the data protection framework to be updated so that the development

[71] Korhonen, 2014, 11

[72] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final 2012/0011 (COD)

[73] Protection of personal data, EU Charter Article 8.
COM(2012) 11 final 2012/0011 (COD), 8: The Commission has also taken fundamental rights of individuals into account in its proposal. It confirms the significance of Article 8 of the Charter related to the protection of personal data.

of new technologies, especially in the area of network environment, as well as the challenges related to globalization can be taken into account. Finally, according to Recital 13 of the Commission's proposal the Regulation should remain technology-neutral to cover the future developments in the area of data protection.

The new proposal provides effective enforcement of data protection rules to Member States to help digital economy to grow and develop in the EU Internal Market, as well as help individuals to control their data. This strengthens legal security and trust to the practical data protection.[74] In order to achieve a stronger privacy framework, the Commission sees regulation as the best way to satisfy the mentioned goal. The Regulation is directly applicable in all the Member States[75] and therefore it, on the one hand, reduces the incoherence between the Member States in the area of data protection legislation, and on the other hand improves the fundamental rights of individuals. Furthermore it contributes the activities in the Internal Market[76] and effectively ensures individuals' right to privacy when transferring their personal data outside the EU.[77]

As a conclusion, the most important reforms of the new EU Data Protection Regulation would be

- coherent data protection legislation in the Member States;
- right to be forgotten (however, this right is already granted for individuals by the Directive and confirmed by the ECJ judgment in Google Spain case[78]);
- stricter rules in relation to the consent of data subject, easier access to his/her data and re-use of data;
- obligatory notifications of data breaches and misuse of data,
- one-stop-shop meaning that companies can patronize with only one authority in one Member State;
- lighten administrational burdens;
- more authorized role of national data protection authorities;
- protection of minors;
- obligatory Data Protection Officer in the companies with certain amount of employees, and

[74] COM(2012) 11 final 2012/0011 (COD), 2-4,
[75] Article 288 of the TFEU: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."
[76] COM(2012) 11 final 2012/0011 (COD), 6
[77] COM(2012) 11 final 2012/0011 (COD), 6
[78] C-131/12

- establishment of European Data Protection Board to replace the current Article 29 Working Party.

To achieve these goals the Regulation will have three times more provisions than the Directive currently has.[79]

There has been progress in respect of the reform of the EU data protection framework. In March 2014 the European Parliament stated its strong support towards the new Data Protection Regulation. Parliament took the reports[80] of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas into account and accepted the changes they had suggested to the Regulation Proposal made by the Commission. EU Parliament has therefore stated its permanent and unchangeable opinion and the next step in the reform is that the Regulation needs to be adopted by the Council of Ministers using the "ordinary legislative procedure".[81]

4. Right to Privacy

Since search engine providers collect and process huge amounts of data it unavoidably creates risks to privacy of human beings. This is why I find it necessary to briefly explore the concept as well as the history of privacy. Right to privacy is not absolute[82], it needs to be in balance with other fundamental and human rights such as freedom of expression which includes the freedom to hold opinions and to receive and impart information and ideas.[83] In this context it needs to be noted, that search engine providers play an important role in the information society by making information easily accessible for Internet users, and the activities of the search engine providers improve the individuals' right to freedom of expression.

[79] Korhonen, 2014, 110-111
[80] Reports for Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee)
[81] European Commission, Press Release Database, Memo, 12.3.2014, available at http://europa.eu/rapid/press-release_MEMO-14-186_fi.htm
[82] COM(2012) 11 final 2012/0011 (COD), 41 paragraph 139
Also the ECJ has highlighted in the cases C-92/09 and C-93/09 (Volker und Markus Schecke ja Eifert) that the right to data protection is not absolute: it must be considered in relation to its task in the society.
[83] Also the Finnish Constitutional Law Committee has stated that those rights are included in the Finnish Constitution in the section regarding freedom of expression (The Constitutional Law Committee, PeVL 54/2002 vp). The Committee has also highlighted some viewpoints which may bring out some special characters related to the use of rights in respect of the freedom of expression (The Constitutional Law Committee: PeVL60/2001 vp, p. 2/I, PeVM 14/2002 vp, p. 3/II)

4.1 History of Privacy

Right to privacy in its modern meaning is a relatively new concept and right. Historically, however, the right to privacy as an idea has been present in the people's lives for a long time. In the Roman and Greek eras a clear division existed between what was considered public and private: all the activities related to state and government were considered public whereas all other activities such as family life was considered private. [84] Fundamentally the protection of privacy means person's right to keep personal things his/her own and not to reveal those to anyone without a justified reason.[85]

The legal regulation of privacy is often associated with the human rights declarations given in connection with the French Revolution. In the age of enlightenment people started to appreciate the privacy as a natural right.[86] Despite its long history, privacy as a concept took its place in the European jurisdiction only just in the past decades whereas in the United States privacy got attention in the jurisprudential discursion and legal praxis already in the end of 1800s[87]. According to Saarenpää, the reason for such a late entrenchment of the concept of privacy was the competition between two important, and at the same time a bit overlapping concepts, *right to privacy* and *right to private life.*[88]

In the Scandinavia privacy as a principle has been in a close relationship with the principle of publicity which stems from the regulation on freedom of printing press (1766)[89] (however, in Norway and Denmark the principle of publicity developed only in the 1970s). The Swedish-Finnish principle of publicity has been a model for Recital 72 of the Directive: "*Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive*". Earlier, the traditional basis in EC law used to be principle of secrecy and the publicity of documents was discretionary.[90]

[84] Neuvonen, 15
[85] Järvinen, 2010, 14
[86] Korhonen, 2003, 101, Konstari, 10
[87] See more about the privacy in the USA in the chapter 4.5
[88] Saarenpää, 2012 (2), 240
[89] Korhonen, 2003, 101
[90] Pöysti, 406, 408, 412

Privacy has been valued and understood differently during the ages. That makes it impossible to find common roots for the right to privacy. Privacy can be considered as an interpersonal concept[91] because it changes together with the culture and values in the society. The concept of privacy is not universal; it has to be evaluated against the set of values existing at a given time.[92] It seems that today people value their privacy but at the same time they couldn't imagine a life without social media and for example Google. Such information society services have made it easier for people to communicate, find information and share information in the Internet. This of course comes with a price: people are ready to give up of some of their privacy in order to be able to use such services.

In the future, when the individuals' right to self-determination, meaning the moral and personal autonomy of an individual[93], strengthens it will influence the importance of privacy in the society. Respectively the risks related to new technological developments and more common use of information technology increases. This will, and has already, impacted the significant growth and diversity of legislation.[94]

4.2 Concepts of Privacy and Data Protection

4.2.1 Concept of Privacy

Many people are confused with all the concepts related to privacy: what is meant with 'privacy', 'right to privacy', 'data protection', 'protection of personal data', and 'right to privacy of private life'. The confusion is natural because the concepts are often used as synonyms with each other.

The concept of privacy got more attention only in the 1990s when the governments realized the increased amount of data which had been collected into various registers. In addition the commercial use of the data became common. The collection of extensive amounts of information was made easy by technological developments. It also enabled the processing of

[91] Saarenpää, 2012 (2), 241
[92] Neuvonen, 12, 17, 22, 29
[93] Habermas, 151-165
[94] Saarenpää, 2012(2), 310

data by private entities whereas decades ago such processing was possible only for public sector.[95]

The concept of privacy is not defined in the Directive. Neither does the Finnish Data Protection legislation provide any definition. This is because of the relativity of the concept which has been taken into account in the Government Bill. It is clearly stated in the Government Bill for Personal Data Act that the protection of privacy can occur differently in different situations[96]. Privacy must be separated from the concept 'right to private life'. Privacy is more extensive compared to right to private life.[97] Protection of private life is considered as an element of privacy, a classical right of freedom, individual's right to live his life without unjustified interference to his private life.[98]

> The concept of privacy has always been problematic. Many researchers have had different kinds of approaches to the concept of privacy. **Bygrave** sees privacy as a "condition or state in which a person is more or less inaccessible to others either on the spatial, psychological or informational plane". Bygrave does not combine the right to privacy with autonomy (self-determination) meaning a person's capacity to control the flow of information relating to him/her even though he admits that privacy can result from the exercise of such control, and vice versa.[99]
>
> **Mahkonen** does not either connect the right to self-determination with privacy because that would result in situations where for example minors would not have a right to privacy. Privacy should be considered from the viewpoint of why privacy is important for a specific individual and how privacy can be violated. Mahkonen considers privacy from an anthropocentric view. He understands privacy as a condition of isolation which requires a social ritual by which a person isolates him-/herself from the others. Isolation is an element of privacy and privacy means the right to be alone. He sees privacy consisting of the right to personality and intimacy whereas data protection as a concept effects above the protection of privacy. Mahkonen uses three concepts to help to define the different aspects of privacy. *Distinctive* point of view highlights the uniqueness and specialty of privacy. *Coherent* point of view therefore brings out the parallel, but not similar, concepts related to privacy such as *privacy and secrecy. Equilibrium* seeks the balance between the opposite interests and goals. A good example would be the right to privacy vs. the right to freedom of expression. In the end privacy is about a meeting place where "I" and "we" attend at the same time. There is a right to privacy but at the same time also communal obligations. According to Mahkonen the starting point

[95] Järvinen, 2002, 30
[96] Government Bill, HE 96/1998
[97] Korhonen, 2003, 102
[98] Saraviita 366 and Pöysti, 483
[99] Bygrave, 2002, 23-24

must be given for "I" to highlight the uniqueness of an individual. The second place is given to the interests of society. [100] This is also the starting point of the ECHR.[101]

Neuvonen does not want to define privacy too strictly. Too narrow definition of privacy could also limit the protection of individuals. According to Neuvonen privacy is about right and social structure, an individual should be able to have a feeling that he/she can be alone also in other than physical ways and can practice self-determination.[102]

Saarenpää seeks means for defining privacy from the ancient Roman legal systematic way of dividing personal rights, property rights and family rights. From that division, a personal right is part of the branch of jurisdiction called 'personality law'[103]. Right to privacy is one of the main principles[104]of personality law. Privacy has its active and passive sides: Saarenpää sees privacy as our right to be alone in respect of other individuals, communities and society. Right to privacy includes also our right to determine how, when and at what price we disclose our personal things to others. [105] Privacy consists of a right to private life, confidentiality of communication, and protection of personal data. Protection of personal data can be seen as a part of privacy but processing of personal data is a wider issue related to our right to self-determination.[106] An interesting point is that in research made in the University of Lapland in the area of law and informatics, the rights related to *data* are considered own principles and they are not tied to the fundamental rights.[107]

4.2.2 Data Protection and Personal Data Protection

History of data protection internationally stems at the latest from the 1960s when there were discussions about modern data protection legislation.[108] In the 1980s data protection legislation achieved an internationally accepted role as an institutional framework for personal data protection.[109]

[100] Mahkonen, 11-19, 22, 63, 76, 81
[101] Mahkonen, 14
[102] Neuvonen, 22, 28
[103] Personality law researches the rights and freedoms related to our right to self-determination as individuals in the society. (Saarenpää, 2012 (2), 230
[104] Other principles of personality law are respect of individual, right to personality, and right to identity (Saarenpää, 2012 (2), 234)
[105] Saarenpää also divides privacy to ten areas: physical -, areal-, social-, media privacy, privacy in the protection of personal data processing, proprietary right to information, right to be evaluated in the right perspective, patient privacy and privacy in communications. Saarenpää 2012 (2), 310-318
[106] Saarenpää, 2012 (2), 221-223, 240
[107] Neuvonen, 25
[108] Saarenpää 2012 (2), 328
[109] Saarenpää 2012 (2), 320

The concept of data protection includes provisions which relate to the *right and protection of privacy* in the processing of personal data. [110] *Data protection* can be therefore seen as an upper concept for *protection of personal data*. The aim of data protection legislation is to protect *all data*, not only personal data.[111] Data protection can therefore be defined as a set of legal and/or non-legal measures which are aimed at safeguarding persons from any privacy violations, such as unlawful processing of personal data.[112]

Sometimes the concepts of *data protection* and *personal data protection* are used as synonyms even though *data protection* covers the whole field of general and special data protection legislation. Personal data protection in Europe includes mainly the Directive and the human and fundamental rights behind it. The Charter of Fundamental rights in the EU ("the Charter")[113] grants the right to data protection for individual and sets up obligations for public authorities as well as for private sector to ensure the protection of processed personal data.[114] This means that the right to data protection is ensured both in vertical (protection against public authorities) and horizontal (obligations of private data controller when processing personal data) relations.[115]

Originally personal data was collected for social aims like taxation and census.[116] The development of personal data protection started after the Second World War and the bad experiences related to the misuse of highly developed Dutch personal data registers in the Holocaust.[117] The history of *personal data protection* in Europe goes back to 1970s, Germany and the state of Hessen, where the protection of personal data began to develop as *data protection*. Also Sweden took part to this *first generation data protection legislation*[118] and enacted its first data protection act, *datalag*, in 1973.[119]

---

[110] Korhonen, 2014, 112 and Bygrave, 2002, 22:
Data protection must be separated from the overlapping concept data security (origins in German: Datensicherung / Datensicherheit). Data security can be understood as an instrument which ensures the confidentiality, completeness, and usability of the data.
[111] Saarenpää 2012 (2), 319
[112] Bygrave, 2002, 22
[113] Charter of Fundamental Rights of the European Union, (2000/C 364/01)
[114] Neuvonen, 65
[115] Neuvonen, 60, 65. See more about privacy as fundamental right in the chapter 4.4
[116] Konstari, 3
[117] Neuvonen, 59
[118] Saarenpää, 2012 (2), 328
[119] Konstari, 3

In the end it has to be noted that the informational rights related to the protection of personal data are therefore inalienable rights of individuals.[120] Therefore, a person has a control over his/her data. This enables the individual, for example, to make such data public in the situations which would define the personal data confidential by law.[121]

4.3 Privacy as a Human Right

Human rights are provisions which resemble the classical liberty rights as well as economic, cultural and social rights.[122] Human rights are non-assignable and belong to every natural person, independent of his/her origin, skin color, age, religion, sex or other characteristics.[123] Some people have, however, claimed that human rights represent the Western values too much and they adapt only to the Western jurisdictions and societies. This character might stem from the violations of human rights in the Second World War which started the development of the human rights in an international scope. The violations made clear that the national constitutions weren't sufficient to protect every individual. [124]

The first and perhaps the most remarkable human rights instrument is the Universal Declaration of Human Rights[125] which was given by the United Nations in 10.12.1948. It resembles the declaration given in connection with the French Revolution and has acted as a basis for other human rights conventions. The Declaration is not legally binding, but *soft law*. [126] However, it can be considered to be international customary law because almost every state has approved it. [127]

---

[120] Pöysti, 432
[121] Kemppinen, 42
[122] Saraviita 27
[123] Ojanen, 24-25: A human rights convention may protect companies indirectly. For example, Article 1 of the first protocol of the ECHR on the protection of property relate legal person already according to its wording: "Every natural or legal person is entitled to the peaceful enjoyment of his possessions."
[124] Ojanen, 3-4, 66
[125] Available at http://www.un.org/en/documents/udhr/
[126] Saraviita, 29
[127] Finland joined UN in 1955 and is a party to all UN conventions on human rights, such as International Covenant on Economic, Social and Cultural Rights; International Covenant on Civil and Political Rights; International Convention on the Elimination of All Forms of Racial Discrimination; Convention on the Elimination of All Forms of Discrimination against Women; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; and Convention on the Rights of the Child.

The most important legal instrument in the respect of human rights is the European Convention on Human Rights (ECHR) which has been framed by Council of Europe and signed by 12 member states on 4 November 1950. The ECHR entered into force on 3.9.1953. The UN Declaration gave the basis for the ECHR and vice versa, the Convention gave effect to the certain rights stated in the UN Declaration of Human Rights[128]. In addition, the ECHR established a supranational court to challenge the decisions made by national courts to ensure the effective execution of human rights in the member states. Any individual, company or non-governmental organization can appeal to the European Court of Human Rights provided that they have exhausted all national remedies.[129]

Article 8(1) of the ECHR grants everyone the right to have his private and family life, his home and his correspondence respected. This right can, according to Article 8(2) of the ECHR be interfered with public authority only when such interference is in accordance with the law and necessary in a democratic society. It can be seen that Article 8(1) has an individual idea of man as a starting point whereas Article 8(2) is steeped in communal scope[130]. In the 1970s, the Council of Europe was unsure whether Article 8 of the ECHR guaranteed sufficiently the protection for individuals in the processing of their personal data. This uncertainty was removed by the CoE Convention (1981)[131]. Privacy has had a highlighted significance in the international and national data protection legislation. Also, starting from the 1980s, the European Court of Human Rights has valued privacy more and as a result the right to protection of personal data as well as the right to private life have become independent rights which may be limited by other human rights such as freedom of expression.[132]

4.4 Privacy as a Fundamental Right

The fundamental rights are guaranteed for natural persons. However the fundamental rights may sometimes extend to give protection also for legal persons. This is because the

[128] Ojanen, 67
[129] Council of Europe, homepage http://human-rights-convention.org/the-texts/the-convention-in-1950/
[130] Mahkonen, 32
[131] See the chapter 3.1
[132] Neuvonen 17-18, 20

interference to the rights of a company may in fact affect the rights of the natural person behind the company (theory of indirect interference).[133]

The European Economic Community (EEC) was established by the Treaty of Rome[134] which didn't contain any fundamental or human rights that would bind the Community institutions.[135] After the Second World War the goals of the EEC related mainly to the economic integration of Europe and the existing fundamental rights related to economic issues, such as free movement of capital and work force.[136]

The lack of binding human and fundamental rights resulted in some negative reactions in the courts of the Member States, for example in Germany. When the precedence of EC law over the national laws was confirmed by the case *Costa v. ENEL*[137] it gave Member States a feeling that Community law had the precedence also over the fundamental rights granted in the national constitutions.[138] Later, the judgment *Solange-I* given by the German Federal Constitutional Court *(Bundesverfassungsgericht*) gave Germany the right not to obey the Community law in cases where it conflicted with Germany's fundamental rights granted in its constitution. This forced the European Court of Justice (ECJ) to consider national fundamental and human rights as a part of Community law as general principles.[139]

The ECJ was buttoned up for a long time against the ECHR and the legal praxis of the European Court of Human Rights[140]. The first time when the ECJ referred to the ECHR was in 1975, 25 years after the ECHR was enacted. Further, the first time when the ECJ referred to the praxis of the European Court of Human Rights was in the end of 1990s. This was extraordinary taking into account the fact that all EC Member States were part of the ECHR.[141]

The European Community proved to value fundamental rights when the ECHR and the Member States' fundamental rights were mentioned in the Treaty on European Union 1992

[133] Ojanen, 24-25
[134] Treaty establishing the European Economic Community, signed 25 March 1957
[135] Ojanen, 95
[136] Saraviita 16-17
[137] C-6/64
[138] Ojanen 95
[139] Saraviita 57-59
[140] When giving the judgment in the case C-131/12 the ECJ could have mentioned the decision of the European Court of Human Rights in *Times Newpapers Ltd. V. UK.* In that case the human rights court stated that Internet news archives fall within Article 10 of the ECHR protecting freedom of expression.
[141] Ojanen 96, 110, 115

(Treaty of Maastricht)[142]. Article F(2) of the Treaty of Maastricht states that "*The Union shall respect fundamental rights, guaranteed by the ECHR... and as they result from the constitutional traditions common to the Member States, as general principles of community law.*"

By the Treaty of Amsterdam[143] 1999 the ECJ was granted an authority to ensure the effective implementation of fundamental rights in the institutions of Union. Article 6(1) includes a general fundamental and human rights clause stating that the Union is based on the Member States' common respect towards democracy and fundamental and human rights. In addition, the European Social Charter (1961)[144] which guarantees social and economic human rights, was connected with other charters of fundamental rights by the Treaty of Amsterdam.[145] By the Treaty of Nice[146] (2001) the EU established a Charter of Fundamental Rights in the EU which covers all the traditional freedom rights as well as economic, civil and social rights.[147] The Charter highlighted the importance of the fundamental rights in the EU. At that time the Charter was not legally binding but was nonetheless referred several times by the ECJ[148]. Finally, by the Treaty of Lisbon[149] the Charter became legally binding on the EU institutions and on national governments, similarly like the EU Treaties[150].[151]

Protection of personal data has, on the European level, become a fundamental right.[152] Articles 7 and 8 of the Charter grant individuals the right to respect for private and family life, and the right to protection of personal data. However, the fundamental rights are not absolute rights and they can be limited if certain conditions are met (Article 52(1)). The Charter is significant, especially when EU deals with cases under its competence in the

[142] The Treaty on European Union (TEU), signed in Maastricht on 7 February 1992, entered into force on 1 November 1993
[143] The Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, as signed in Amsterdam on 2 October 1997
[144] The European Social Charter is a Council of Europe treaty which guarantees social and economic human rights. It was adopted in 1961 and revised in 1996.
[145] Saraviita 17, Ojanen 110
[146] The Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts
[147] Saraviita 17-18
[148] Ojanen, 101-104
[149] 2007/C 306/01, Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007
[150] The judgment C-131/12 demonstrates how the enactment of the Lisbon framework strengthens the standards for data protection under EU law (see Kuner, 2014, 28)
[151] Korhonen, 2014, 110 and the website for the EU Commission related to the Charter of Fundamental Rights available at http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm
[152] Saarenpää, 2012 (2), 240

Internal Market[153] such as the Google Spain case C-131/12. In addition, the fundamental rights are considered as primary law in the EU law which means that they act as a basis for secondary legislation such as EU regulations and directives, for example the Data Protection Directive.[154] For example, Articles 7 and 8 of the Charter played an important role in the Google Spain case.

The Charter also defines its relationship with the ECHR. It is stated in the Charter that the meaning and scope of fundamental rights has to be at least the same as granted in the ECHR. In practice this would mean that individuals might have better rights when applying the Charter than granted in the ECHR. Vice versa, the restrictions of human rights in the ECHR cannot be used to limit the rights granted in the Charter.[155]

All in all, the right to protection of personal data guaranteed in the Article 8 of the Charter confirms the principles of the EU Data Protection Directive and the extended interpretation of Article 8 of ECHR.

> **The Finnish Constitution.** Article 8 of the Charter is also in line with Section 10 of the Finnish Constitution (11.6.1999/731). When the Finnish Constitution was drafted the legislators took, for example, the provisions of the ECHR into account in order to bring the systems closer to each other.[156] In Finland the inhabitants are protected by, first of all the Finnish Constitution which is then completed by the international conventions on human rights. Such conventions were created by the Council of Europe, the International Labor Organization (ILO) and the United Nations.[157] These systems mentioned above are overlapping and they aim to protect the fundamental rights of human beings.[158]
>
> In the reform of the constitutional legislation (1995) the institutional right to privacy was included in the new Section 10 among with the new extended fundamental rights such as secrecy of confidential correspondence. Before the reform was made the right to privacy became materialized through the provisions protecting the secrecy of communication and domestic peace.[159]

[153] Neuvonen, 56
[154] Ojanen 113
[155] Ojanen, 105-107, 109
[156] Government Bill (HE 309/1993)
[157] Ojanen, 1
[158] Saraviita, 27
[159] Saraviita 364-365

The right to the protection of personal data is guaranteed in Section 10(1) of the Constitution. There it is written that "*More detailed provisions on the protection of personal data are laid down by an Act."* The protection of personal data is executed by multiple data protection laws, the most important of which is the Personal Data Act (523/1999). The proviso in 10(1) refers to a need to protect the privacy of individuals against both public and private sector[160].[161] Due to the narrow concept and the short history of the protection of personal data, it has not yet deserved a position as a fundamental right. Instead it is seen as a part of larger entirety of right to privacy.[162]

The first sentence of Section 10(1) is written: "*Everyone's private life, honor and the sanctity of the home are guaranteed."* The division of the concepts "*right to private life"* and *"right to privacy"* is not remarkable in this context, especially because the Committee for Constitutional Law has seen no significance in such distinction.[163] The right to private life is a classical liberty right which relates a little to the protection of domestic peace. It also covers the right personal identity[164].

4.5 Privacy in the USA

Because Google is a company established in the USA and with a US based views to privacy I find it necessary to have a look at privacy in the USA.

USA is part of the Western legal culture and more particularly the Common Law family. The culture is called Western because its ideologies stem especially from Europe.[165] Common Law is based on case law meaning judicial precedents made in the legal praxis. It must not be mixed with custom law meaning justice based on a customary practice. The core principles of the Common Law system are the *stare decisis doctrine* meaning the validity of the judicial precedents, pragmatic and improvising style, and lack of codifications, whereas the core of the Roman-Germanic family in Europe includes the precedence of written law, formality, deep distinction between public and private law, extensive codifications.

---

[160] Ojanen, 35: The fundamental rights protect both horizontally and vertically. In practice, fundamental rights between private persons may create tensions between opposite fundamental rights, such as right to privacy and freedom of expression.
[161] Saraviita, 370
[162] Neuvonen, 41
[163] The Finnish Constitutional Law Committee (PeVL 25/1998 vp.)
[164] Saraviita, 369, 379
[165] Husa, 145-148

In the US Legal system the privacy laws are concerned with the collection, use and disclosure of personal information.[166] The rights related to information are seen as copyrights, data use rights, data disclosure rights and data access rights. These rights are settled into the following fields of laws: copyright, patent, trade secret, privacy, communication and criminal law.[167] Originally the right of privacy in the US was conceived as a right to inviolate personality independent of any rights of property. Later, the right of privacy became a means of protecting economic interests described as 'property' or 'proprietary' interests.[168]

The history of privacy in the USA goes back to 1890 when Warren and Brandeis published their famous article "The Right of Privacy". They stated that individual's protection in person and in property is a principle as old as the common law, however the exact nature and extent of such protection has to be defined again from time to time to meet the demands of the changing society. In their article Warren and Brandeis came to the conclusion that the right to life means the right to enjoy life and therefore also the right to be let alone.[169] Also William O. Douglas (1898-1980), the Judge of the US Federal Supreme Court has stated that "The right to be let alone is indeed the beginning of all freedom"[170]. The right to privacy in the US is based on judicial precedents[171] given by the courts. Little by little this system has created a network including cases[172] related to the right to privacy.[173] Also the articles of researchers during the years have had an impact on the development of the right to privacy.[174]

The US Constitution (1787) has had a highlighted status in the US legal system and the whole legal system leans strongly to the Constitution which is hierarchically above other laws. Especially the first ten amendments (Bill of Rights) of the Constitution relating to the fundamental rights of US citizens, have a significant position in the legal system. The US Constitution consists of case law created by the US Federal Supreme Court, which takes the

---

[166] Solove & Schwarz, 166
[167] Korhonen, 2003, 295-296
[168] Beverley-Smith, 281
[169] Warren & Brandeis, 289-290
[170] Järvinen, 2010, 14
[171]The two earliest cases dealt with privacy of letters. However, in the 1890s there were a few cases that spoke definitely of the personal right of privacy without connection to property, contract or breach of confidence (Hofstadter and Horowitz, 15-17)
[172] The oldest case related to the right to privacy was *Boyd v. United States (1886)* where a citizen was protected from an illegal interference of the State.
[173] Mahkonen, 35
[174] Korhonen, 2003, 108-111: Important researchers were William L. Prosser who analyzed four privacy related objects which could be violated (1960); and Alan Westin who, in his article Privacy and Freedom (1967), discussed the basic conditions of privacy meaning solitude, intimacy, anonymity, and reserve.

principles set out in the Bills of Rights as well as legislation of the federal states into account when giving precedents[175]. The US courts are not bound to the judgments they have given. This is mainly because the reform of the US Constitution is extremely difficult. Therefore an easier way to change the law is to interpret it differently. [176]

Because the US Constitution does not guarantee the right to privacy (except in the 4th Amendment to domestic peace and protection of confidential communication), the 14th Amendment of the Constitution (constitutional protection of property) has been referred to when there is a need to protect one's privacy. This has led to the situations where the value of the data has to be examined and therefore personal data has been associated with the protection of property.[177]

The protection of personal data in the USA is structured by economic and marketing solutions. USA has a model called *the property rights model* which aims to protect personal data. According to the model an individual has a right to *sell* his/her personal data and get back some of the value which the personal data has in the market. This model provides a new approach to the intellectual property rights of information. Many American companies spend a lot of time, money and energy in collecting, organizing and processing of personal data. Therefore they consider themselves as owners of such information.[178]

In the US the right to indemnities acts as a basis for right to privacy. Also Warren and Brandeis took the right to indemnities as a starting point for their famous article[179]. The right to indemnities means that if privacy of an individual is violated, the individual can require compensation for damages resulting from such a violation. Therefore personal data as well as privacy in general can be seen as property of person of which the person can determine by himself.

In Europe privacy has traditionally had its basis in the human and fundamental rights.[180] The conflict between the strict protection of personal data in Europe and the free enterprise in the

[175] Mahkonen, 35
[176] Husa, 145-148, 157-158, 167-170
[177] Neuvonen, 68-69
[178] Korhonen, 2003, 296-298
[179] Warren & Brandeis, 319: "An action or tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel."
[180] Neuvonen, 69

US is big. This creates tensions between American companies and European legislation.[181] Also the disclosures that Edward Snowden made about the United States' National Security Agency (NSA) spying on European countries raised the tension even more in 2013. NSA as well as other agencies in the Western countries, for example Sweden's National Defence Radio Establishment (FRA = Försvarets radioanstalt), had spied on communications which had gone through Sweden. The spying has later been justified by telling citizens that it improves both national and citizens' safety. This safety-thinking originates from the terror attacks in New York in 2001 which changed many countries' attitude towards the restrictions of privacy: national safety can restrict individual's right to privacy.[182]

5. The World of Search Engines

5.1 Google as an Example

Google was established in 1998 by two students Larry Page and Sergey Brin. The markets for search engines were totally different back then: the field was monopolized by AltaVista, which started its search engine as a mere research project in 1995. However, Google soon took the search engine markets and its search algorithm proved to be excellent: a minimalistic search page with no advertisement and nothing extra on it, just a quick and effective search. In 2004 Google listed to the stock exchange and figured out a new way to do business: smart marketing. It started to collect user data which it sold further to advertisers in the World Wide Web (WWW) in order to be able to allocate the ads better to Internet users. Google as a huge stock company is not a "free service". It does what it does to show a profit to its stock owners.[183]

The Article 29 Working Party (WP29)[184] has acknowledged the crucial role of search engine providers in the information society as intermediaries. Search engines contribute on the development of the information society and therefore are necessary in today's world.[185] It

[181] Järvinen, 2002, 414
[182] Neuvonen, 19-20
[183] Järvinen, 2010, 221
[184] Article 29 of the Directive sets up a working party (WP29) on the protection of individuals with regard to the processing of personal data. The WP29 shall have advisory status and act independently.
[185] WP148, 5

seems, however, there is a conflict of opposite interests in the activity of the search engine providers. Firstly the protection of data related to data subjects must be taken into account and secondly the interest of data controllers and the media are important as well.

From the viewpoint of information society services, the most important task that search engines are doing is to help their users to find information on the Web. This information can be found in various formats: text, pictures, videos, sound and others. This task is very important because there billions of web pages on the World Wide Web and it would be extremely difficult to find information without a search engine, which process information by crawling, analyzing and indexing the web[186].

Some search engines are specifically aimed at building profiles of people based on personal data found from the Internet. This is the bad side of search engines when it comes to protecting the Internet user because the profile created in the Internet can affect individuals if the personal data in the search results are incorrect, incomplete or excessive.[187] Our private lives are open to surveillance more than in the past. The public identity created by a search engine gives an image about an individual to the search engine user, who makes the search about someone. This public profile may affect how we view our colleagues and friends, and vice versa, how they see us.[188]

Search engines process huge amounts of various types of user and content data, for example search queries meaning the search history of an individual revealing person's interests, relations, and intentions[189]. This data is used for commercial purposes as well as for data mining by law enforcement authorities or national security. Search engine may also republish data in a so-called 'cache'. [190]

[186] WP148, 13
[187] WP148, 5
Note also that the ECJ confirmed a right to be forgotten for individuals by the case C-131/12.
[188] Halavais, 139
[189] See the chapter 7.2.1 about user and chapter 7.2.2 content data.
[190] WP148, 5-7, See more about the cache functionality and search engine as a data controller in the chapter 9.1

5.1.1 Case C-131/12 – Google Spain v. AEPD and Mario Costeja Gonzáles

Search engines have become an ineradicable part of our daily life. Also, it is rare for someone not to appear by name somewhere in the Internet. However, when a person appears on a search engine that has an effect that person is put on the global stage[191]. This has led to ego-surfing and self-googling: people want to monitor the image which is given of them in the Internet. Such "*personal brand management"* in the Internet gives a temptation to shape one's own image given by search engines.[192] For individuals it is important to know what other Internet users might see when googling one's name. The search result may give the first impression of a person. If the description of the person in search results is incomplete, lacks important features or emphasizes certain ones, image of a person to others might be totally wrong.[193] Other possibility is that search engines reveal material that is related to an individual but does not put him/her in the best light. Instead, such information in the search results may give a person bad publicity and haunt him/her for years.[194]

Self-googling was also done by Mr. Mario Costeja González, a Spanish national resident who entered his name into Google's search engine and as a result obtained links to two pages of the newspaper La Vangurdia Ediciones SL ('La Vangurdia) which publishes a daily newspaper with a large circulation in Catalonia. Those pages included an announcement of a real-estate auction connected with attachment proceedings for the recovery of social security debts. Mr. Costeja Gonzáles' name appeared in connection with those announcements dated in 19th January and 9th March 1998.

On that basis Mr. Costeja Gonzáles lodged a complaint with the Spanish Data Protection Authority (AEPD) against La Vanguardia and against Google Spain and Google Inc. By the complaint, Mr. Costeja Gonzáles requested La Vangurdia to remove or alter appeared pages so that the personal data related to Mr Costeja Gonzáles would no longer appear in the results of search engines. Mr. Costeja Gonzáles also requested Google Spain or Google Inc. ('Google') to remove or conceal the personal data related to him in connection with the links to La Vangurdia from Google's search results. According to Mr. Costeja Gonzáles those

[191] Halavais, 140
[192] Halavais, 140
[193] Halavais, 141
[194] Halavais, 142-143

results containing his personal data are no longer relevant because the proceedings which they relate to have been fully resolved years ago.[195]

The AEPD rejected Mr. Costeja Gonzáles complaint against La Vangurdia on a basis that the publication of the information related to real-estate auctions was legally justified and it had taken place upon order from the Ministry of Labour and Social Affairs. Furthermore the announcement was published to give maximum publicity to the auction. Instead, the complaint against Google was upheld and the AEPD considered that operators of search engines are subject to European data protection legislation because they process data for which they are responsible and at the same time act as *intermediaries* in the information society. The AEPD stated that locating and disseminating data by the search engine providers may endanger individuals' fundamental right to data protection and the dignity of persons in general. Therefore AEPD held Google liable for data processing it carries out in the context of its searching services and required Google to withdraw Mr. Costeja Gonzáles' personal data from its search results. The AEPD didn't find necessary the erasure of data from the source website, La Vangurdia's website, in where the data appeared the first time.[196]

On the basis of AEPD's decision, Google brought separated actions against that decision before the Audiencia Nacional, the National High Court. The court joined the actions. The court raised a question related to obligations of search engine operators. Are search engine providers responsible for protecting personal data of individuals in the case where individuals "do not wish that certain information, which is published on third parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to Internet users indefinitely". According to the court, the answer to that question depended on the interpretation of the Directive 95/46 to which the court decided to ask for a preliminary ruling[197] from the European Court of Justice.[198]

Further in my thesis I will question the role of search engine – are they data controllers or perhaps some other actors in the data protection playfield? In addition, I will research the main definitions related to the Google case: processing and personal data. Before those

[195] C-131/12, paragraphs 14-15
[196] C-131/12, paragraphs 16-17
[197] Treaty on the Functioning of the European Union, Article 267 on preliminary ruling.
[198] C-131/12, paragraphs 18-20

definitions, I will shortly write about the Courts decision in the Google case related to the territorial application of the Directive.

5.1.2 Territorial Application of the Directive in the Case C-131/12

Territorial application[199] of the Directive is important for the reason that if the Directive was not applicable in the case, there would be no further questions to be answered related to responsibilities of non-European search engines in the European market. The Directive and therefore national laws shall be applied to the case C-131/12 according to Article 4(1)(a) of the Directive if

> "(a) the 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;

The European Court of Justice has stated in the case C-131/12 (Google Spain) that the processing of personal data is carried out in the meaning of Article 4(1)(a) when the operator of a search engine sets up a subsidiary or branch in a Member State, and if the intention of such subsidiary is to promote and sell advertising space offered by that search engine which orientates its activity towards inhabitants of that Member State.[200] The statement of the ECJ receives support from Recital 19 of the Directive which states that the determining factor in

[199] Commission proposes in it Proposal for new Data Protection Regulation (COM(2012) 11 final 2012/0011 (COD)) that the Regulation shall apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union (paragraph 1). Additionally, the Regulation shall apply to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are **aimed at** (original proposal was written "related to" but amended by Albrecht report, changes in bold): **(a)** the offering of goods or services to such data subjects in the Union**, irrespective of whether payment is required for the goods or services** …; or (**b**) the monitoring of such **data subjects**. Originally the paragraph (a) was written without the bolded part. It was later amended by the Albrecht report to include a reference to the payment. Paragraph (b) was written as follows: "the monitoring of their behavior" but was also amended later by the Albrecht report because the term "monitoring behavior would be too narrow and not include collection and processing of personal data about Union residents. The proposal and amendments thereto have been accepted by the EU Parliament in March 2014 and they will not change anymore.

[200] C-131/12, paragraph 100(2)

respect of the establishment is the effective and real exercise of an activity through stable arrangements. Legal form of such establishment is not the determining factor.

According to Google, however, the processing of personal data in the case C-131/12 is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain. Google claimed that Google Spain's activity is limited to providing support to Google group's advertising activity which is separate from its search engine service.[201]

The ECJ stated, however, that "the Directive does not require the processing of personal data in question to be carried out '*by'* the establishment concerned itself, but only that it be carried out '*in the context* of the activities' of establishment.[202] Therefore, since Google Spain promotes and sells advertising space offered by the search engine, the processing of personal data for the purposes of the service of a search engine is carried out 'in the *context* of the activities' of the establishment of Google Spain in the Member State.[203] Furthermore, the display of personal data on a search results page constitutes processing of such data. Since the display of advertising linked to the search terms is shown together with search results including personal data, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State.[204] Therefore Google Inc. was considered to be the data controller in the case.

Additionally, in order to protect the fundamental rights and freedoms of natural persons which the Directive seeks to ensure, in particular their right to privacy, the ECJ stated that it cannot be accepted that "the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by the Directive".[205] Even though the case has significant implications internationally and in relation to Internet the ECJ failed to say anything concerning the effects of the case on the

[201] C-131/12, paragraph 51
[202] C-131/12, paragraph 52
[203] C-131/12, paragraph 55
[204] C-131/12, paragraph 57
[205] C-131/12, paragraph 58
See also: C324/09 L'Oreal (paragraphs 62, 63). The situation, in which a company located in a third state offering services targeted at consumers within EU and having no obligation to comply with EU law, cannot be accepted because such situation would undermine the effectiveness of EU rules.

Internet as well as for non-EU data controllers.[206] The judgment gave an effect to the Directive in the Internet outside the borders of the EU meaning the non-European companies with personal data processing activities in connection with the establishment of a subsidiary to the EU. The judgment of the ECJ is interesting when taking into account the ECJ's earlier judgment *Lindqvist* in which it stated that "the Directive should not be interpreted so as to be applicable to the entire Internet"[207].

> The international aspects of the ruling create interesting questions. How, for example, to act with companies which are not established in the EU in the meaning of the Directive and the interpretation of Article 4 in the case C-131/12? What is the significance of the judgment in such situations where webpages, which are registered for example in the US, have nothing to do with the EU? Should they be under the scope of the EU law on the basis that they are accessible by the EU-citizens, or on the basis that the judgment gives *everyone* a right to be forgotten (see below)? In my opinion a wide interpretation of the judgment might be necessary in the future to allow an effective and practical protection of individuals. However, it should be remembered that the freedom of expression should not suffer from such protection. One and a rather absurd option to clarify the territorial application of the EU data protection law would be to technically create boundaries to the accessibility of the Internet, meaning that only Americans could access US based websites, EU-citizens could access EU-based websites etc. However, I do not support such an option because it would weaken the freedom of expression and the global economy. However, some kind of common rules such as internationally binding conventions should be adopted in the future in respect of online services accessible globally to everyone.

The ECJ did not limit the individuals' right to be forgotten to the EU citizens but allowed it to all natural persons[208]. This means that an individual with no connection to EU other than the fact that he/she uses Internet services that are also accessible in the EU, can seek for the right to be forgotten[209]. This kind of a possibility could lead to forum shopping and "right to suppression tourism[210]" by non-EU citizens.[211] Such an unlimited possibility to apply the Directive around the world is in conflict with the ECJ's statement in the *Lindqvist* that the

[206] Kuner 2014, 14
[207] C-101/01 Lindqvist, paragraph 69
[208] Recital 2 of the Directive: Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals. In addition, Article 8 of the Charter guarantees the right to data protection to everyone.
[209] Note, however the WP225, 8: in the new guidelines given by the WP29 the EU DPAs have stated that they will focus on claims where there is a clear link between the data subject and the EU.
[210] Kuner, (2014, 9) prefers to use "right to suppression" instead of "right to be forgotten" because the personal data are delete only from the search results of the search engine, not from the entire Internet.
[211] Kuner, 2014, 14-15

Directive should not be interpreted so that it is applicable to the entire Internet. Therefore, some limits should be set up in order to obey the previous judgment.[212]

5.2 Regulation of Search Engines

Due to technology-neutral nature of many EU legal instruments, search engines are not directly defined anywhere in the data protection legislation of the European Union. The ECJ, however defines the "*Internet search engine*" as "a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference"[213] This definition covers the major providers of Internet search engines such as Google, Bing and Yahoo.[214] The question is, therefore, does the definition cover other internet service providers who provide search services with a large-scale functionality such as new databases, Internet archives and social networks? According to Kuner, it is not possible to make a distinction between the large Internet search engines and other service providers due to the strong basis of the judgment on fundamental rights. Therefore the definition of the 'internet search engine' should be broadly interpreted to cover a variety of online services that provide search functionality and not just the major search engines.[215] Other opinion was given by the WP29 which stated, concerning the case C-131/12, that the scope of the ruling should not be extended to "internal" search engines meaning search tools of websites, in particular search tools of newspapers' websites. This is because those "internal" search engines do not establish a complete profile of the individual but only search for information from a certain webpage. [216] The ruling should therefore only cover "external" search engines meaning the major search engines such as Google, Bing, and Yahoo.

What laws then apply to search engine providers when they provide search functionalities? If a search engine provider processes personal data or decides the purposes and means of such processing in the meaning of the Directive the provisions of the Directive must be

[212] Kuner, 2014, 16
[213] C-131/12, paragraph 21
[214] WP29 Press release: European DPAs meet with search engines on the "right to be forgotten", 25 July 2014
[215] Kuner, 2014, 9-10
[216] WP225, 8

complied with (the material scope of the Directive in Article 3(1)). Later in my thesis I will question the applicability of the Directive in relation to the activity of search engines: do search engine providers process *personal data* and if so, do they *determine the purposes and means* of the processing.[217] If the Directive is applicable that means that also the national data protection laws, which are established by implementing the Directive, are applicable in the case where the conditions of the territorial scope of the Directive are fulfilled (see Article 4(1) of the Directive)[218].

In the context of the eCommerce Directive (Directive on Electronic Commerce, 2000/31/EC), which was enacted to develop and improve the electronic commerce in the Internal Market[219], search engines have been denoted namely as information society service providers providing information location tools[220]. This means that they provide services to help Internet users locate the information they need quickly. According to the Article 1(2) of the Directive 98/48/EC[221] information society service means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[222]. All these four criteria need to be fulfilled in order for a service to be an information society service defined in the eCommerce Directive. In addition, the information society service needs to have an economic purpose.[223]

The eCommerce Directive has been implemented in Finland as the "Act on provision of information society services (458/2002), hereinafter eCommerce Act. It seems that search services provided in the Internet can be considered as information society services[224] if they fulfill all the four requirements mentioned above in connection with the directive 98/48/EC. The only problem seems to relate to the requirement of remuneration since the users do not usually pay for service provider when they use search engines. However, in the Finnish Government Bill it is stated that the remuneration can be received not only explicitly from

[217] See the chapter 7.2 about search engines processing personal data, and chapter 9 about search engine's role
[218] See more about the Finnish Personal Data Act (523/1999) in the Chapter 3.1
[219] Korhonen, 2014, 80-81
[220] WP148, 5
[221] Article 2 of 2000/31/EC refers to Directive 98/34/EC which specifies the concept of information society service. Directive 98/32/EC amends the Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.
[222] See also Recital 18 of the eCommerce directive which defines the information society service more detailed.
[223] Innanen & Saarimäki, 62-63
[224] Innanen & Saarimäki, 229-230

the users of the service but also elsewhere, for example from advertisers.[225] As a conclusion, the eCommerce Act could be applicable to search engines. However, in the end, the role and liabilities of Internet search engine providers in the eCommerce Directive is still not that clear. This is noted also in Article 21(2) of the eCommerce Directive which states that there is a need "*for proposals concerning the liability of hyperlinks and location tool services"* clearly meaning the Internet search engine providers.

There is also another directive I want to introduce as a potentially applicable directive in relation to Internet search engine service providers: ePrivacy Directive (2000/58/EC), which has been implemented in Finland as the "Act on the Protection of Privacy in Electronic Communications (516/2004). This directive applies to service providers who provide electronic communications service, meaning "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting*" (Art 2(c) of the directive 2002/21/EC[226]). However, the definition does not apply to search engine services when search engine providers exercise editorial control over the content that is transmitted. Google, for example, provides search results in a particular order of preference. According to Article 2(c) of the directive 2002/21/EC "*services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are excluded."*. ePrivacy Directive normally applies to telecommunication companies as well as companies who provide public communication networks for the group of people which, however, has not been defined in advance.[227]

If applied strictly, search engines do not, in general, fall under the scope of the new regulatory framework for electronic communications of which the ePrivacy Directive (2002/58/EC) is part.[228] However, if a search engine provider offers additional services they may fall under the scope of an electronic communications service. This kind of service could be, for

[225] Government Bill (HE 194/2001 vp), Detailed groundings for Section 2 "information society service". Also the Finnish Data Protection Ombudsman Reijo Aarnio mentioned in our discussions on 8.10.2014 that the eCommerce Act should be applied to search engine providers because they clearly provide information society services, regardless of whether such service costs or doesn't cost to the user.
[226] Directive 2002/21/EC for a common regulatory framework for electronic communications networks and services, which covers also the directive (2002/58/EC)
[227] Helopuro- Perttula –Ristola, 1
[228] WP148, 12

example, a publicly accessible email service[229]. Such a service would have previously fallen under the scope of the Data Retention Directive 2006/24/EC. However, this directive was found invalid by the judgment of EJC in joined cases C-594/12 and C-293/12[230].

6. Data Processing

It is important to notice that the Directive applies only when *personal data* are *processed.*[231] Also, all the legal restrictions of the Directive are directed towards the 'processing of personal data'. [232] The Directive applies both to automated data processing and to manual processing to the extent that such data 'form or are intended to form part of a filing system'[233]. However, there are some exceptions to the material scope of the Directive listed in Article 3(2)[234].

Processing is defined in Article 2(b) of the Directive very broadly:

> *Processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by*

[229] WP148, 12

[230] **Digital Rights Ireland Ltd,** C-594/12 and C-293/12. The main goal of the Data Retention Directive was to harmonize Member States' legislation "concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or public communications networks". Such data includes for example traffic and location data as well as related data necessary to identify the individual "for the purpose of the prevention, investigation, detection and prosecution of serious crime" such as terrorism.
The court stated that "by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data… Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that interference is actually limited to what is strictly necessary… By adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality."

[231] Kuner, 2007, 98-99

[232] Kuner, 2007, 75

[233] Directive 95/46, Article 2(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

[234] Directive 95/46, Article 3(2). This Directive shall not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[235]

The concept of processing exists also in the CoE Convention, but is a little narrower than in the Directive. The definition in the CoE Convention does not, for example, cover the collection of data nor data processing carried out entirely manually. However, there is a possibility for Contracting States to apply the rules laid down in the CoE Convention also to data processed manually. In the OECD Guidelines, as well as in the Directive the regulatory focus is on the 'processing' of personal data regardless the way in which the data are organized.[236] In the Finnish Personal Data Act processing is defined in Section 3(2): *processing of personal data* means the collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data. The broad definition of processing means in practice that almost all the actions directed at personal data are considered processing if not excluded by law.[237]

There are several judgments given by the European Court of Justice which reflect the broad definition of processing in the meaning of the Directive. The most famous case in relation to Internet and processing is called case *Lindqvist*. In its judgment in the Lindqvist case the ECJ stated that placing information about individuals on an Internet site constitutes 'processing' of personal data.[238] In the case Österreichischer Rundfunk and Others, the ECJ stated that when personal data is processed, "all processing must comply, first, with the 'principles relating to data quality' set out in Article 6 of the directive and, second, with one of the 'criteria for making data processing legitimate' listed in Article 7[239]. The Court also stated in the same judgment that when the provisions "govern the processing of personal data liable for infringe fundamental freedoms, in particular the right to privacy, must [the Directive] 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

[235] In the Commission's proposal (page 41) "processing" is defined as follows (parts different than in the Directive are in bold):" 'processing' means any operation or set of operations which is performed upon personal data or **sets of personal data**, whether or not by automated means, such as collection, recording, organization, **structuring**, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction"
[236] Bygrave, 2002, 51
[237] Vanto, 28-29
[238] Case C-101/01 Lindqvist, paragraph 25
[239] C-465/00 - Österreichischer Rundfunk and Others, paragraph 65

ensures." [240] Noteworthy is, that not all personal data processing creates threat to privacy of individuals. For example, authorities might have a legal authorization to process personal data to ensure the benefits and security for an individual.[241]

6.1 Data Quality and Legitimate Processing

The Directive sets out conditions for processing of personal data. **Article 6 of the Directive contains the principles relating to data quality**[242]. Firstly, personal data must be processed fairly and lawfully and it must be collected only for specified, explicit and legitimate purposes which must be clearly communicated[243] to data subjects before collecting the data[244]. Personal data cannot be processed later for any other purposes (exceptions exists, such as processing for historical, statistical or scientific purposes) than the purposes decided before collecting the data. Companies must, therefore, in practice always keep in mind what the purpose of the processing is when collecting personal data.[245] This is always important but especially in today's world with complex digital networks where huge amounts of data are collected and the temptation to use personal data for multiple other purposes than the original one may increase.

Personal data must be suitable for purposes meaning that they must be adequate, relevant and not excessive in relation to the purposes for which they were originally collected. This means that only certain amount of data should be collected which is sufficient to fulfill the purposes. Data controller has to ensure, by taking reasonable steps, that the personal data are accurate and kept up to date. If the personal data is no longer needed for the purposes for which they were collected, data controller must take care of the destruction of such data. These principles

[240] C-465/00 - Österreichischer Rundfunk and Others, paragraph 68 (refering also to the case Connolly 274/99 P)
[241] Järvinen, 2002, 30
[242] In the Finnish Personal Data Act (523/1999) the principles related to data quality are implemented to the chapter 2 and are the following ones: principles of accuracy (including obligations to (i) plan the processing of personal data, (ii)protect personal data and (iii)assessment of necessity of data. Data must also be accurate, correct and relevant, and processed only for legitimate purposes in the necessity needed.
[243] See Articles 10 and 11 of the Directive. In practice, data subjects are informed by a register caption made by data controller.
[244] Kuner, 2007, 100
[245] Kuner, 2007, 100-101

create a life cycle for personal data and Article 6(2) gives data controller obligations to comply with the above mentioned principles.

In the Commission's proposal for the Regulation the principles related to personal data processing correspond those mentioned in Article 6 of the Directive with couple additional elements.[246] Such elements are principles of transparency, data minimization, and the establishment of a comprehensive responsibility and liability of the controller.[247] The mentioned principles require that data subject should be informed of the existence of the processing operations, purposes of them and the life cycle of data collected. Also other rights of data subjects should be informed.[248] The principle of transparency requires that any information, when it is addressed to the public or to the data subject, should be easily accessible and written in clear, plain and understandable language. Principle of transparency is important especially in situations where the increase of actors and technological complexity in practice are present, such as online advertising. Furthermore, children should deserve specific protection.[249]

Article 7 of the Directive includes the criteria for making data processing legitimate.[250] Data controller must obtain an unambiguously given consent from the data subject. The consent is defined in Article 2(h) of the Directive to mean "freely given specific and informed indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Because the Directive was implemented by the Member States, the requirements related to a consent vary on a country basis. Some national laws impose more strict requirements for a consent whereas in some Member States the requirements are not that strict but still in the line with the conditions set out in the Directive. In the Finnish Personal Data Act, in Section 3(7) the consent means "any voluntary, detailed and conscious expression of will, whereby the data subject approves the processing of his/her personal data". The consent does not necessarily have to be written but data subject must be informed, for example by privacy statement, the purpose of the use of his/her personal data. Even though the consent is not written it must be a conscious choice made by the data subject.

[246] COM(2012) 11 final 2012/0011 (COD) 23
[247] COM(2012) 11 final 2012/0011 (COD), 8
[248] COM(2012) 11 final 2012/0011 (COD), 25, paragraph 48
[249] COM(2012) 11 final 2012/0011 (COD) 24 paragraph 46
[250] Finnish Personal Data Act (523/1999), Section 8 contains the general conditions for data processing based on the Directive.

Furthermore, even a silent consent may fulfill the requirements of the definition; however, in a conflict, the data controller has the burden of proof to demonstrate the existence of a consent.[251]

In the Commission's proposal for the new Regulation[252] (Article 4(8)) the consent should be freely given, specific, informed and explicit indication of data subject's wishes. The word "explicit" has been added to the definition to avoid a confusing parallelism with the "unambiguous" consent.[253] According to the Albrecht report, data subject's consent should also be bound to one or more specific purposes.[254]

If no consent is asked from the data subject, processing must be necessary for example for protecting the vital interests of the data subject or to perform a contract to which the data subject is a party. Processing can be carried out also if it is necessary for a controller to be in compliance with legal obligations or if processing is carried out in the public interest. This means that the controller might be obliged to meet certain obligations that might need to be carried out by governmental authority. This becomes materialized often when the governmental activities are outsourced to the private sector and the line between governmental functions and private sector activities is blurred[255].

Processing is also possible without a consent if it is necessary for the legitimate interests of the controller or for the third parties whom the data are disclosed to. However, data cannot be processed for such purpose if such interests are overridden by fundamental rights and freedoms of the data subject, such as individual's right to privacy. The definition of "legitimate interests" varies depending on national law[256]. Article 7(f) of the Directive tries to balance the interests of both data controllers and data subjects. Therefore it has to be interpreted case by case and the priority must be given to the fundamental rights and freedoms

[251] Government Bill (HE 96/1998), detailed groundings, chapter 1.1
[252] COM(2012) 11 final 2012/0011 (COD), 42
[253] COM(2012) 11 final 2012/0011 (COD), 8
[254] Albrecht report, amendment 89
[255] Kuner, 2007, 244
[256] Kuner, 2007, 77

of data subjects. In addition, for Article 7(f) to be applicable, data controller must process personal data legitimately, the legitimate interests are not enough[257].

> In the case C-131/12 the legal ground for the processing personal data can be found in Article 7(f). However, the fundamental right to privacy of a data subject prevails as a general rule and it overrides the economic interests of the search engine. Individual's right to privacy and data protection also generally prevails over the rights of Internet users who want to have access to personal data through search engines when the search is made by using the person's name.[258]

The proposal of the Commission proposes that also in the future the legitimate interests of data controller may form the basis for data processing.[259] However, the part of Commission's proposal concerning legitimate interests has been deleted and amended by the Albrecht report and a new and more detailed provisions have been accepted instead. The justification for the amendment was that the new text gives clearer guidance and provides legal certainty for data processing based on legitimate interests of the data controller. [260]

Other content of the proposal related to data processing are conditions of the lawfulness of the processing of personal data of children in relation to information society services offered directly to them. In addition, the proposed Article 9 sets out the general prohibition for processing special categories of personal data and the exceptions from that general rule. The Article 9 of the proposed Regulation is built on the current Article 8 of the Directive relating the processing of special categories of data such as sensitive data.[261]

---

[257] Kuner, 2007, 245
[258] WP225, 3, 5-6
[259] COM(2012) 11 final 2012/0011 (COD), 43, proposal for Article 6 (f): "processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks."
See also paragraphs 38, 39 and 56 related to legitimate processing
[260] Albrecht report, amendments 99-102
[261] COM(2012) 11 final 2012/0011 (COD), 8

6.2 Does Google Process Data?

The first step to figure out the role of search engine providers, and especially the role of Google, is to find out whether Google processes data in the meaning of the Directive. Google Search works with a "googlebot", a crawler function, which crawls constantly and systematically on the Internet using the hyperlinks of source web pages to move from the website to another and collect more data. Those websites send a copy of their web pages to Google and the copies are then automatically analyzed by Google's indexing function. The search terms and key words are collected from the websites and recorded in the index of Google Search. The combined key words form the index of the search engine which is then used to provide search results to users. The copies of the pages visited by the crawler are registered in the cache memory of the search engine for the purpose of indexing and displaying the search results.[262] When the user has made a search in the Google Search, the copy of the sought source web page, which is stored in the cache[263] can be displayed. The cache is frequently updated but sometimes there are situations in which the search result displayed by the search engine does not correspond to the source web page because of the changes made to it or its deletion.[264]

According to the Spanish national court Google's actions in respect of Google Search consists of locating information published or included on the Internet by third parties. Google automatically indexes such data, stores it temporarily and finally makes it available to Internet users according to a particular order of preference.[265] Due to the broad definition of "processing" it is clear that Google processes data in the meaning of the Directive.

Also the ECJ has stated in its judgment in the Google Spain case (C-131/12) that "exploring the Internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine '*collects'* such data which it subsequently '*retrieves'*, '*records'* and '*organizes'* within the framework of its indexing programmers, '*stores'* on its servers and, as the case may be, '*discloses'* and '*makes available'* to its users in the form of lists of search results." All the mentioned operations are expressly referred in

[262] Opinion of Advocate General Jääskinen, paragraph, 73
[263] See more about the cache memory in the chapter 9.1
[264] Opinion of Advocate General Jääskinen, paragraph 74
[265] Opinion of Advocate General Jääskinen, paragraph 70

Article 2(b) of the Directive and therefore Google's actions must be classified as "processing".[266] Further in my thesis I will research whether the data that Google processes includes personal data or not[267].

7. Personal Data

The concept of *knowledge* has changed in the ages but what has remained is that knowledge has to be truthful and arguable. The same conditions apply to *information,* but it has also another meaning as shared information or communication. In the field of data protection the concepts of *data* and *information* are often used as synonyms.[268] *Data* can be distinguished from *information:* in the fields of computer and information science, data often refers to signs, patterns, characters or symbols which become *information* only when interpreted. Therefore *data* can be considered as 'potential information' whereas *information* is 'data communicated and understood'.[269]

There are three situations related to personal data and Internet. The first is the situation where elements of personal data are published on any web page on the Internet for the first time. This webpage is called *a source web page*. The second situation is when an Internet search engine operator provides search results that direct the Internet user to the source web page. This kind of service is familiar to all of the Internet users nowadays: almost all the information is searched from the Internet by using the search engines like Google Search. Third case might be more invisible to Internet users despite the fact that this might be the most important case when it comes to the protection of users' personal data. Third case occurs when an Internet user performs a search using an Internet search engine. By doing so, some of his/her personal data are automatically transferred to the Internet search engine provider.[270] Data in the third situation is called *user data*, whereas the search results contain *content data*. I will carry out a more deeply research about those concepts further in my thesis and compare them with the term of *personal data* in the Directive.

[266] C-131/12, paragraph 100(1)
[267] See the chapters 7.1 and 7.2
[268] Korhonen, 2003, 13-16
[269] Bygrave, 2002, 20
[270] Opinion of Advocate General Jääskinen, paragraph 3

7.1 Definition of Personal Data

Personal data[271] is defined in Article 2(a) in the Directive 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 social identity*".

When the Directive was enacted in the beginning of the 1990s the objective was to have as wide and general notion of personal data as possible in order for it to cover all the data which could be linked to a natural person. The broad definition of personal data was adopted already in the CoE Convention.[272] Personal data was also defined in Article 1(b) of OECD Guidelines from the year 1980 meaning *"any information relating to an identified or identifiable individual (data subject)"*[273]. The OECD Guidelines have been updated in 2013 but the definition of personal data has remained the same[274].

> Personal data was defined in the Finnish Personal File Act (471/1987) as a description of a person or that person's characteristics or living circumstances which can be recognized as depicting a certain natural private person or his family or those living with him in the same household.[275] The same definition was maintained in the updated Personal Data Act (523/1999)[276].
>
> In the Commission's proposal personal data is defined to be "any information relating to a data subject" (Article 4(2)). This definition lacks the wording "identified or identifiable. This is because the definition of "data subject" has been separated from the definition of personal data. Commission has proposed that "data subject" shall mean (amendments made by Albrecht report in bold) *"an identified natural person or a natural person who can be identified or* ***singled out****, directly or indirectly,* ***alone or in combination with associated data,*** *by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to* ***a unique identifier****, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, social or gender identity or* ***sexual orientation*** *of that person"* (Article 4(1))[277].

[271] In Finnish *henkilötieto*. For the Finnish definition, see the Personal Data Act (523/1999)
[272] WP136, 4. See more about the CoE Convention above in the chapter 3.1.
[273] OECD Guidelines, 1980
[274] OECD Guidelines, 2013
[275] Saarenpää, 1997, 57
[276] Government Bill (HE 96/1998), 34-35.
[277] Albrecht report, amendment 84

The definition of personal data has a great importance when it comes to the applicability of the Directive. The Directive is only applicable when personal data is being processed. If only general data is processed and not personal data, the Directive is not applicable and no protection for *data only* is needed. Because of the importance of the concept of personal data I want to split the term into four parts and explore them more deeply.

7.1.1 Any Information

First part is *any information* meaning all the information available in whatever form. This can mean images, text, sound, IP-address, car's license number[278], name, e-mail address etc.[279] "Any information" should therefore be interpreted widely. Any information can also include data related to person's private and family life as well as sensitive data meaning namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data concerning criminal offences or convictions. If "any information" includes such sensitive data, Article 8 of the Directive imposes stricter regulations and obligations on the data controller to protect it[280]. Also more general data related to a person's working relations and social and economic behavior are considered to be personal data. [281] Noteworthy is also that the fact that data are publicly available does not affect their status as 'personal data'[282]. In addition, the information does not have to be true or proven in order for it to be personal data[283].

Even though the definition of personal data in the Directive covers 'any information' not all information merits protection as 'personal data' in the meaning of the Directive. Some

[278] The Finnish Data Protection Board, Case 2/932/2009 (1.2.2010)
[279] C-131/12, paragraph 100(3): "…the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a **person's name** links to web pages, published by third parties…". It seems that the judgment covers only person's name. However, according to Kuner (2014, 11), the emphasis on the protection of fundamental rights may make it difficult to argue that the scope of the search terms should not be limited to other personal data. This means that limitation to names only would not be accepted.
[280] Millard, 167
[281] WP136, 6-8
[282] WP20, 11
[283] Pitkänen – Tiilikka – Warma 2013, 42.

information is clearly 'non-personal' for example meteorological information. Also data which has been made anonymous or pseudonymous (to conceal or hide data subjects' identities) as mentioned in Recital 26[284] of the Directive can be seen as 'non-personal' because they can no more be related to a certain person.[285] However, another question is whether anonymized data shall still be considered personal data in a case where anonymized data is easily restorable to its original form. In my opinion the level of anonymization matters when considering whether data is personal or non-personal.

7.1.2 Relating to

The second element in the concept of personal data is "relating to". The Directive does not provide any definition *when* data relates to an individual and this has been a rather continuous issue[286]. Therefore the Article 29 Working Party has clarified the situation in its opinion 4/2007 on the concept of personal data. The information "relates" to an individual when the information is *about* that individual. Clear situations are when the data relate for example, to an individual as an employee of a company. However, in some situations the data relate to an individual only indirectly. These kinds of data are for example car license numbers, IP-address and cookies which need another data set to help to identify a person to which the data relates to, i.e. identification cannot be made directly. WP29 introduces three more elements in respect of the element "relates to". The first element is called *content element* and it is at hand when the data *contains* information about the individual, for example results of medical analysis. Second element is the situation when the data are used for some *purpose*, for example, to evaluate the behavior of the individual (call log of a company). Data can also be

[284] Recital 26: "…the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible".
[285] Millard, 167-168. Also: However, the interpretation and application of Recital 26 are not straightforward, especially, when considering how to 'anonymize' or 'pseudonymize' personal data sufficiently to take data outside the DPD."
[286] Lloyd, 43. See also the case: Durant v. Financial Services Authority (2003, EWCA, Civ 1746, UK), where The Court of Appeal pointed out that the information is not "personal data" in the meaning of the Directive if it does not "relate to" the individual in the relevant sense unless it: "is information that affects privacy of the person, whether in his personal or family life, business or professional capacity. Court referred to Recital 10 of the Directive which then refers further to Article 8 of the ECHR.

considered to relate to an individual if the behavior of an individual *results* from the use of the data.[287]

These three elements (*content, purpose, result)* can help to indicate when the data *relates to* an individual. The elements do not need to be applied at the same time, it is enough that only one element is present in order to justify that the information relates to a certain individual.[288]

7.1.3 Identified or Identifiable

The third element is crucial in my thesis. It is about an *identified or identifiable* natural person. Normally an individual is identified or can be identified from a group of persons by using 'identifiers' meaning particular pieces of information which hold a particularly privileged and close relationship with the individual. These kind of factors can be for example name, profession, hair color and height. A person can be identified either directly or indirectly. Normally an individual is identified directly by his/her name.[289] However, a name is not always enough. For example first names are very rarely unique[290]. If you search for John Smith by using Google Search from the Internet, you get approximately 19,900,000 search results containing the name "John Smith"[291]. In this case, more information than just a name is needed to identify a certain individual and prevent confusion between that person and possible namesakes. If the search results do not contain such information like birthdates, telephone numbers or other identifiers, it may be difficult to find the correct result for the purposes of the user[292]. However, sometimes only the name is enough. This is the case when referring to, for example, Barack Obama. The assumption is that everyone knows he is the president of the USA. Therefore the question, whether information can be considered to be 'personal data' depends on context: it is pretty easy to identify an individual from the classroom than from the whole country. [293]

---

[287] WP136, 9-12
[288] Lloyd, 45-46
[289] WP136, 12-13
[290] Halavais, 142
[291] The number of search results retrieved on 18th November 2014
[292] Halavais, 142
[293] Millard, 168

An individual can also be identified *indirectly*. Indirect identification is possible for example by using a telephone number, car registration number [294], social security number, passport number or just a combination of pieces of information (for example age, place of residence and occupation).[295]

The element of identification has an important role and therefore it is also mentioned in Recital 26 of the Directive:

> "*Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, 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 …* "

Attention here is paid to the sentence "*whereas to determine whether a person is identifiable account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person"*[296]. According to the WP29 this means that only a hypothetical possibility to single out an individual is not enough. "A*ll the means likely reasonable to be used…to identify the said person"*[297] should be taken into account. If such a possibility does not exist or is negligible the person should not be considered as 'identifiable'. As a conclusion the information is not considered as 'personal data' if a person is not identifiable or identified.[298] This is the problem when it comes to the 'content data' meaning the search results appearing on the web page of a search engine[299]. It can be said that because of the wide definition of personal data, "data are usually presumed to be 'personal data' *unless* it can be clearly shown that it would be impossible to tie the data to an identifiable individual"[300]. This conclusion would lead into a situation in which all the content data in search engine's search results would be considered as personal. This is

[294] Finnish Data Protection Board, case 2/932/2009 (1.2.2010)
[295] WP136, 12-13
[296] COM(2012) 11 final 2012/0011 (COD), 21, paragraph 23. In its proposal for new Regulation, Commission has used the content of Recital 26 of the Directive as a basis for the new definition of "data subject".
[297] See Bygrave, 2002, 44: "The Swedish version of Recital 26 formulates the criteria for identification in the terms of those means for identification which are *reasonably capable* (as opposed to likely) of being put to use ('*alla hjälpmedel som… rimligen kan komma att användas…*')
[298] WP136, 18
[299] See more closely about the relationship of content data and personal data in the chapter 7.2.2
[300] Kuner, 2007, 92

because there is always someone that can tie the data in the search result to an identified individual. However, the context matters a lot in this situation.

Finally, it should be emphasized that what matters is the *capability* or *potentiality* of the identification rather than the actual achievement of the identification.[301] If we think about the definition of personal data in the Directive, an individual can also be identifi*able (note the suffix),* not just identified.

> Some variation exists between the jurisdictions as to how stringent the requirement of individuation is. Swedish data protection law has very stringent requirements whereas in Finland the data can be 'personal' even if they can be linked to the 'family' or 'household' unit.[302] The Government Bill (HE 49/1986)[303] states that the interpretation of the concept of personal data should be as wide as possible. Therefore the protection is extended to the person's family or people living in the same household (*group privacy[304]*).
>
> As an example how Finnish courts interpret identification, the Finnish Supreme Administrative Court stated that the patient could not be identified from the logbook of hospital's device which was used in the examination of the patient, because the log did not contain any information descripting the individual or his characters or living conditions. It contained only information related to the activity of the device and therefore the log was not a register file in the meaning of Article 3(1.3) Finnish Personal Data Act. Therefore, the logbook of the device did not create a filing system containing personal data (person register). However, the patient could possibly have been identified if other information of the patient had been combined with the information from the device log. This however, didn't make the log of the device a register file. [305]

7.1.4 Natural Person

The fourth element of the concept of personal data is "natural person" meaning human beings.[306] The concept of natural person is defined in Article 6 of the Universal Declaration of Human Rights: *"Everyone has the right to recognition everywhere as a person before the law."* WP29 opinion on the concept of personal data covers also for example the data on

[301] Bygrave, 2002, 44
[302] Bygrave, 2002, 47. See also the Finnish Personal Data Act, Article 3(1): "personal data means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household".
[303] HE 49/1986, 23
[304] Konstari, 55-60
[305] The Finnish Supreme Administrative Court (KHO) 27.9.2013/3084, record number: 1025/2/12
[306] WP136, 21

dead persons, unborn children and legal persons. Data on dead persons is not normally considered as personal data in the meaning of the Directive because the dead are no longer natural persons. However, such data may receive some protection indirectly in certain cases. This is the situation for example when the data controller does not know that a person is dead and continues to provide protection for his/her data. Noteworthy is that the Member States may give more stringent regulation on the protection of personal data of the dead. Also, when it comes to unborn children, the national legislation decides whether their data is to be considered as personal data or not.[307]

Legal persons are not covered by the Directive in principle. This is clearly stated in Recital 24 of the Directive: "*Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive*". Sometimes, however, some provisions of data protection laws may still indirectly apply to legal persons. This is the case when for example the name of the legal person derives from that of a natural person.[308]

In some cases where the Directive does not apply and thus cannot provide personal data protection, protection can still be provided by the ECHR Article 8, which protects the right to private and family life.[309]

7.2 Does Google Process Personal Data?

The question does Google *process data* was already answered in the chapter 6.2 above. Now, what is relevant for the role of Google and search engine providers in general, is the question does Google *process personal data*. If it does, it needs to comply with the principles related to data quality and conditions of legitimate processing which I have represented earlier in the chapter 6.1. In this chapter, I will first represent the two types of data which Google processes: user data and content data. In the connection with those representations I will research whether user data and content data include personal data or not. This research is obligatory and important for the clarification of Google's legal role and its responsibilities

[307] WP136, 21-22
[308] WP136, 22. See also the E-privacy Directive (2002/58/EC), Articles 1(2), 12 and 13
[309] ECHR Article 8 (1): "Everyone has the right to respect for his private and family life, his home and his correspondence."

towards data subjects. If personal data is processed, Google has to comply with the applicable provisions of the Directive.

In the case C-131/12 Google claimed that it does not process personal data. The basis for the statement was that Google collects data which are already published on third parties' websites without selecting between personal data and other information.[310] On the contrary, Mr. Costeja Gonzáles and the Italian, Austrian, Spanish and Polish Governments together with the European Commission considered that the activity of Google clearly involves 'data processing" within the meaning of the Directive.[311] Noteworthy is that the ECJ has already held that processing information which is already been published in unaltered form in the media can be considered 'processing' in the meaning of the Directive[312]. The questions asked by the Spanish national court did not include a question whether it is 'personal data' what Google processes[313]. That is why I want to have a closer look to the broad definition of personal data and find out whether search results include personal data.

7.2.1 User Data

7.2.1.1 What Kinds of User Data Does Google Process and for What Purposes?

Google, and other search engine providers, process two types of data: user data and content data. First, I research more deeply the concept of user data. Google strives to gather all the international data and make it conveniently accessible for as many people as possible.[314] The most well-known services that Google provides are Google Search, Google Chrome, Google Maps, Google Drive, Google Translator and the e-mail service Gmail. [315] Google is also constantly developing new services, for example relating to pattern and voice recognition. Google therefore provides a broad supply of services for free. But everyone knows that there is no free lunch. Services in the Internet may look free but they are anything but free. Internet

[310] C-131/12, paragraph 22
[311] C-131/12, paragraph 23
[312] C-131/12, paragraph 30. See also the case C-73/07 Satakunnan Markkinapörssi and Satamedia, paragraphs 48 and 49.
[313] C-131/12, paragraph 27
[314] About Google: http://www.google.fi/intl/fi/about/
[315]More information about Google's products can be found at http://www.google.fi/intl/fi/about/products/

users might not have to pay a fee in the traditional way by using money, but they pay for the services by giving their personal data to service providers.[316]

We need to remember that Google is a huge stock exchange company whose main goal is to show a profit to its stockholders. Google gets its money from the advertising technologies and services which it provides to companies having websites[317]. Simply put, Google sells the data it has collected from its users to other companies which then use the data for advertising and profiling purposes.

It is all about the user. When an Internet user visits websites that use Google's advertising and other products the web browser automatically sends certain information to Google including for example the web address of the page visited and the user's IP address. Also cookies may be set on the user's browser. General term for the data that Google collects is *log data.* Log data are the most important data that are processed by the search engine and it gives Google the outlines of the use of the service.[318] The purpose for collecting log data is typically to find out who has used the service, when the service has been used and why. Log data are necessary in many ways: they ensure the data security of the systems and detect malware and errors. Log data also ensures the legal protection of the users.[319]

According to Google they use the information collected for example to make ads more effective, provide user's behavior data to advertisers to help them understand how visitors engage with their sites, improve user's Internet experience, and improve Google's products.[320]

Google collects user data in two ways. **Firstly, Google collects all the information which is given to it by the user.** Such operational data related to the user data are for example data on registered users as well as data obtained from other services such as e-mail service.[321] For example, if a person wants to have a Google Account he/she needs to register and create a profile in order to be able to use the service. By registering, Google asks some of the person's

[316] Järvinen, 2010, 217
[317] Van Dijk, 91: "99% of Google's revenue (29.3 billion US dollars) in 2010 was from advertising.
[318] WP148, 6
[319] Innanen & Saarimäki, 96
[320] Google, its partners and privacy, available at http://www.google.fi/intl/fi/policies/privacy/partners/
[321] WP148, 6

personal information including his/her name, e-mail address, telephone number and/or even credit card information. [322]

Secondly, Google receives lots of information of the user who uses Google's services. This data includes information concerning the use of Google's services: what services are used and how. The amount of collected information per person is huge. Google collects user's *device information* (hardware model, operating system version, unique device identifiers like IMEI-number of the mobile phone, and mobile network information including phone number). Another important group of data collected is *log information* telling Google how the user has used Google's service. This group of data includes for example the search queries made by an Internet user, time and date of calls, duration of calls, SMS routing information, Internet protocol address (IP-address), device event information like browser type and language, URL-addresses of the web sites the user has visited and cookies. Log information is automatically collected and stored in Google's server logs. [323]

Location information is processed when the user uses Google's location services like Google Maps and Google Drive. [324] There are two types of location information collected by Google. First type is called *implicit location information*. It does not tell Google where the user's device is located but might tell Google, by using the user's search query, which places the user is interested in. This enables Google to provide user with personalized information. By collecting implicit location information Google can provide the user with advertisements related to places the user is interested in. For example, if you are planning a trip to Paris, Google knows this and provides you ads relating to Paris. Other type of collected location data is *Internet traffic information* such as IP address, device based location services such as Wi-Fi access points, GPS signals and device sensors. An IP address is collected to make the services more user-friendly, for example the correct language is provided on the basis of collected IP address.[325]

Other types of information collected are unique application numbers (operating system type), local storage (collecting and storing information locally on user's device), and cookies and

[322] Google's privacy policy available at http://www.google.fi/intl/en/policies/privacy/
[323] Google's privacy policy available at http://www.google.fi/intl/en/policies/privacy/
[324] Google's privacy policy available at http://www.google.fi/intl/en/policies/privacy/
[325] Google's location data available at http://www.google.fi/intl/en/policies/technologies/location-data/

anonymous identifiers.[326] A cookie is a small piece of text sent to the user's browser by a website that has been visited. Cookies can make the Internet experience more useful and easy for the user, since they help the browser to remember for example the preferred language and other settings. Cookies are also used to improve the quality of search engine's service by tracking the user trends and preferences[327].

Google uses cookies in order to collect information of the user. By using cookies it also provides relevant interesting ads to the user by using the information of user's behavior in the Internet. [328] There are two types of cookies: web cookies and flash cookies. *Web cookies* are provided by the search engine and stored on the user's computer. They may contain information about user's operating system and browser. They are more useful for search engines because they stay with the user even though the IP address might change[329]. Also, if several users share the same Internet connection, the cookie can identify every individual user on a different device. *Flash cookies* are also installed by some search engines. Flash cookies usually back up the normal web cookies and they cannot be simply erased. Users can refuse all cookies but by doing so some features in the Internet may not function properly and the user experience might be pretty poor. [330]

7.2.1.2 Is User Data Personal Data?

Above I represented a long list of user data that Google collects. The question is, however, does user data include personal data i.e. can the user be identified or does the data relate to the user? The clearest situations, whether user data contains personal data, relate to the data which includes user's profile information. This information comes up when the user for example establishes a profile or registers for a Gmail-account. Usually user can be directly identified by his/her name. This, however depends on the context as noticed above in the chapter 7.1.3. Profile information, including name and other identifiers such as date of birth, place of residence and telephone number combined together usually make a clear reference

[326] Google's privacy policy available at http://www.google.fi/intl/en/policies/privacy/
[327] WP148, 4-7
[328] http://www.google.fi/intl/en/policies/technologies/cookies/
[329] More about IP address see the Chapter 7.2.1.2
[330] WP148, 4-7

to a certain individual and therefore such information can be considered to be personal data in the meaning of the Directive. Telephone number or credit card information alone cannot, however, be used to identify the person directly but only indirectly by using other sets of data as a help. In any case, both direct and indirect possibilities to identify an individual mean that the data contains personal data.

When it comes to the location data, log data and device data the question about potential personal data gets more difficult. One example is the significance of an IP address[331]. An IP address means a series of numbers which identify computers when they connect to the Internet[332]. An IP address can either be dynamically generated each time a user connects to the Internet, or a user's computer may use the same IP address for each connection (static IP address)[333]. This distinction between the static and dynamic IP-addresses determines whether the specific IP address is considered to be personal data or not.[334]

By collecting the IP address search engines can track and correlate all the web searches that originate from a single IP address. In addition, when an IP address is used together with a unique ID cookie distributed by a search engine, the identification of an individual can be improved. An IP address provides also user's location information.[335] IP address has been considered to be personal data according to the WP37 Opinion where it is stated that: "*Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on*

[331] The Finnish Act on the Protection of Privacy in Electronic Communications (516/2004) defines IP-address as confidential identification data when it is used in the transmission of communication, regardless whether IP-address is connected to a natural person or not (see more about IP address as an identification data: Helopuro – Perttula – Ristola, 291).

[332] See also WP37, 8: "The Internet is a network of computers communicating with each other on the basis of the Transport Control Protocol/Internet Protocol (TCP/IP). … On the Internet, every computer is identified by a single numerical IP address of the form A.B.C.D. where A, B, C and D are numbers in the range of 0 to 255 (e.g. 194.178.86.66)."

[333] See also WP37, 11: Individuals using a modem or a terminal adapter (ISDN). In this case the subscriber will receive an IP address for the duration of his/her connection and this address will probably change the next time he/she dials up. This is called a dynamic IP address. In the case of a connection by ADSL or via video cable, the IP address will usually be static, as far as those connections are permanent.

[334] Kuner, 2007, 97

Also according to Finland's Data Protection Ombudsman Reijo Aarnio as well as on the basis of my own experiences, the dynamic IP address may stay the same for a longer period, it does not change each time when the new connection is created. Therefore there is a possibility to identify a user who has a dynamic IP address instead of the static one.

[335] WP148, 4-6

the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2(a) of the Directive ...)[336]. Also the Finnish Data Protection Board has stated that an IP address is 'personal data"[337]. Despite the fact that an Internet Service Provider (ISP) cannot always in reality identify the user (for example if an occasional user accesses a public computer in a library), an ISP has to treat all the IP information as personal data. This is because an ISP cannot distinguish with absolute certainty that the data correspond to users that cannot be identified.[338] These conclusions will apply equally to search engine operators[339] and they need to consider all user data to be personal data. Individuals behind IP addresses cannot in most cases be directly identifiable by ISPs but the identification can be achieved by a third party[340].

Other log data collected by search engines are *search log information* meaning the search queries that the user has made by using the search engine. Such information includes, for example, the date and time of the search, the source of the search (IP address and cookies) as well as data on the clicks and the content offered (links and advertisement)[341]. Extensive search histories provide a profile about an individual and they contain a footprint of that person's interests, relations and intentions[342]. Search log information can be used both for commercial purposes and as an instrument for law enforcement authorities or national security services to find out information about an individual.[343] Search queries can be referenced to a certain individual by combining several queries by a single user as well as using the so called 'vanity searches' (people searching for information about themselves). This was proved in the AOL case in 2006[344] in which AOL published a sample of queries and results of some 650.000 users during a 3 month period. The names of the users had been replaced by numbers in order to anonymize the people behind the searches. However, by

[336] WP37, 21
[337] Finnish Data Protection Board 1/2006 available at: http://www.finlex.fi/fi/viranomaiset/ftie/2006/20060001
[338] WP136, 17
[339] WP 148, 8
[340] WP148, 8
[341] WP148, 7
[342] WP148, 6
[343] WP148, 7
[344] In 4th August 2006, AOL Research, released a compressed text file on one of its websites containing twenty million search keywords for over 650,000 users over a 3-month period. This lead to a class action lawsuit accusing AOL, among other claims, of violating the Electronic Communications Privacy Act, which was filed against AOL in the U.S District Court for the Northern District of California in September 2006.

using the means represented above, such as combining the search queries, the individuals were identified.[345] As a conclusion, search queries can be considered as personal data.

7.2.2 Content Data

Content data in respect of search engines is the data that is provided for users on, for example Google Search. The search results are content data, and they are gathered from the content that the search engine has collected with the help of its crawler function. This retrieved content contains personal data if the source web pages do[346]. But who is responsible for the content data? Is it the source web page where the data has originally been published? Or is it the search engine that displays such data in its search results? Before answering those questions we need to explore whether content data contains 'personal data' in the meaning of the Directive. This is a crucial step because if personal data doesn't exist in the search results, the Directive is not applicable[347].

The question about personal data in the search engine's content data can be answered by finding out whether an individual can be *identified*[348] from the search results. According to Kuner the possibility of matching data processed by a computer to a specific individual depends on a number of factors[349] such as the context. Who is searching for information, what does he/she already know about the person who he/she is searching for? Are there some other data available to help the matching of the search result and an individual? Usually the users of a search engine know pretty much what and who they are looking for and for what purposes, and that makes the searching easier.

The basis for current data protection legislation is that the processing of personal data constitutes a threat to the subject's rights and freedoms. On the contrary, if an individual cannot be identified there can be no significant threat to his/her privacy.[350] Therefore, it can

[345] WP148, 4
[346] Opinion of Advocate General Jääskinen, paragraph 34
[347] Article 3(1): "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."
[348] See more about identification in the chapter 7.1.3.
[349] Kuner, 2007, 91
[350] Lloyd, 48

be said that if a person cannot be identified directly or indirectly from the search engine's search results there is no risk for his/her privacy. However, noteworthy is that the risk exists in the reality. That is why, for example according to the Finnish Act on the Protection of Privacy in Working Life (13.8.2004/759), Section 4, the employer has to collect all the data related to the employee/job applicant from him/herself. This means that the employer is not allowed to "google" the employee or the job applicant. The search results might be inaccurate or incorrect and therefore misleading which may lead to a situation that the employer assumes that some other person is the applicant. So there is a possibility that the employer identifies the applicant/employee, but there is also an opposite possibility which leads to unwanted situations. The reality is that googling is done by more than three-quarters of employers when screening applicants. Additionally, more than a third of the employers had eliminated a candidate from consideration based on the information they found as a part of that search.[351]

Google provides search results together with an extract including additional content to make the results more user-friendly. These extracts can include text, audiovisual content or sometimes even snapshots of the source web page. This content can be retrieved from the original website or from the search engine provider's devices.[352] When the set of data is taken together to the extract it can then be easier to match the data to a particular person[353]. This argument leads to the conclusion that the search result (for example the name) *together with* the extract can be considered personal data. However, not all the extracts are that informative and do not therefore always include any useful information to help in identifying the person. In these cases it is necessary to follow the hyperlink to the source web page to find out does the data relate to a certain person.

In addition, the same principles represented above about an Internet user using a public computer in a library applies to the case when there is a need to solve whether the search results contain personal data or not. If the search engine provider knows that some of the data can be related to an identifiable natural person but some not, it should consider *all the data* in the search results as personal data and provide sufficient protection for all individuals appearing in the search results.

[351] Mayclim T. Growing number of job searches disrupted by digital dirt, 2006 , Execunet. Retrieved November 13 2014, from http://www.execunet.com/m_releases_content.cfm?id=3349
[352] Opinion of Advocate General Jääskinen, paragraph 35
[353] Kuner, 2007, 92

Currently the Directive establishes a binary manner: if information is personal data, the Directive applies to it in full force. If information is not personal data no regulations apply to it. There have been suggestions about a risk based approach as an option for the mentioned binary manner. Millard suggest, on the basis of the Report of the Coe Convention[354], that rather than applying all the requirements related to personal data set up by the Directive "it should be considered in context which requirements should apply and to what extent, based on a realistic risk of harm and likely severity"[355]. Additionally, rather than considering solely if information is personal data it would make more sense to consider the circumstances in a particular processing, such as assess the risks of identification.[356] As an example: if you belong to a group with 100 members, the chances and risks of identifying you are 1 out of 100. Our dear friend John Smith belongs to a group of 19,900,000 members (Google search results) so the risks and chances to identify him are pretty minor. These examples show how important role the context has in relation to identifying a particular person from the search results.

In the end, however, it would be too complicated to have such a risk based approach to personal data in the search engine provider's search results. This is because every user has a different kind of context in which he/she is searching for information about someone and that context is personal. Every person sees the data in the search results differently. Also, a risk based approach could lead to the situation where for example persons with a common name, such as John Smith, would receive lower protection than persons with a unique name. Therefore, all personal data in search results should be treated coherently.

---

[354] Report en the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_09%20FINAL.pdf (French only). Jean-Marc Dinant, 'Rapport sur les lacunes de la Convention no 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques' T-PD-BUR(2010)09 (I) FINAL (Conseil de l'Europe, 5 November 2010) (8))

[355] Millard, 185.

Millard, 186:" Sweden's data protection act represents a risk-based approach with reduced regulation of personal data contained in unstructured material such as word-processing documents, webpages, emails, audio, and images, presumably based on risks being considered lower here. Sweden relaxed compliance requirements for processing such material, provided it is not included or intended for inclusion in a document-management system, case-management system, or other database…. However, security requirements apply, and processing of such personal data must not violate data subjects' integrity (privacy). See more detailed in Personal data protection – Information on the personal data Act, 4th end (2006), Swedish Ministry of Justice, and the Swedish Data Protection Act (1998:204) (Swedish Personal Data Act)

[356] Millard, 186

8. Data Controllers and Data Processors

8.1 Importance of the Concepts

The division to two concepts, data controller and data processor, has a huge importance since they determine who shall be responsible for the compliance with the EU data protection rules. Defining the concepts means allocating the responsibilities between the parties. The concept of a data controller is also essential because by determining who the data controller is, it makes it possible to determine the applicable national law.[357] National laws give controller responsibilities such as obligation to notify data subjects who are subject to data processing and register data processing with the national data protection authority.[358]

The classification to controller and processor has important consequences since the most data protection obligations under the Directive must be fulfilled by a controller and the controller is in many cases liable for any data protection violations. Data processors, instead, have a reduced role. Data processors process data only on behalf of a controller and under the guidance given by the controller.[359] Data processors need to adopt adequate security measures and comply with the instructions given by the data controller.[360]

8.2 Data Processor

In the proposal of the Directive a new concept "processor"[361] was represented.[362] "Processor" was neither written in the CoE Convention nor in the OECD Guidelines. Data processor is defined in Article 2 (e) of the Directive as follows:

> *"'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".*[363]

[357] WP169, 2-4
[358] Kuner, 72
[359] Kuner, 2007, 69-70
[360] Kuner, 2007, 72
[361] In Finnish: tietojen käsittelijä
[362] WP169, 4
[363] COM(2012) 11 final 2012/0011 (COD), 42: The definition for "processor" remains the same in the new Regulation.

In the Finnish Personal Data Act the term data processor hasn't been directly defined. Data processor is mentioned in Section 3(6) in connection with the definition of a third party. According to that Section, third party means "a person…other than….data processor…" However, in the Government Bill (HE 96/1998) processor is defined as a party who processes data on behalf of the controller[364].

The concept of a processor interacts with the concept of a data controller. The definition is important because it distinguishes, together with the concept of controller, who shall be responsible for the obligations set out in the Directive. A processor is not normally subject directly to the obligations set out in the Directive[365]. However, the definition of a processor has an important meaning in relation to Articles 16-17 of the Directive regarding confidentiality and security of data processing[366]. According to those Articles data processor cannot process personal data unless directed to do so by the controller or by national law. In addition, the processor must ensure the appropriate technical and organizational controls to prevent any unlawful use or disclosure of personal data. Therefore, the processor must perform a risk assessment to determine the potential risks to individuals' rights as a result of the processing of personal data.[367]

As stated in the definition in Article 2(e) of the Directive, processor can be a natural or a legal person, public authority, agency or any other body. This definition provides a broad range of actors to be data processors[368]. The definition is the same when it comes to data controller[369]. What is interesting, is the fact that the existence of a processor depends on the decision made by the controller[370]. Processor has to be a separate legal entity with respect to the controller and it must process personal data on behalf of a controller. This means that the processor is serving the interests of the controller under the mandate and guidance given by the controller.[371] If the processor does not comply with the guidance and acts merely as a

[364] Government Bill (HE 96/1998), 36
[365] Millard, 194
[366] WP169, 2
[367] Herrmann, 237
[368] WP169, 27
[369] See the chapter 8.3
[370] WP169, 25
[371] WP169, 25

data controller determining the purposes and means of processing, it can be considered as a data controller. [372]

8.3 Data Controller

Concept of controller[373] is defined in the Article 2(d) of the Directive as follows:

> *"'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."*

The concept "controller" was originally taken to the Directive from the Coe Convention[374] where it meant mainly "controller of the file" and was mentioned only once in relation to the data subject's right to be informed. In the proposal of the Directive, which was made in the early 1990s, the definition of a controller was no longer used for a static object "the file" but it was changed to relate to activities such as "processing" and "operation"[375].

This change gave a controller a much wider and more dynamic meaning. Also, when the concept of the controller was bound to processing activities it gave information a life cycle from its collection to its destruction. Another changes to the definition were a possibility of "pluralistic control" as well as an extended set of obligations for controller.[376]

---

[372] WP169, 25

[373] Data controller in Finnish, Personal Data Act / henkilötietolaki 3(4)§: 4) *rekisterinpitäjällä* tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty

[374] See chapter 3.1

[375] This was also the case in the OECD Guidelines from the year 1981 in which data controller was defined as "*a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*". The definition has remained the same in the updated Guidelines 2013 except it having a minor change from domestic law to national law.

[376] WP169, 3-4

Due to the changes in the concept of a controller, the role of a controller increased. The controller was made responsible for ensuring the rights of data subjects, such as informing the data subject, giving the data subject an access right to his/her data, and giving the data subject a right to object the processing of his/her personal data. The controller must also notify the national data protection supervisory authorities in certain situations, and the controller is liable for any unlawful processing of personal data.[377] In relation to the sets of actions mentioned above, the data controller may function also as the "chief data user" and as a data processor.[378]

> In the Commission's proposal the definition of a controller (Article 4(5)) maintains its basic idea but the definition is amended to be more accurate (changed parts in bold)[379]: *'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes,* ***conditions*** *and means of the processing of personal data; where the purposes,* ***conditions*** *and means of processing are determined by* ***Union law or Member*** **State law,** the controller or the specific criteria for his nomination may be designated by Union law or by **Member State law**".
>
> The proposal also sets obligations for data controller. Controller shall, for example, adopt policies and implement appropriate measures to ensure and it must be able to demonstrate that the processing of personal data is performed in compliance with the Regulation. Controller should also implement mechanism that data protection is ensured by design and by default. If data controller is not established in the EU it must designate a representative in the Union (with exceptions). Also, when certain conditions are met, data controller has to appoint a data protection officer. Controller is, similarly as stated in the Directive, responsible for choosing a processor which can ensure the appropriate measures for data processing. The Regulation sets also obligations related to data security and data protection impact assessment.[380]

Due to the importance of the definition of a data controller in my thesis, I want to carry out a deeper research on the definition of a data controller by dividing the definition represented in the Directive in four pieces:

(i) a natural person, legal person or any other body,

(ii) (who) determines,

[377] WP169, 4
[378] Bygrave, 2002, 21
[379] COM(2012) 11 final 2012/0011 (COD), 41-42
[380] COM(2012) 11 final 2012/0011 (COD), Chapter IV

(iii) (the) purposes and means (of the processing of personal data)

(iv) alone or jointly with others (multiple controllers)

This division helps the conclusion in the end of my thesis: who shall have the role of the data controller and why? Are search engines data controllers or not? And if they are, in which situations?

8.3.1 Natural Person, Legal Person or Any Other Body

The party who can be a data controller is defined broadly already in the CoE Convention and the same definition is adopted also in the Directive which refers to a broad series of subjects. According to Article 2(d) of the Directive, Google, as a legal entity and a stock exchange company, is eligible to be a data controller since it is a legal person.

National laws and practice established both in the public and private sector may indicate the data controller. Sometimes in an environment with multiple actors it might be difficult to distinguish who the data controller actually is. This kind of situation is for example when a person is working for a company and processes data in his/her daily work. In such a case the company should be considered a controller because it determines the purposes and means of the processing. Also, if a natural person is appointed to be the data protection officer (DPO) for the company he/she will act on behalf of a legal entity but is not a controller. The case may be different, if an employee acting within a legal person uses data for his/her own purposes so that the legal person does not have the control over such use. Then a natural person, employee, is a controller.[381] However, there is one exception stated in the Article 3(2) of the Directive: natural persons are not defined as data controllers if they process data for their purely personal or household activities purposes. Also, in today's information technology world I need to remind that it is possible for a natural person or a legal entity to be a data controller without owning a computer i.e. when data is processed manually. The data controller is responsible also for manually collected and processed data.[382]

[381] WP169, 15-16
[382] Lloyd, 55

8.3.2 Determines

In the CoE Convention a controller was defined as a body who *is competent to decide* about the data processing. A same kind of definition was written in the OECD Guidelines according to which a data controller is a body which "*is competent to decide* about the contents and use of personal data". Competence was defined according to the national law[383]. The Finnish Personal Data Act does not use the term "determine" in the meaning of the Directive. Instead it is written in Section 3(4) that "*controller means a person, corporation, institution or foundation, or a number of them, for the use of whom a personal data file is set up and who is* ***entitled to determine*** *the use of the file, or who has been designated as a controller by an Act*". The Personal Data Act requires the controller to be entitled, i.e. it has to have a right to process personal data. This requirement is not included in the definition in the Directive. The requirement in the Personal Data Act may have negative consequences: if an entity processes data unlawfully and therefore it isn't entitled to process data, according to the Personal Data Act, such entity would not be a controller and would therefore not be liable for any damages for data subjects.[384]

In its first proposal the Commission proposed a solution where it was no more required to check the competence of a data controller from national laws. Instead, the Commission proposed to have a new term "*who decides*" in the definition. However, in the final and adopted text the outcome was a body "*which determines*". This result made it possible for anybody to be a controller irrespective of a specific competence conferred by law.[385]

The new definition of "determination" created in connection with the concept of a controller became a Community concept having an independent meaning in the Community law. The capacity to "determine" may arise from different kinds of elements and circumstances or from a specific attribution by law.[386]

The Article 29 Working Party represents three categories of situations from which the capacity to determine may stem. Firstly, the capacity to control data can stem from an *explicit legal competence* meaning that the body is nominated to be a controller by national or

[383] WP169, 8
[384] Pitkänen – Tiilikka - Warma, 58
[385] WP169, 8
[386] WP169, 8

Community law. These kinds of situations are for example situations in which private entities are entrusted with certain public tasks. Secondly, the control to determine can stem from an *implicit competence*. This means situations, in which the role of a controller is naturally attached to the functional role of a private organization. Such situations are for example employee-employer relationships.[387]

Control over the personal data can thirdly stem from a *factual influence.* The assessment of the factual circumstances can help to determine who the controller is. Sometimes, mainly in complicated environments using information technologies, parties need contractual relations to help to allocate the responsibilities between the parties[388]. Such contracts may be silent or explicitly determine who the controller is. However, the terms of the contract cannot be decisive, the factual circumstances have to be taken into account. Contracts are acceptable as long as they match the reality. Noteworthy is also, that parties just cannot allocate the responsibilities how they want to, the definition of a data controller is a mandatory legal provision from which the parties cannot deviate or negotiate. If such a deviation would be possible, data protection laws would not have effectivity. [389]

In the reality it may be difficult to recognize who the controller is, but some factors may help in such situations. The degree of actual control, the image given to data subjects as well as the expectations of data subjects can be assessed.[390] There is a growing number of actors who do not consider themselves as determining the processing activities. Many actors see themselves mainly as "facilitators" and not as responsible data controllers. In such cases the assessment of factual actions and the three factors mentioned above might be the only feasible options to determine who the controller is.[391] This was also the case in the case Google Spain (C131/12) in which Google claimed that it was not the controller of the personal data appearing in its search results and therefore did not have the responsibility of the data controller either. In the chapter nine of the thesis I will research more deeply the case Google Spain and the role of an Internet search engine provider under the Directive.

---

[387] WP169, 10
[388] Belgium Privacy Commission: decision on 9 December 2008: In the SWIFT case contractual designation was used to determine SWIFT data processor. However, the factual actions of SWIFT was the decisive factor and SWIFT was considered to be a controller.
[389] WP169, 8, 11-12
[390] WP169, 12
[391] WP169, 12

If a natural person or a legal entity cannot be concluded to be a controller by using the categories above, the most likely situation is that a person or an entity is not a controller since it has no factual nor legal influence to determine the purposes and means of processing.[392]

Finally, noteworthy is that there is no difference whether the purpose and means are determined lawfully or unlawfully. The only thing that matters is the fact that someone in reality "determines" the purposes and means of processing, and that actor shall in the end be responsible for personal data it has processed.[393]

8.3.3 Purposes and Means of Processing

Now when we have defined the term "determine" it is time to explore *what* a party should determine in order to qualify as a controller. In the CoE Convention the emphasis was in the purpose of automated data files, categories of personal data and the operations to be applied to them. The Commission made only minor language modification to the definition in the CoE Convention ("the purposes of the file") but finally ended up in a bit more dynamic definition "the purposes and objectives of the processing" instead of a static "file". The final Council Common Position proposed a shortened version from the Commission's proposal: "purposes and means".[394]

The main questions are, *why and how* data are processed. When answering those two questions together it can help to determine whether an entity is a controller or not. According to the opinion of the Article 29 Working Party "purpose" means "*an anticipated outcome that is intended or that guides your planned actions*". Purpose is something that only the controller can determine[395]. Purpose is important also on the other hand: data must be collected for legitimate purposes only.

"Means" has a meaning "*how a result is obtained or an end is achieved"*.[396] "Means" is a bit more complicated term than the purpose. It can mean for example technical ways of

[392] WP169, 12
[393] WP169, 9
[394] WP169, 12, 14
[395] WP169, 15
[396] WP169, 13

processing personal data such as which hardware and software shall be used in processing. The term covers also the questions *which data shall be processed and for how long? Do third parties have access to data and if so, on which grounds?* "Means" also creates a life cycle for information because the controller must decide which data shall be deleted and which not. As you can see, the question related to *how* includes both technical and organizational questions. Determining the "means" has to, however, concern the essential elements of the means and a controller needs to determine the core elements of the means. Sometimes the situation may be that the elements such as technical and organizational means are decided exclusively by the processor. In such cases, the means should represent a reasonable way of achieving the purpose determined by a controller. The data controller should also be fully informed about the means used. Noteworthy is, however, that if a processor has an influence on the purpose and it carries out the processing also for its own benefits it might be considered a controller or possibly a joint controller together with the original controller.[397]

8.3.4 Multiple Controllers

According to the definition of a controller in the Directive, it is possible to have multiple controllers of the same data set. This definition is implemented in almost every Member State: for example the Finnish Personal Data Act recognizes the concept of a co-controller. However some Member States, such as France, do not explicitly recognize such concept of a "co-controller".[398]

The concept of joint control was not mentioned in the CoE Convention. It was firstly introduced by the EU Parliament before the adoption of the Directive.[399] The Commission proposed a definition which covered only the equal determining of a single processing operation by controllers.[400] However, the most important thing is that the controllers *together* determine the purposes and means of data processing. A classic example is the situation where travel agency, airline and hotel together collect and process passenger data for same purposes[401]. In the end, it is not possible to create an exhaustive list of the different kinds of

[397] WP159, 14
[398] Kuner, 2007, 70
[399] WP169, 17
[400] WP169, 18
[401] Pitkänen – Tiilikka - Warma, 55

joint controls. In reality there are multiple arrangements which are possible.[402] A data subject must also be informed of a joint control and the fact that all the actors of processing are responsible for the obligations set out in the Directive. Data subjects' rights must be ensured so the co-controllers must fully comply with the obligations of the Directive, even though certain flexibility in allocating the responsibility is acceptable.[403]

8.4 How to Distinguish the Roles in Practice?

It is not always easy to distinguish who the data controller is and who shall bear the responsibilities related to processing of personal data. Even though the concepts seem pretty clear, the interpretation of them might be difficult since the concepts lack clarity in reality. If it is not possible to clearly determine whether a party is a controller or processor or perhaps another actor such as a third party, it becomes almost impossible for parties to know what their exact compliance obligations are[404]. Further, this creates threat to privacy and data protection of individuals.

When the Directive was enacted in the beginning of 1990s there was a much clearer distinction between the parties to notice, on the one hand, which party has a control over the processing of data and, on the other hand, which party is only processing data on behalf of the other party.[405] However, the development and globalization in the area of information and communications technology have given rise to new and difficult issues related to concepts data controller and data processor[406]. Complex business environments especially in big multinational companies make it even more difficult to allocate the data protection responsibilities correctly. This fact also lowers the protection of data subjects[407]. It is pretty common nowadays for parties to process data together which makes the allocation of responsibilities difficult. In addition, rapidly changing technology, evolving business environments and changing relationships of the parties complicate the issue even more.[408]

[402] WP169, 18
[403] WP169, 22, 24
[404] Kuner, 2007, 72
[405] Kuner, 2007, 72
[406] WP169, 2
[407] WP169, 2
[408] Kuner, 2007, 71-72

Sometimes parties try to allocate responsibilities by contractual relations. Parties enter into contracts which decide who the data controller is and who shall act only as a processor. Big multinational companies use intra-company agreements to clarify the often complicated situations. However, when using such agreements the content of the agreements should fit the facts in the reality[409]. Let's take an example of an international company which has its headquarters in the United States, and multiple affiliated companies around the world processing personal data, also in the EU. Databases of the company are located in the U.S. This company has to live with a certain amount of ambiguity when it tries to determine which of its legal entities are data controllers and when, and which entities are data processors. In this kind of situation the factual circumstances are the thing that matters in determining the role of a legal entity: which entity really *determines the purposes and means of processing?*[410] Which entity processes data *on behalf of a controller?*[411] A substantial inquiry into company's practices and procedures may be necessary to determine who has the ultimate control over specific data[412]. The company also needs to comply with all applicable rules related to international transfers of personal data if it transfers personal data from country to another. Especially EU provisions in this field of data protection are very strict.

When it is clear who the controller is, i.e. who has an ultimate control over the data processed and who determines the purpose and means of the processing, it is easy to direct the responsibilities correctly. Often data controllers outsource the processing activities. A controller is responsible for choosing a processor who can provide satisfactory guarantees regarding technical and organizational security measures (Article 17 of the Directive).[413] In such a case there must always be a written agreement between the parties which obliges the processor to act only under the instructions given by the controller. The controller can also act as a data processor, it is not mandatory to choose another company to process data on behalf of it. In the end, whether data controller acts as a data processor at the same time or outsources the processing activities to another entity, the data controller is the one who has

[409] Kuner, 2007, 73
[410] See the chapter 8.3.2
[411] See the chapter 8.2
[412] Kuner, 2007, 70-71
[413] Millard, 194

the responsibility over the personal data, and who is liable for compensate data subjects for any losses that have occured from the processing.[414]

9. Google as a Data Controller?

9.1 Situations in Which Google is a Data Controller

Earlier in the thesis I have come to a conclusion that Google processes personal data in the meaning of the Directive[415] and therefore the Directive shall be applicable to such processing of personal data. However, this conclusion is not enough to tell the legal role of Google. The key question is, when defining the role of Internet search engine providers, in which contexts does the search engine provider *determine* the purposes and means of the processing of *personal data*, and in which contexts it perhaps has another role[416]. There are also sub questions under the main question which can be asked when defining the controller: why is the processing taking place? Who initiated the processing? Has the controller *chosen* to process personal data for its own purposes?[417] Google has a dual role: firstly it processes *user data* and secondly it provides Internet users an information location tool providing search results (*content data*) to users' searches. Below I go through different kinds of contexts in which Google might be a data controller.

The first context is a search engine provider's control over the user data. As defined above in the chapter 8.3.2 the control over data can stem from an implicit competence. This kind of situation exists when Google provides its services, such as an e-mail service 'Gmail' to Internet users. In relation to Gmail Service, Google clearly determines the purposes and means of processing of user data and can therefore be clearly considered as a data controller. Firstly, the processing of user data takes place in order for Google to provide Gmail for Internet users. The purpose of collecting the user data is to provide users with a personal e-

[414] Lloyd, 56
[415] See the chapter 7.2
[416] Depending on the context, a search engine could have some other role other than a data controller. These roles, which are represented in the EU data protection legislation are: i) data processor (Article 2(e)), ii) recipient (Article 2(g)), iii) third party (Article 2(f)), iv) recipient (Albrecht report, amendment 88). However, due to the limited amount of pages, I won't go through those roles (except data processor in the chapter 8.2)
[417] WP169, 8

mail account. Therefore it must also be Google who initiates the processing in relation to such user data. Furthermore, by providing services where it requests the user to register into service by his/her name, Google has chosen to process personal data. In addition, when it comes to other types of user data, such as log data, Google can be considered as a data controller because it clearly determines the purposes and means of the processing: Google collects log information for the purposes to improve its service and to direct targeted ads for the users[418]. The Directive creates a clear set of responsibilities for search engines as controllers of user data[419].

The second context is about Google's control over its index. Control over personal data can stem also from a factual competence. This is the situation with the indexes of search engines. Google clearly controls the index of its search engine. This control over the index can be shown by three examples. *Firstly*, Google determines how the index is structured. The index links key words to the relevant URL[420] addresses, which enables Google to block certain search results by not displaying web pages from certain countries. *Secondly*, an Internet search engine service provider also controls the index in the sense that it decides whether 'exclusion codes[421]' on source web pages are to be complied with or not.[422] *Thirdly*, due to the sufficient control over its indexes and over the data included in them, a search engine can be considered a data controller when it comes to the removal of personal data from its index and search results. [423] The right to be forgotten, which relates to the removal of personal data from the search results was confirmed by the ECJ's judgment in the case C-131/12[424].

Other cases where a search engine provider can be considered a data controller relate to targeting personal data for added-value services (meaning collecting telephone numbers, email-addresses etc.), advertising on the basis of personal data as well as building profiles of

[418] Google Privacy Policy available at: https://www.google.fi/intl/fi/policies/privacy
[419] WP148, 3
[420] URL is an abbreviation of the words "uniform resource locator".
[421] C-131/12, paragraph 39: Exclusion codes are codes such as 'robot.txt' file and 'noindex' or 'noarchive' tags
[422] Opinion of Advocate General Jääskinen, paragraph 91. See more about of the use of exclusion codes in the chapter 9.2.2
[423] WP148, 14
[424] C-131/12, paragraph 100(4). Note also that some EU Member States have specifically regulated the responsibility of search engine providers to remove content data from the search index. This responsibility has been based on the right of objection (Article 14 of the Directive 1995/46/EC and of the Directive 2000/31/EC) the e-Commerce Directive

individuals[425]. If search engines act purely as *intermediaries of information*[426] they are not considered data controllers. In such situations, *information providers* are the principle data controllers.[427]

> **Cache memory as a special case.** According to the WP29, Google may be considered a data controller if it stores complete parts of the content on the Web on its servers, including the personal data in the content. If search engine service providers provide such caching service they may be considered data controllers. A cache might be needed when there is a temporary inaccessibility to the website itself. In this situation a cache memory may provide content to the user. The problem is the retention period of the content in a cache: data should only be retained in a cache the period necessary to address the problem of above mentioned temporary inaccessibility to the website. If the data are retained longer than necessary such activity may be considered as an independent republication by a search engine. In such a situation, the WP29 holds the search engine responsible for compliance with the EU data protection laws if the data in the cached publications contains personal data.
>
> The problem with cache memories is that if the original publication is altered, the controller should immediately comply with any requests to update the cached copy. Also a temporary blocking of the cached copy is an option until the website has been revisited by the search engine.[428] If those options are not used, a search engine service provider is considered a data controller. In its opinion concerning the preliminary ruling of the case C-131/12, the EU's advocate General Jääskinen states that contents of the cache memory do not fall within the control of the service provider because the cache is a result of completely technical and automated processes which produce a mirror image of the data retrieved from source web pages.[429] However, if the search engine has decided not to comply with the exclusion codes[430] it is a sign of a control over personal data included in the cache.[431]

9.2 Google's Responsibility towards Personal Data in the Search Results

The main research problem in my thesis is, whether Google is a data controller of the personal data in its search results. This question has also been discussed in the ECJ's judgment in the case C-131/12. As a background, source web pages on the Internet often have personal data on their websites, such as names, images, addresses, and other indications with help of which an individual can be identified. When a search engine crawls the Internet

---

[425] WP148, 3
[426] Article 1(2) of the eCommerce Directive: the liability of Internet service providers who act as intermediaries is set out in the eCommerce Directive 2000/31/EC.
[427] WP148, 14
[428] WP148, 15
[429] Opinion of Advocate General Jääskinen, paragraph 92
[430] See the chapters 9.1 and 9.2.2.
[431] Opinion of Advocate General Jääskinen, paragraph 93

and collects data from the visited web pages it does not distinguish between personal data and non-personal data. Such crawling, indexing and displaying of data for search purposes is automated and works without any human interaction. Therefore the character of data as 'personal data' remains unknown to the Internet search engine service provider. [432]

The question is, therefore, does Google *determine* the purposes and means of the processing of the *personal* data in its search results? First question is about *determining the purposes and means.* The second question relates to *personal data*. Has Google chosen to process personal data i.e. does Google determine the purposes and means of the *processing of personal data*?

According to the Advocate General Jääskinen Google cannot be considered as a data controller of personal data in its search results because it does not determine the purposes and means of processing *personal data*[433]. This is because the character of the data remains unknown to the Internet search engine provider. When both personal data and other data are processed in a haphazard and random manner this should not make the processor of such set of data the controller of that random data.[434] If a search engine is made a controller of the random set of data it automatically processes, this would lead to a situation where the Directive is interpreted too widely. Such interpretation could make even a smartphone owner a data controller because his/her device automatically processes data, which *may* include personal data[435]. According to Jääskinen, the data controller should be aware of the existence of certain defined category of information, such as personal data, and that the controller processes such data with an intention which relates to their processing *as* personal data.[436]

Google's statement in the case C-131/12 was similar with Advocate General's opinion above. Google stated that it has no knowledge of personal data and therefore it does not exercise control over the data.[437] An opposite opinion was given by Mr. Costeja Gonzáles and the Spanish, Italian, Austrian, and Polish Governments who, together with the European Commission, considered that the purpose of the processing by Google is distinct from the original purposes of the publishers of websites. Therefore their statement was that Google

[432] Opinion of Advocate General Jääskinen, paragraph 72
[433] Opinion of Advocate General Jääskinen, paragraph 100
[434] Opinion of Advocate General Jääskinen, paragraph 81
[435] Opinion of Advocate General Jääskinen, paragraph 81
[436] Opinion of Advocate General Jääskinen, paragraph 82
[437] C-131/12, paragraph 22

should be considered a data controller of the content of its search results.[438] Third opinion was given by the Greek Government. It considers Google merely as intermediary, except when they store data in a cache[439] for a period which exceeds the time which is technically necessary.[440]

As seen from the multiple opinions above the issue concerning search engine's role is difficult. I will represent some further opinions in addition to the above mentioned to highlight the issue. ***Firstly*** **there is a fact that Internet search engine service providers do not have a real control over the data on a third-party source web page**. Search engines are dependent on the copies[441] of the source web page and updates that are made on source web pages. Furthermore, the search engines cannot delete information from the web sites they index, since such information resides on servers hosted by third parties.[442] The main task of the search engine providers is to provide information location tools to Internet users.[443]

Secondly**, there is a possibility that Google is not a data controller is if acts purely as an intermediary.** Recital 47 of the Directive builds on the legal principle according to which "automated, technical and passive relationships to electronically stored or transmitted content do not create control or liability over it"[444]. If Google acted purely as an intermediary, Recital 47 would apply. However, Google does not just transmit data but it organizes it in the certain order by taking advantage of the behavior of the Internet user in the Internet as well as having the popularity of web pages as basis (such an activity is also called as "*Googlearchy*"[445] meaning that the most ranked web sites become even more popular).[446] Additionally, source web pages can buy a tool (Google Adverts) from Google by which they can make their websites findable in the Google Search. In order to enable these services Google must process data. This means that it does not purely act as an intermediary.

[438] C-131/12, paragraph 23
[439] See more about 'cache' as a special case in the chapter 9.1
[440] C-131/12, paragraph 24
[441] Opinion of Advocate General Jääskinen, paragraph 86
[442] Kuner, 2014, 9.
[443] Opinion of Advocate General Jääskinen, paragraph, 84
[444] Opinion of Advocate General Jääskinen, paragraph 87
[445] Van Dijk, 47 (see more about Googlearcy: Hindman, Matthew: The Myth of Digital Democracy, 2008)
[446] Van Dijk, 47

Thirdly **Advocate General Jääskinen claims that Internet search engine service providers cannot in law or in practice fulfil the obligations** provided in Articles 6, 7 and 8 (principles related to data quality and legitimate processing of personal data) of the Directive in relation to the personal data on third-party source web pages. Jääskinen finds it reasonable that Google as a search engine should not be considered as a controller of such data. According to Jääskinen, an opposite opinion would conclude to an absurd situation since it would make Internet search engines being incompatible with EU law.[447] I understand what Jääskinen means but the statement that someone is not able to comply with the law and due to such inability it should not be considered responsible for some of its actions, is absurd. However, I agree that it would be impossible for a search engine, for example, to ask for a consent from every data subject whose information is disclosed in the search results, first of all for a reason that a search engine provider would not have capacity and resources to identify every person whose personal data is placed on a source web page. Additionally, the identification of individuals whose data is contained in the current search results in the Google Search would be almost impossible.

Google's purpose "is to organize the world's information and make it universally accessible and useful"[448] In my opinion this is the main purpose which Google has determined. The means for realizing the purpose is to process huge amounts of data. Google's goal can be interpreted in two ways. First of all, Google should be aware that "world's information" unavoidably includes personal data. Therefore, Google could be easily considered as a data controller. Other way to interpret the goal is to say, as Google claimed in the case C-131/12 that it does not distinguish between personal data and other information when it collects the data. This may be true but when taking the fundamental rights of an individual into account, especially individual's right to data protection, the first way of interpretation receives more support. In addition, as researched earlier in the thesis (see the chapter 7.2.2) search results may include personal data, and therefore all the content data must be processed as they were personal data. As a conclusion it could be said that Google has *chosen to process personal* data for its own purposes and by its own means.

[447] Opinion of Advocate General Jääskinen, paragraphs 89-90
[448] About Google, available at: https://www.google.fi/intl/en/about/

9.2.1 Effective Implementation of the Right to Be Forgotten

Now, when Google, by the judgment of the ECJ, was made a data controller of the personal data in its search results and therefore given the obligations to execute the individual's right to be forgotten I want shortly to write about the effective implementation of the said right. Also, the new guidelines (26.11.2014) [449] on the implementation of the ECJ's judgment in the case C-131/12 adopted by the WP29 are shortly referred to in this chapter. The guidelines contain a common interpretation of the judgment as well as common criteria to be used by the national data protection authorities when dealing with complaints related to the said right.[450]

As a background, the ECJ has stated in its judgment that search engines play a decisive role in the overall dissemination of data in the Internet. Without search engines' activity Internet users would not possibly find the web page they are searching for.[451] According to the ECJ, the activity of the search engines has a significant effect on individuals' fundamental rights to privacy and to the protection of personal data. The ECJ wants to hold search engines liable for their actions so that individuals' rights could actually be achieved.[452]

In my opinion, it is true that the activity of search engines has an effect on individuals' fundamental rights. I also agree with the ECJ that such an activity has an effect to individuals' right to privacy but I would like to elaborate that such an activity has also positive effects to other fundamental rights of individuals, such as freedom of expression, including individuals' right to receive information. The ECJ has a risk based approach on the activity of search engines in modern society[453] and it has not thought the societal benefits that the Internet brings[454]. General Advocate Jääskinen has, however, recognized the importance of the case for the global Internet. According to Jääskinen there is a need to strike "a correct, reasonable and proportionate balance between the protection of personal data, the coherent

[449] WP225, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Costeja González" C-131/12, Adopted on 26 November 2014
[450] Article 29 Data Protection Working Party, Press Release, 26.11.2014, Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten"
[451] C-131/12, paragraph 36
[452] C-131/12, paragraph 38
[453] C-131/12, paragraph 80
[454] Kuner, 2014, 18

interpretation of the objectives of the information society, and legitimate interests of economic operators and internet users at large"[455].[456]

The ECJ has further stated in its judgment in the case C-131/12 that the concept of a 'controller' should have a broad meaning in order to ensure *the effective and complete* protection of data subjects.[457] When defining Google as a data controller in relation to the personal data in its search results, the ECJ also confirmed in the judgment that individuals have a right to be forgotten when certain conditions are fulfilled.[458] Due to Google's role as a data controller Google has to ensure that individuals have such a right.

Currently the ECJ has given the authorization and power for search engines to decide who shall have the right to be forgotten. This means that the search engines have to decide about the fundamental rights of an individual. The judgment has been criticized on a justified reasons: if such balancing between the fundamental rights is difficult even for courts, private companies are simply not in a position to make such complex decisions. At least some guidelines or involvement of the data protection authorities[459] is needed to some extent. [460] This need has recently been answered by the new guidelines given by the WP29 on 26th November 2014 for the national DPAs for the situations in which they need to deal with complaints related to the right to be forgotten.

The amount of requests relating to 'right to be forgotten' is huge: by the 10th of October 2014 Google had received 144,954 requests so far involving 497,695 URLs.[461] There is a lot of work for Google to deal with all those requests[462]. In practice Google must, when implementing the right to be forgotten, first *identify the individual* who is requesting the deletion. As described in the chapter 7.1.3, that is not always easy. Secondly, the search

[455] Opinion of General Advocate Jääskinen, paragraph 31
[456] Kuner, 2014, 21
[457] C-131/12, paragraph 34
[458] C-131/12, paragraph 100(4)
[459] Some DPAs have stated that if their involvement is needed in cases involving assertion of the right to be forgotten, they will concentrate on only on cases when there is "clear evidence of damage and distress to individuals" (see Kuner, 2014, 17). Note that the ECJ has stated that an individual has the right to be forgotten regardless of any possible damage to him/her (see C-131/12, paragraph 96: …" it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject..")
[460] Kuner, 2014, 25-26
[461] See http://money.cnn.com/2014/10/10/technology/google-forgotten/
[462] WP225, 7: Search engines must follow national data protection laws, including timeframes in which an answer to the request of an individual must be given. This is very hard considering the huge amount of requests.

engine provider must decide whether the personal data in its search results fulfill the conditions of Articles 12(b)[463] and 14(1)(a)[464] of the Directive which must be interpreted in a way that the search engine provider is able to address the right to be forgotten correctly. If a search engine makes wrong decisions, for example deletes information that does not fulfill the conditions set out in the Directive, it may violate the fundamental rights of an individual. There may also be a possibility that the history is changed on a wrong basis. At this point it is worth mentioning that search engines should not, when executing the right to be forgotten, notify the affected source web pages on the fact that the webpage can no longer be accessed via the search engine in response to a specific name-based query. This is because there is no legal basis for such communication, i.e. processing of personal data, under EU data protection law.[465]

I find the right to be forgotten as a necessary right and the ECJ's judgment as a step forward in the protection of individuals' personal data. However, I do not find the execution of such right effective. The material as well as the territorial scope of the right to be forgotten in respect of the search engine results is much wider than the real ability to enforce the right effectively in practice[466]. However, the ECJ seems to expect that the right to be forgotten will be implemented in a way that it allows the easy, quick and effective implementation of the right[467]. In respect of the implementation of the 'right to be forgotten' I agree with the statement of the WP29: "data protection rules only contribute to the protection of individuals if they are followed in practice"[468]. This rule should had been followed in the ruling of the C-131/12.

In my opinion, the most effective way to ensure individuals' right to data protection would had been that *only* the source web pages were liable for data subjects' personal data when it comes to the right to be forgotten[469]. By this I mean that the search engine provider should

[463] Article 12(b): Member States shall guarantee every data subject the right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.
[464] Article 14(1)(a): Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
[465] WP225, 3
[466] Kuner, 2014, 3
[467] C-131/12, paragraph 84
[468] WP12, 5
[469] See the chapter 9.2.2

not be liable for ensuring that individuals have the right to be forgotten. I would even propose that the fundamental right of freedom of expression as well as the search engines could be taken advantage of: individuals could check their "global profile" by using the global search engines such as Google. This global profile would help individuals to find all[470]the source web pages which include their personal data. If such personal data is incorrect or irrelevant, the individual could easily contact the source web page and request for a deletion or a concealment of such personal data related to him/her. This system would decrease the number of requests to a single search engine provider. When the source web page corrects or deletes the information, such information will also be corrected or removed from the search engine's search results in connection with the updates of search engine's index and cache.

The basis for my opinion, first of all, is that the judgment C-131/12 is currently applied only to the domain names which are European ones, such as www.europa.eu and www.google.fi. However, all the personal data which have so far been removed from the search results of www.google.fi can be found at www.google.com. I do not consider that the data protection of individuals is effective when the removed links or personal data can be found just by changing the domain name. Also the WP29 considers that the scope of the de-listing of search results should be extended to all relevant domains, including .com. This is because the current limited interpretation of the judgment to EU domains enables the circumvention[471] of EU law and therefore hinders the effective and complete protection of individuals.[472]

Secondly, the implementation process is heavy for search engines and it does not give advantage to the Internet users who want to be forgotten, because the personal data can still be found from the Internet after the delisting of it from the search results. This is because the ECJ has expressly stated that the right to be forgotten only affects the results obtained on searches made by the *name*[473] of the individual. The ruling does not suggest that the *complete*

[470] See the paragraph 44 of the opinion of the EU's General Advocate Jääskinen relating to "innumerable pages including personal data"
[471] An effective and complete protection of data subjects' rights according to the EU law requires that the EU law cannot be circumvented. See also Recital 19: "When a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities."
[472] WP225, 3, 9
[473] The WP29 has found that the term "name" is not specifically defined in the ruling C-131/12. Therefore it can be considered that the right to be forgotten applies to possible different versions of the name such as family names or different spellings (see WP225, 9).

deletion of the web page from the indexes of the search engine is needed.[474] In practice this means that the individual's personal data can be found from search engines' search results by using other search terms than a person's name. Original information can of course also be found by accessing the source web page directly. [475]

This kind of interpretation does not ensure the effective and complete right to privacy for individuals. Therefore I would suggest that the source web pages should be requested to execute the right to be forgotten instead of the search engine providers. This would be the best and the most effective way to protect an individual and it would ensure that incorrect or irrelevant personal data is deleted from the Internet for good. Noteworthy is, however, that there is no obligation on data subjects to contact the source web page when they want to exercise their rights towards the search engines[476] but such an option exists. The data subject has therefore two possibilities to choose from: he/she can either contact directly the source web page and request the deletion of his/her personal data, or request that the exclusion codes should be used by the source web page. Another option is that the individual may contact the search engine provider and address the request towards it.[477]

9.2.2 Role and Responsibilities of the Source Web Page

As mentioned above, I propose that the source web pages should have the responsibility to ensure the individual's right to be forgotten because that is the most effective way of ensuring such a right. Even though the search engine provider is considered as a data controller in relation to the personal data in its search results I would propose that also the source web page has some kind of a responsibility *in respect of the personal data in the search results*. Such a responsibility can be set with the help of the consent given by the data subject as well as the exclusion codes used or not used by the source web page. The responsibilities of both search engine and source web page should be clearly allocated. Therefore, I do not mean that

[474] WP225, 9
[475] WP225, 2, 6
[476] WP225, 2
[477] WP225, 6-7

there should be any kind of a joint control between the source web page and a search engine provider.[478]

The exclusion codes are the key to the conclusion. The source web page naturally is a data controller in respect of the personal data which have *only* been published on a source web page. However, as we know the information in the Internet can be copied and used by all of the users and other actors of the Internet. Therefore, the personal data published on a source web page should be protected somehow.

The publisher of personal data to the Internet has tools to set safeguards to its web page, such as exclusion codes. 'Exclusion codes' can be used by the source web page if it does not want certain information on its web page to be retrieved for dissemination through search engines. Also caching can be excluded by exclusion codes. By using such codes, source web pages can therefore advise search engines not to index or store a source web page, or to display it within the search results.

According to the WP29, it is essential that search engine providers respect and comply with the exclusion codes set up by the source web page. If the source web page sets up exclusion codes after the crawling and indexing the web page, the search engines should carry out updates on their indexes and cache as soon as possible.[479] The compliance with the exclusion codes is optional for search engines but Google, for example, together with other major search engine providers claims that it complies with the codes set up by the source web page.[480]

The use of the exclusion codes may, however, be more than an optional solution for the source web page. The publisher of personal data on the Internet needs to consider whether it has a legal basis for publication and whether that basis includes indexing of this information by search engines[481]. If there is no legal basis for giving search engines a permission to index

[478] C-131/12, paragraphs 39-40: According to the ECJ, if the source web page does not use exclusion codes in its web page it does not create an indication that the search engine provider is released from its responsibilities related to processing of personal data. Further, such lack of using exclusion codes by the source web page would make both the source web page and the search engine co-controllers. This option would not remove search engine's responsibilities.
[479] WP148, 14
[480] Opinion of Advocate General Jääskinen, footnote 28
[481] Note also the case C-101/01 Lindqvist: the operation of loading personal data on an Internet page must be considered to be processing of personal data. Therefore, the publisher of source web pages containing

the publisher's web page, then sufficient safeguards, such as exclusion codes, should be set up.[482]

In my opinion, the data subject's consent is the defining factor when allocating the responsibilities. **If a consent is asked from the data subject** for dissemination of data subject's personal data by the source web page there is no need to use exclusion codes and the search engine is allowed to crawl and index the source web page. Further, there is no need to a right to be forgotten, because the consent has been given (exceptions may exists if the data subject for example cancels the consent). **If no consent is asked**, the source web page has to use exclusion codes. *If the search engine complies with the codes*, there is no problem because the search engine does not crawl and index the source web page. *If the search engine does not comply with the codes,* it is solely responsible for any damages occurred by the processing and dissemination of the personal data of the data subject.

10. Conclusions and Future Problems

In this chapter I want to put together all of my findings. *The first* conclusion is that search engine providers process data in the meaning of the Directive. This is because of the broad definition of "processing" in the Directive. *Secondly*, I came into a conclusion that the data processed by search engine providers includes personal data. This is because all the content data that may include personal data should be defined as "personal data". The context is the key factor that matters here: every user who searches information from the Internet has a subjective context and it is very likely that he/she identifies the person he/she is looking for by searching with the correct search words. This wide interpretation of the content data as personal data is also in line with individual's fundamental right to privacy.

Thirdly, an internet search engine provider can be considered a data controller in relation to the user data it processes. For example Google has clearly determined the purposes and means of the processing of such data. In relation to the content data, meaning personal data

personal data is a controller of processing of personal data within the meaning of the Directive. As such the publisher is bound by all the obligations the Directive imposes on the controllers (Jääskinen, paragraph 40).
[482] WP148, 14

in the search results, the role of a search engine provider is in general the data controller because it has chosen to process personal data for its purposes to provide Internet users with search results in a certain order. Search engine providers are sometimes said to be intermediaries but at least in relation to Google the concept does not apply. This is because Google does not only transmit data but also processes it for its own purposes and uses editorial control over the content data when organizing the results in a certain order and creating the extracts[483].

Fourthly, the effective implementation of the right to be forgotten is important but does not currently work as hoped by the ECJ. I would suggest that the source web page should bear the main liability when it comes to the effective implementation of the right to be forgotten. To ensure the fundamental right of a freedom of speech, Google and other search engine providers could be used as a help when locating the personal data from the Internet. When directing the requests to source web pages instead of a few major search engine providers the burden of ensuring the effective execution of individual's right to data protection would be shared between multiple actors and service providers on the Internet. In addition, when the incorrect or irrelevant personal data had been deleted from the source web page they would also be deleted from the search results of the search engine provider when it updates its indexes.

The fifth conclusion relates to the question how the responsibilities then should be shared between the source web page and the search engine provider in respect of the personal data *in the search results.* The starting point is the consent of the data subject whose personal data will be published on the source web page. The use of the personal data and further the use of the exclusion codes depends on the content of the consent. The responsibilities of the source web page and the search engine depend firstly on the consent and secondly on the use of and the compliance with the exclusion codes.

If the source web page, which originally published the personal data on the Internet, uses exclusion codes but a search engine provider does not comply with them, the latter can be considered responsible for personal data. However, if the exclusion codes are complied with

[483] I have also discussed this with the Finnish Data Protection Ombudsman, Reijo Aarnio who agreed that Google uses editorial control over the data when organizing it in the specified order. According to Aarnio, such activity is undemocratic processing of data: Google may decide which search results appear at the top of the result list.

by the search engine provider, there is no issue: the source web page is the data controller because the data published on its web page is not indexed by the search engine. The final situation is that the source web page has not used the exclusion codes and has allowed for example Google to crawl and index the data from the web page. In such a situation, the source web page is responsible for the personal data.

Finally, I would like to highlight that the world we are living in – a network society – gets more and more complicated every day. This means that determining the roles of the actors dealing with personal data in the Internet gets more difficult in today's complex business environments and companies are unsure about their obligations. The division to data controller and data processor might maintain its place in the data protection framework but in the future it may be necessary to reconsider the role differentiation again. There might be a need for new kinds of roles in the data protection area when the amount of new actors increases at the same time with the development of new technologies.

Perhaps the clearest way would be to let the parties agree on the role division. Then it would be clear for all, including the individuals as well as the companies processing data, who shall bear the responsibilities imposed to a controller by the legislation. This would be the easy way and it would no more be necessary to examine the factual actions of the parties. Perhaps, when there were proper agreements in place, also the parties would act according to the obligations written in the agreements and not just avoid their responsibilities.

Additionally, the regulation of the Internet needs further discussion. The case C-131/12 could had been a significant step towards the regulation of the Internet especially in the EU data protection point of view but it lacks the consideration of the case's long-term implications[484]. The territorial and material scope of the Directive need more detailed guidance and hopefully this will be taken into account in the future data protection legislation. Furthermore, the effective execution of the fundamental rights of individuals in relation to data protection needs more actions which really work in the reality, not just on a paper. In addition, the significant role of the search engine providers should be taken advantage of in the today's society and also in the future. Perhaps the search engine providers need own legislation where their effects on the society in both negative and positive meaning are taken into account.

[484] Kuner, 2014, 30