University of Helsinki

Faculty of Law

Big Data as an Essential Facility: the Possible Implications for Data Privacy

Master’s thesis

Jere Lehtioksa

Master's degree programme in International Business Law and Public International Law, MICL

Supervisors: Juha Vesala – Ellen Eftestöl-Wilhelmsson

Competition Law

March 2018

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty Faculty of Law		Laitos/Institution– Department
Tekijä/Författare – Author Jere Lehtioksa		
Työn nimi / Arbetets titel – Title Big Data as an Essential Facility: the Possible Implications for Data Privacy		
Oppiaine /Läroämne – Subject Competition Law		
Työn laji/Arbetets art – Level Master's thesis	Aika/Datum – Month and year 03/2018	Sivumäärä/ Sidoantal – Number of pages 67

Tiivistelmä/Referat – Abstract

This thesis covers the interplay and possible conflicts between EU competition law and data privacy regulation in relation to big data containing users' personal data that companies possess. The research questions concern whether dominant companies can be forced to grant access to their data sets to their competitors. The thesis will then analyze whether as a result of granting such access, companies could violate the applicable privacy regulations by sharing their users' personal data without adequate consent from them.

According to EU competition law, there has to be an abuse of a dominant position for the prohibitions of EU competition law to apply. This thesis will first seek to define whether big data can amount to an essential facility and as a result become a tool for abuse. The answer to the above question depends largely on the nature and uses of the particular data set. Another factor having relevance is the market structure and possible entry barriers present.

The thesis will then provide an overview of the EU General Data Protection Regulation (''GDPR''), which provides for rules concerning the processing of personal data of individuals. Under the GDPR, once personal data has been collected, it can only be used for the purpose it was collected for unless consent is provided by the data subject. Furthermore the GDPR places emphasis on information duties to the individuals whose data is being processed.

As a result there is legal uncertainty for companies that face requests from competitors for access to their data. Furthermore it might not prove to be simple task for the regulators and courts to assess when access to data truly is necessary and on what terms such access should be granted and monitored.

The conclusion is that data can under certain circumstances amount to an essential facility, without which other companies cannot survive on the markets. This is however a case specific issue and cannot be assumed automatically. Imposing access too readily risks reducing the incentives for the companies to invest in big data.

On the other hand when granting access to a competitor, the provisions of the GDPR should be complied with. The situation is not satisfactory and there is considerable legal uncertainty for companies facing requests to share their data sets containing personal data. The thesis recommends that sector specific regulation might be the answer to these concerns.

Avainsanat – Nyckelord – Keywords
Essential facilities – big data – data privacy – competition law remedies

Säilytyspaikka – Förvaringställe – Where deposited
E-thesis

Muita tietoja – Övriga uppgifter – Additional information

References

Bibliography

Abrahamson (2014)

Abrahamson, Zachary, 2014. ‘’Essential Data’’ In *Yale Law Journal*, Vol. 124, 2014.

Autorité de la Concurrence and Bundeskartellamt (2016)

Autorité de la Concurrence and Bundeskartellamt ‘’Competition Law and Data’’ 10th May, 2016 p. 11. Available at <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> (accessed 14 March 2018).

Choi (2010)

Choi, Jay Pil, 2010. ‘’Compulsory licensing as an antitrust remedy’’. In *WIPO Journal*, Vol. 2(1), 2010.

Cowen (2016)

Cowen, Tim 2016. ‘’Big Data as a Competition Issue: Should the EU Commission's Approach Be More Careful’’. In *European Networks Law & Regulation*, Vol. 4, 2016.

DMA Group (2018)

DMA Group, Acxiom study, ‘’Data Privacy: What the Consumer Really Thinks’’. 2018, page 4. Available at <https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf> (accessed 16 March 2018).

Diker – Ünver (2017)

Diker Vanberg, A. – Ünver, MB., 2017. ‘’The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?’’ In *European Journal of Law and Technology*, Vol 8, No 1, 2017. Available at <http://ejlt.org/article/view/546/726> (accessed 22 March 2018).

Duch-Brown – Martens (2017)
Duch-Brown, Nestor – Martens, Bertin – Mueller-Langer, Frank, 2017. ‘’The economics of ownership, access and trade in digital data’’. In *JRC Technical Reports, JRC Digital Economy Working Paper*, 2017, p. 7. Available at <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf> (accessed 15 March 2018).

EDPS (2014)
European Data Protection Supervisor, Preliminary Opinion ‘’Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy’’, 2014, para. 83. Available at <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> (accessed 21 March 2018).

Eagles (2006)
Eagles, Ian – Longdin, Louise, 2006. ‘’Gambling on Essential Facilities: Withholding Data as an Abuse of Market Power in European Competition Law’’. In *New Zealand Business Law Quarterly*, Vol. 12, 2006.

ENISA (2015)
The European Union Agency for Network and Information Security (ENISA) ‘’Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics’’, 2015, p. 13. Available at <https://www.enisa.europa.eu/publications/big-data-protection> (link to download the document) (accessed 20 March 2018).

European Data Protection Supervisor ‘’the History of the General Data Protection Regulation’’. Available at <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> (accessed 20 March 2018).

Executive Office of the President (2016)
Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, May 2016, p. 5. Available at <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf> (accessed 14 March 2018).

Ezrachi – Maggiolino (2012)
Ezrachi, Ariel – Maggiolino, Mariateresa, 2012. ‘’European Competition Law, Compulsory Licensing, and Innovation’’. In *Journal of Competition Law & Economics,* 2012, Vol. 8(3).

Finnish Competition and Consumer Authority (2013)
The Finnish Competition and Consumer Authority, ‘’KHO määräsi Suomen Numeropalvelulle 90 000 euron sakot määräävän markkina-aseman väärinkäytöstä’’. Available at <https://www.kkv.fi/ajankohtaista/Tiedotteet/2013/1.2.2013-kkvn-tiedote-kho-maarasi-suomen-numeropalvelulle-90-000-euron-sakot-maaraavan-markkina-aseman-vaarinkaytosta/> (accessed 19 March 2018).

Finnish Data Protection Ombudsman (2015)
The Finnish Data Protection Ombudsman ’’Lausunto liikenne- ja viestintäministeriön massadataa (big data) koskevasta selvityksestä’’, 2015. Available at <http://www.tietosuoja.fi/fi/index/ratkaisut/lausuntoliikenne-javiestintaministerionmassadataabigdatakoskevastaselvityksesta.html> (accessed 22 March 2018).

Geradin – Layne-Farrar – Petit (2012)
Geradin, Damien – Layne-Farrar, Anne – Petit, Nicolas, 2012. *EU Competition Law and Economics*. Oxford University Press, Oxford.

Geradin – Kuschewsky (2013)
Geradin, Damien - Kuschewsky, Monika, 2013. ‘’Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue’’. 2013, p. 11. Available at SSRN: <https://ssrn.com/abstract=2216088> or <http://dx.doi.org/10.2139/ssrn.2216088> (accessed 16 March 2018).

Ghosh (2012)
Ghosh, Subha, 2012. ‘’Commercializing Data’’. In *Elon Law Review,* Vol. 3, 2012.

Grac-Aubert (2015)
Grac-Aubert, Violette, 2015. ‘’A love and hate relationship? Recent developments in data protection and competition law’’. In *European Competition Law Review,* Vol. 36(5), 2015.

Graef (2015)
Graef, Inge, 2015. ‘‘Market Definition and Market Power in Data: The Case of Online Platforms’’. In *World Competition*, Vol. 38(4), 2015.

Graef (2011)
Graef, Inge, 2011. ‘’Tailoring the Essential Facilities Doctrine to the IT Sector: Compulsory Licensing of Intellectual Property Rights after Microsoft’’. In *Cambridge Student Law Review*, 2011, Vol.7.

Hellstrom – Maier-Rigard – Wenzel (2009)
Hellstrom, Per – Maier-Rigaud, Frank – Wenzel, Friedrich, 2009. ‘’Remedies in European Antitrust Law’’. In *European Antitrust Law*, Vol. 43, 2009.

Hirvonen (2011)
Hirvonen Ari, 2011. *Mitkä metodit? Opas oikeustieteen metodologiaan*. Yleisen oikeustieteen julkaisuja 17, pp. 21-25. Available at <https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf> (accessed 14 April 2018).

Hoeren (2014)
Hoeren, Thomas, 2014. ‘’Big data and the ownership in data: recent developments in Europe’’. In *European Intellectual Property Review*, Vol. 36(12), 2014.

Hou (2012)
Hou, Liyang, 2012. ‘’The essential facilities doctrine – what was wrong in Microsoft?’’. In *International Review of Intellectual Property and Competition Law*, Vol. 43(4), 2012.

Information Commissioner’s Office ‘’Guide to the General Data Protection Regulation’’. Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/> (accessed 21 March 2018).

Information Commissioner’s Office ‘’Anonymisation: managing data protection risk code of practice’’. Available at <https://ico.org.uk/media/1061/anonymisation-code.pdf> (accessed 21 March 2018).

Kalimo – Majcher (2017)
Kalimo, Harri – Majcher, Klaudia, 2017. ''The concept of fairness: linking EU competition and data protection law in the digital marketplace''. In *European Law Review*, Vol. 42(2), 2017.

Kallasvuo (2015)
Kallasvuo, Karoliina, 2015. ''Oikeus siirtää tiedot järjestelmästä toiseen'', Referee-artikkeli, 2015, in *Viestintäoikeuden vuosikirja*.

Kennedy (2017)
Kennedy, Joe, 2017. ''The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown''. In *Information Technology & Innovation Foundation*, March 2017.

Koponen – Mangiaracina (2013)
Koponen, Jonas – Mangiaracina, Annamaria, 2013 ''No Free Lunch: Personal Data and Privacy in EU Competition Law''. In *Competition Law International*, Vol. 9(2).

Kroes (2010)
Kroes, Neelie, 2010. ''Towards more confidence and more value for European Digital Citizens (SPEECH/10/452; 17 September 2010) Available at <http://europa.eu/rapid/press-release_SPEECH-10-452_en.htm> (accessed 15 March 2018).

Kuschewsky – Geradin (2013)
Kuschewsky, Monika – Geradin, Damien, 2013. ''Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges''. In *Tilburg Law School Legal Studies Research Paper Series*, No. 020/2013, 2013, p. Available at <http://ssrn.com/abstract=2341232> (accessed 20 March 2018).

Lambrecht – Tucker (2015)
Lambrecht, Anja – Tucker, Catherine E., 2015. ''Can Big Data Protect a Firm from Competition?'', 2015, p. 16. Available at SSRN: <https://ssrn.com/abstract=2705530> or <http://dx.doi.org/10.2139/ssrn.2705530> (accessed 15 March 2018).

Lerner (2014)

Lerner, Andres V., 2014. ‘’The Role of ‘’Big Data’’ in Online Platform’’. In *Antitrust Writing Awards*, 2014, p. 10. Available at: <http://ssrn.com/abstract=2482780> (accessed 15 March 2018).

Lianos (2013)

Lianos, Ioannis, 2013 ‘’Some Reflections on the Question of the Goals of EU Competition Law’’. In *CLES Working Paper Series* 3/2013, 2013, p. 13. Available at <https://www.ucl.ac.uk/drupal/cles/sites/cles/files/cles-3-2013new.pdf> (accessed 14 March 2018).

Mattioli (2014)

Mattioli, Michael, 2014. ‘’Disclosing Big Data’’. In *Minnesota Law Review,* Vol. 99, 2014.

Marini-Balestra – Tremolada (2017)

Marini-Balestra, Federico –Tremolada, Riccardo, 2017. ‘’Digital markets and merger control: balancing big data and privacy against competition law - a comment on the European Commission's Decision in the Microsoft/LinkedIn Merger ‘’. In *European Competition Law Review*, Vol. 38(7), 2017.

McKinsey Global Institute (2004)

McKinsey Global Institute, 2004. ‘’Big data: The next frontier for innovation, competition, and productivity’’. 2004, p. 1. Available at <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx> (accessed 14 March 2018).

McKinsey Global Institute (2011)

McKinsey Global Institute, 2011. ‘’Big data: The next frontier for innovation, competition, and productivity’’, 2011, p.2. Available at <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx> (accessed 15 March 2018).

Meriani (2017)
Meriani, Marianna, 2017. ‘’Digital platforms and the spectrum of data protection in competition law analyses’’. In *European Competition Law Review,* Vol. 38(2), 2017, 38(2).

Metsämäki (2017)
Metsämäki, Mikko, 2017. ’’Uusi tietosuoja-asetus tulee: Suuri hämmennys vallalla’’ in Kauppalehti, 29.12.2017. Available at <https://www.kauppalehti.fi/uutiset/uusi-tietosuoja-asetus-tulee-suuri-hammennys-vallalla/bH73hEtX> (accessed 22 March 2018).

Motta (2008)
Motta, Massimo, 2008. *Competition Policy – Theory and Practice.* Cambridge University Press, Cambridge.

O’Donoghue – Padilla (2006)
O’Donoghue, Robert – Padilla, Jorge A., 2006. *The Law and Economics of Article 82 EC*. Hart Publishing, Portland.

OECD (2013)
OECD ‘’Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing’’ 2013, p. 319. Available at <http://dx.doi.org/10.1787/9789264193307-en> (accessed 14 March 2018).

OECD (2014)
OECD ‘’Data-driven Innovation for Growth and Well-being Interim Synthesis Report October’’ 2014 p. 7. Available at <https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf> (accessed 16 March 2018).

OECD (2016)
OECD ‘’Bringing Competition Policy to the Digital Era’’ DAF/COMP(2016), 2016, p. 8. Available at <https://one.oecd.org/docment/DAF/COMP(2016)14/en/pdf> (accessed 15 March 2018).

OECD Digital Economy Papers (2013)
OECD "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, 2013, p. 19. Available at <http://dx.doi.org/10.1787/5k486qtxldmq-en> (accessed 20 March 2018).

Ohm (2013)
Ohm, Paul, 2013. ''The Underwhelming Benefits of
Big Data''. In *University of Pennsylvania Law Review*, Online, 2013, p. 339. Available at <http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1113&context=penn_law_review_online> (accessed 15 March 2018).

Ong (2005)
Ong, Burton, 2005. ''Building brick barricades and other barriers to entry: abusing a
dominant position by refusing to licence intellectual property rights''. In *European Competition Law Review* Vol. 26(4), 2005.

Polonetsky – Tene (2013-2014)
Polonetsky, Jules – Tene, Omer, 2013-2014. ''Privacy and Big Data:
Making Ends Meet'', In *Stanford Law Review*, Vol. 66, 2013-2014.

Piraino (2000)
Piraino, Thomas A. Jr., 2000. ''Identifying Monopolists' Illegal Conduct under the Sherman Act''. In *New York University Law Review*, Vol. 75(4), 2000.

Raspaud (2014)
Raspaud, Elena Linde, 2014. ''Google as an Essential Facility: An Ill-Fitting Doctrine''. In *Common Law Review*, Vol. 13, 2014.

Rubinfeld – Gal (2017)
Daniel L., Rubinfeld – Michal S. Gal, 2017. ''Access Barriers to Big Data''. In *Arizona Law Review*, Vol. 59:339, 2017.

Sokol – Comerford (2016)
Sokol, Daniel D. – Comerford, Roisin, 2016. ‘’Antitrust and Regulating Big Data’’. In *George Washington Law Review*, Vol. 23, 2016.

Stalla-Bourdillon – Knight (2016)
Stalla-Bourdillon, Sophie – Knight, Alison, 2016. ‘’Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data’’. In *Wisconsin International Law Journal*, Vol. 34(2), 2016.

Stucke – Grunes (Research paper) (2015)
Stucke, Maurice E. – Grunes, Allen P., 2015. ‘’No Mistake About It: The Important Role of Antitrust in the Era of Big Data’’. In *the Antitrust Source,* April 2015, Research Paper #269, p. 8. Available at <http://ssrn.com/abstract=2600051> (accessed 19 March 2018).

Stucke – Grunes (2015)
Stucke, Maurice E. – Grunes, Allen P., 2015. ‘’Debunking the Myths over Big Data and Antitrust’’. In *CPI Antitrust Chronicle*, Vol. 2015(2), 2015.

Stucke – Grunes (2016)
Stucke, Maurice – Grunes, Allen, 2016. Big Data and Competition Policy. Oxford University Press, Oxford.

Shelanski (2013)
Shelanski, Howard A., 2013. ‘’Information, Innovation, and Competition Policy for the Internet’’. In *University of Pennsylvania Law Review*, Vol 161, 2013.

Statement of the Finnish Competition and Consumer Authority (2016)
Statement of the Finnish Competition and Consumer Authority ‘’Luonnos valtioneuvoston periaatepäätökseksi massadatan liiketoiminnan edistämisestä’’, 2016. Available at <https://www.kkv.fi/ratkaisut-ja-julkaisut/aloitteet-lausunnot-ja-kannanotot/2016/luonnos-valtioneuvoston-periaatepaatokseksi-massadatan-liiketoiminnan-edistamisesta/> (accessed 17 March 2018).

Stothers (2001)
Stothers, Christopher, 2001. ‘’Refusal to supply as abuse of a dominant position: essential facilities in the European Union’’. In *European Competition Law Review*, Vol. 22(7), 2001.

Ursic (2016)
Ursic, Helena – Custers, Bart, 2016. ‘’Legal Barriers and Enablers to Big Data Reuse’’. In *European Data Protection Law Review*, Vol. 2, 2016.

Waller – Tasch (2010)
Waller, Weber – Tasch, William, 2010. ‘’Harmonizing Essential Facilities’’. In *Antitrust Law Journal*, Vol. 76, 2010.

Warma – Nieminen (2016)
Warma, Eija – Nieminen Jussi, 2016. ’’Tietosuoja ja kilpailuoikeus – määräävässä markkina-asemassa olevan yrityksen toimitusvelvollisuudesta ja tietosuojalainsäädännöstä’’. In *Defensor Legis*, Vol. 4, 2016.

Whish (2008)
Whish, Richard, 2008. *Competition Law*. Oxford University Press, Oxford.

Official Sources

Primary Law

The Charter of Fundamental Rights of the European Union
The Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities C 364/1*.

Consolidated version of the Treaty on the Functioning of the European Union
Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal C 326, 26.10.2012, p. 47–390*.

Secondary Law

Directive 96/9/EC
Directive 96/9/EC of 11 March 1996 on the legal protection of databases. *OJ L 77, 27.3.1996, p. 20–28*.

Regulation 2016/679
Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal L 119, 4.5.2016, p. 1–88*.

Non-regulatory Instruments Issued by the Commission

Communication from the Commission (2014)
Communication from the Commission - Towards a Data-Driven Economy. COM(2014) 442 final.

Communication from the Commission (2009)
Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings. *OJ C 45, 24.2.2009, p. 7–20*.

DG Competition discussion paper (2005)
Commission, DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses, 2005.

Decisions Adopted by the European Commission

Google/DoubleClick
Case No COMP/M.4731 *Google/DoubleClick*, Decision of 11 March 2008.

Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV
Case No COMP/M.6314 *Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV*, Decision of 4 August 2012.

Sea Containers v. Stena Sealink (Commission)
Case COMP IV/34.689 *Sea Containers v. Stena Sealink*, Decision of 21 December 1993.

TomTom/Tele Atlas
Case No COMP/M.4854 *TomTom/Tele Atlas* Case of 14 May 2008.

Facebook/Whatsapp
Case No COMP/M.7217 *Facebook/Whatsapp*, Decision of 3 October 2014.

Microsoft (Commission)
Case COMP/C-3/37.792 *Microsoft* Decision of 24 March 2004.

Sea Containers v. Stena Sealink (Interim Measures)
Case 94/19/EC *Sea Containers v. Stena Sealink - Interim measures* Decision of 21 December 1993.

Press Releases of the European Commission

European Commission, *Commission launches public consultation on Database Directive*. Available at <https://ec.europa.eu/digital-single-market/en/news/commission-launches-public-consultation-database-directive> (accessed 15 March 2018).

European Commission ‘’Commission seeks feedback on commitments offered by Google to address competition concerns’’. 2014, Available at <http://europa.eu/rapid/press-release_IP-13-371_en.htm> (accessed 23 March 2018).

Material from the Website of the European Union

Speech of Vestager, Margrethe (2016)
Speech of Margrethe Vestager - *Big Data and Competition*. Available at <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/big-data-and-competition_en> (accessed 14 March 2018).

Speech of Almunia, Joaquin (2014)

Speech of Almunia, Joaquin ‘’Public policies in digital markets: reflections from competition enforcement’’. 2014. Available at <http://europa.eu/rapid/press-release_SPEECH-14-515_en.htm> (accessed 16 March 2018).

Speech of Almunia, Joaquin (2012)
Speech of Almunia, Joaquin ‘’Competition and personal data protection’’. 2012. Available at <http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> (accessed 17 March 2018).

Speech of Vestager, Margrethe (2016)
Speech of Vestager, Margrethe ‘’Competition in a big data world’’. 2016. Available at <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en> (accessed on 19 March 2018).

Commission factsheet (2011)
Commission ‘’Fines for breaking EU Competition Law’’. 2011. Available at <http://ec.europa.eu/competition/cartels/overview/factsheet_fines_en.pdf> (accessed 20 March 2018).

Case Law of the Court of Justice of the European Union

Oscar Bronner
Judgment of the Court of 26 November 1998. Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and others. Case C-7/97, EU:C:1998:569.

Microsoft Corp v. the Commission
Judgment of the Court of First Instance (Grand Chamber) 17 September 2007. Microsoft Corp v. the Commission. Case T-201/04, EU:T:2007:289.

United Brands
Judgment of the Court of 14 February 1978. United Brands Company and United Brands Continental BV v Commission of the European Communities. Case 27/76, EU:C:1978:22.

GlaxoSmithKline Services Unlimited et al. v Commission
Judgment of the Court (Third Chamber) 6 October 2009. GlaxoSmithKline Services Unlimited et al. v Commission. Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 P, EU:C:2009:610.

Deutsche Telekom AG v the Commission
Judgment of the Court (Second Chamber) 14 October 2010. Deutsche Telekom AG v the Commission. Case C-280/08 P, EU:C:2010:603.

Asnef-Equifax
Judgment of the Court (Third Chamber) 23 November 2006. Asnef-Equifax et al. v. Asociación de Usuarios de Servicios Bancarios (Ausbanc). Case C-238/05, EU:C:2006:734.

UsedSoft GmbH v Oracle International Corp.
Judgment of the Court (Grand Chamber) 3 July 2012. UsedSoft GmbH v Oracle International Corp. Case C-128/11, EU:C:2012:407.

Ryanair Ltd v PR Aviation BV
Judgment of the Court (Second Chamber) 15 January 2015. Ryanair Ltd v PR Aviation BV. Case C-30/14, EU:C:2015:10.

Fixtures Marketing Ltd v Oy Veikkaus Ab
Judgment of the Court (Grand Chamber) of 9 November 2004. Fixtures Marketing Ltd v Oy Veikkaus Ab. Case C-46/02, EU:C:2004:694.

Hoffmann-La Roche & Co. AG v the Commission
Judgment of the Court of 13 February 1979. Hoffmann-La Roche & Co. AG v the Commission. Case 85/76, EU:C:1979:36.

Continental Can
Judgment of the Court of 21 February 1973. Europemballage Corporation and Continental Can Company Inc. v. the Commission Case 6/72, EU:C:1973:22.

Michelin

Judgment of the Court of 9 November 1983. NV Nederlandsche Banden Industrie Michelin v the Commission. Case 322/81 EU:C:1983:313.

SGL Carbon v Commission

Judgment of the Court (Second Chamber) of 29 June 2006. SGL Carbon v Commission. Case C-308/04 P, EU:C:2006:433.

IMS Health

Judgment of the Court (Fifth Chamber) of 29 April 2004. IMS Health GmbH & Co. OHG and others v. the Commission. Case C-418/01, EU:C:2004:257.

CBEM

Judgment of the Court (Fifth Chamber) of 3 October 1985 Centre belge d'études de marché — Télémarketing (CBEM) SA and Compagnie luxembourgeoise de télédiffusion SA Information publicité Benelux SA. Case 311/84, EU:C:1985:394.

Magill

Judgment of the Court of 6 April 1995. Radio Telefis Eireann (RTE) and others v the Commission. Joined Cases C-241/91 P and C-242/91 P.

Omega

Judgment of the Court (First Chamber) of 14 October 2004. Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn Case C-36/02 Omega, ECLI:EU:C:2004:614.

Opinions of the Advocate Generals

Opinion of Advocate General Jacobs in Oscar Bronner (1998)

Opinion of Advocate General Jacobs delivered on 28 May 1998. Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and Others. Case C-7/97, EU:C:1998:264.

Case Law of National Courts

Attheraces (2005)
Judgment of 21 December 2005. Attheraces Ltd & Anr and The British Horseracing Board & Anr [2005] EWHC 3015 (Ch).

MAO:178-179/09 (2009)
Market Court Judgment of 6 April 2009. Case MAO:178-179/09.

Article 29 Working Party Opinions and Guidelines

WP 29 (2008)
Article 29 Data Protection Working Party ''Opinion 1/2008 on data protection issues related to search engines'', 2008, 00737/EN WP 148 p. 8. Available at <http://194.242.234.211/documents/10160/10704/WP148+-+Opinion+on+data+protection+issues+related+to+search+engines> (accessed 21 March 2018).

WP 29 (2016)
Article 29 Data Protection Working Party17/EN WP259 Guidelines on Consent under Regulation 2016/679.

Abbreviations

EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
GDPR	Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal L 119, 4.5.2016, p. 1–88.
MAO	Markkinaoikeus (the Finnish Market Court)

OECD	Organisation for Economic Cooperation and Development
TFEU	Consolidated version of the Treaty on the Functioning of the European Union Consolidated version of the Treaty on the Functioning of the European Union. Official Journal C 326, 26.10.2012, p. 47–390.

Contents

1. Introduction

1.1 The increasing significance of big data and its implications for competition

The term big data has become a widely used term in the past years. Big data can broadly be said to encompass large amounts of different types of data that is produced with high velocity and originates from a vast number of different types of sources. This vast mass of data is then processed with the help of powerful processors, software and algorithms.[1]

The significance of big data lies in the word 'big'. Indeed big data has quickly become one of the most important economic asset that a company can have and it has the potential to create significant competitive advantage for companies and increase innovation and growth. The benefits of big data include the development of new data-based goods and services, improvement in production, marketing through targeted advertisements and decision-making and enhanced research and development.[2]

With such huge competitive advantage for companies controlling such data sets, the question arises whether the collection and exploitation of data can raise entry barriers for companies entering the market and not having such assets at their disposal.[3] The barriers can be of technological, legal, or behavioral in nature.[4] Some entry barriers are unique to big data, such as the need to be able to store and analyze large volumes of data.[5] Especially in consumer social networking platforms, the collection of big data through free-access services funded by advertising can potentially raise competition concerns.[6] However, the point is not to say that possession of large data sets in itself is an issue that the competition law should interfere. Instead it must be asked whether a data set is replicable or not. Furthermore, the ability of a company to process and utilize data is more crucial than the sheer volume of data.[7] Even EU's Competition Commissioner Margrethe Vestager has in her speech noted

[1] Communication from the Commission (2014), p. 4.
[2] OECD (2013), p. 319.
[3] Autorité de la Concurrence and Bundeskartellamt (2016), p. 11.
[4] Rubinfeld – Gal (2017), p. 369.
[5] Ibid, p. 348.
[6] Marini-Balestra – Tremolada (2017), pp. 342-343.
[7] Ibid, p. 343.

that companies need to ensure that they don't use data in a manner that stops other companies from competing.[8]

How does competition law then regulate these types of situations? First of all the main aim of the EU competition law is the protection of the process of competition. More specifically, competition law is concerned in companies harming consumer welfare for instance by reducing input, reduce quality and innovation.[9] One particular form of a harmful practice by a dominant company behaves in anticompetitive manner towards its competitors.[10] The EU competition law only intervenes in behavior of dominant companies in relation to such conduct. This begs the question of whether a company could be held dominant under the EU competition law through controlling big data.

A company is dominant where it enjoys a position of economic strength making it possible for it to prevent effective competition being maintained on the relevant market by giving it the power to behave in manner that is to an appreciable extent independent of its competitors, customers and ultimately of its consumers.[11] There are various factors to consider in defining the dominance of company such as the relevant market shares,[12] constraints caused by the actual competitors, constraints caused by the credible threat of potential competitors' entry into the market and those resulting from countervailing buyer power.[13] It is often argued that big data is ubiquitous, cheap to acquire and available on a wide scale.[14] However, this might not be the case always as the organization, storage, and analysis of big data matter in addition to the mere control of such data.[15] The report conducted by the French and German Competition Authorities (''Franco-German report'') states that there are arguments towards the collection and exploitation of data as raising entry barriers and being a source of market power.[16]

[8] Speech of Vestager, Margrethe (2016).
[9] Whish (2008), p.1.
[10] Ibid, pp. 2-3.
[11] Judgment of the Court of 14 February 1978. *United Brands Company and United Brands Continental BV v Commission of the European Communities*. Case 27/76, EU:C:1978:22. Para. 65.
[12] Geradin – Layne-Farrar – Petit (2012), p. 189.
[13] Communication from the Commission (2009), para. 12.
[14] Stucke – Grunes (2016), p. 42.
[15] Cowen (2016), p. 16.
[16] Autorité de la Concurrence and Bundeskartellamt (2016), p. 11.

Once it is established that a company is dominant, it cannot in general refuse to supply its competitors its essential facilities or else it risks infringing EU competition law.[17] The essential facilities doctrine makes it possible for the competitors of a dominant company to gain access to the essential facility of the dominant company when the facility is indispensable and certain other requirements are met.[18] This thesis will refer to the access by competitors as 'forced access'.

However in relation forced access it must be borne in mind that many data sets in fact contain information of individuals (customers and users of the products of the companies). The EU General Data Protection Regulation[19] (''GDPR'') provides for rules concerning the processing of personal data of individuals. According to the GDPR, personal data encompasses any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly, in particular by reference to an identifier, which can be for instance the person's name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[20] The GDPR provides for various safeguards for personal data. For instance it should be transparent to people that their personal data are processed and to what extent the personal data are processed. Especially the information on the identity of the party who actually processes the personal data ('processor') and the purposes of the processing must be communicated to the person.[21]

As a result, dominant companies holding big data that containing personal data face difficulties in complying with both competition law and the GDPR when facing requests from competitors to share their big data, which can lessen legal certainty.

While both competition law and the GDPR are EU level legislation, they do have different background and purposes. For competition law the main principles are fairness, economic

[17] Case No 94/19/EC *Sea Containers v. Stena Sealink - Interim measures*, Decision of 21 December 1993. Para. 66.
[18] Judgment of the Court of 26 November 1998. *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and others*. Case C-7/97, EU:C:1998:569. Para. 41. For the innovative product requirement see judgment of the Court of First Instance (Grand Chamber) 17 September 2007. *Microsoft Corp v. the Commission*. Case T-201/04, EU:T:2007:289. Para. 632.
[19] Regulation 2016/679.
[20] Article 4 of the GDPR.
[21] Recital 39 of the GDPR.

welfare, market integration, and protection of consumers and the freedom to compete.[22] The ECJ has held[23] that the protection of the interests of competitors or of consumers is not the only interest protected by the EU treaty but also the structure of the market and competition as such. Article 102 Treaty on the Functioning of the European Union (''TFEU'')[24] does not only to practices which may cause damage to consumers directly, but also to practices which are detrimental to consumers through their impact on competition.[25] On the other hand the goals of data privacy rules are to protect privacy through the use of informational self-determination whereas the goal of competition law is to ensure and enable an efficient and functioning competition in the markets.[26] According to the Finnish Data Ombudsman, the purpose of data privacy regulation is to secure the protection of privacy and other fundamental rights as well as building and maintaining trust while at the same time offering proper prerequisites for the processing of data.[27] However, some commentators have argued that competition and data privacy share common objectives which are to protect fairness, ensuring freedom and choice and preventing harm.

There seems to be no clear stand so far on whether the EU competition law should take into consideration data privacy related matters as is demonstrated in the case of *Asnef-Equifax*[28], where the ECJ held that issues relating to the sensitivity of personal data are not, as such, a matter for competition law but that of data protection regulation.[29] However some scholars are of the view that the EU competition law should take into consideration data protection issues. For instance Meriani argues that data protection issues cannot be excluded from consideration under competition law despite its different goals whenever the data protection issues can have an effect on the competition law.[30] Indeed there have been other comments at the EU level supporting the need to consider privacy related matters in relation to competition law as Margrethe Vestager has in her speech noted that companies need to ensure that

[22] Lianos (2013), p. 13.
[23]Judgment of the Court (Third Chamber) 6 October 2009. *GlaxoSmithKline Services Unlimited et al. v Commission*. Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 P, EU:C:2009:610. Para 63.
[24] Consolidated version of the Treaty on the Functioning of the European Union Consolidated version of the Treaty on the Functioning of the European Union. Official Journal C 326, 26.10.2012, p. 47–390.
[25] Judgment of the Court (Second Chamber) 14 October 2010. *Deutsche Telekom AG v the Commission*. Case C-280/08 P, EU:C:2010:603. Para. 176.
[26] Warma – Nieminen (2016), p. 569.
[27] The Finnish Data Protection Ombudsman (2015).
[28] Judgment of the Court (Third Chamber) 23 November 2006. *Asnef-Equifax et al. v. Asociación de Usuarios de Servicios Bancarios (Ausbanc)*. Case C-238/05, EU:C:2006:734.
[29] Ibid, para. 63.
[30] Meriani (2017), p. 93.

they don't use data to prevent other companies from competing. However, she went on to emphasize that there is not a problem just because a company hold a large amount of data since the point of big data is that it has to be big.[31]

This thesis will focus on competition law but will also seek to include relevant data privacy rules where appropriate. By doing this, it will be demonstrated that there is a potential for a conflict between the application of these two areas of law.

1.2 Research questions

The object of this thesis is to analyze the issues raised by the accumulation of big data to companies and the possible implications from the point of view of competition law. The particular emphasis being on the doctrine of essential facilities found in the competition law under which a dominant company's facility can be made subject to a forced access by competitors.[32] The aim is to provide answers to the following questions:

1. Can the accumulation of big data to a dominant company result in such data assets being held as an essential facility under the EU competition law?

2. What are the possible issues and concerns arising from forced sharing of data assets containing personal information of users?

3. How should the forced sharing of data assets containing personal data be regulated to ensure that the possible concerns are dealt with properly?

1.3 Methodological and structural remarks

This thesis aims to analyze the current state of EU competition law. Certain aspects of the GDPR are also analyzed in relation to the possible data privacy related issues arising from the sharing of big data containing personal data. The topic of the thesis is multisided in the sense that the research questions are located in the intersection of competition law and data

[31] Speech of Vestager, Margrethe (2016).
[32] See for instance *Oscar Bronner* (supra note 18).

privacy law, although the main focus in on competition law. For these purposes, the primary research method is the legal dogmatic method.

The Legal dogmatic method has as its aim the study of the current existing legal system and state of law. The dogmatic method both interprets and systemizes the norms. In addition to the analysis of legal rules, this method can also be used to study the legal principles as a norm contains both rules and principles. This is evident in this thesis as both the current state of the competition law and data privacy rules contained in the Treaty on the Functioning of the European Union and the GDPR will be discussed in addition to the legal praxis of the courts. The dogmatic approach also encompasses the weighing of the legal principles, which requires that the principles are interpreted. This thesis will embark on the weighing of legal principles of competition law and data privacy and will use interpretation of the existing norms as a means to achieve this goal.[33]

The dogmatic method is not a pure description of law as it also contains statements on how the laws should be interpreted and systemized.[34] This approach also introduces an element of *de lege ferenda research.* As a result this thesis seeks to provide recommendations on the possible ways to solve the collision between forced sharing of big data and the data privacy rules.

Finally there are some elements of comparative methodology at times due to the fact that competition law and data privacy law are EU level legislation. However, only a light version of a comparative method is used. For instance there are some instances where it is necessary and informative to analyze a case from a Member State court in order to understand the larger legal framework.

1.4 Scope of the research

This thesis seeks to address the question of how the EU competition law governs the situations where companies gain possession of large data sets known also as big data. Accordingly, the main area of law of the thesis is competition law but the intersection of data privacy

[33] Hirvonen (2011), pp. 21-25.
[34] Ibid, p. 25.

regulation and competition law will also be discussed. The main issue is whether the competition law doctrine of essential facilities, where dominant companies can be forced to allow competitors access to their facility, is compatible with the GDPR, which provides for the protection of personal data. For the purposes of the thesis it is assumed that the data sets in question contains personal data although this is not the case always (for instance purely numerical data). Furthermore, the term personal data in this thesis is understood in the same sense as in the GDPR.[35] This thesis will consider situations where the company possessing the data set is in fact dominant under the EU competition law rules although in reality this is not always the case and could be the subject of a separate research.

Furthermore, there are various legal protections available for the owners of databases in the EU such as those provided in the Database Directive.[36] These forms of protection will be discussed briefly, but are not the main focus of this thesis.

As for the jurisdictional remarks, the thesis will primarily focus on the EU level competition law case law and Commission decisions with some jurisprudence of the EU Member State courts also analysed where appropriate for the sake of providing useful examples on the matters discussed.

[35] Article 4 of the GDPR provides that personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
[36] Directive 96/9/EC.

2. Big data

2.1 Characteristic of big data

This thesis will closely relate to big data and its implication to companies conducting business in the markets. Big data plays a huge role in today's society and the growth of big data technology and services were expected to be USD 16.9 billion in 2015 with an annual growth rate of 40%.[37]. Companies receive big data from a variety of sources such as when people upload messages and photos over social media or their phones transmit their locations.[38]

There is no single definition for big data. One definition of big data is that it means large amounts of different types of data that is produced with high velocity from a large number of various types of sources and requires tools and methods such as powerful processors, software and algorithms.[39] Big data encompasses datasets which have a size that cannot be captured stored, managed or analyzed by typical database software tools.[40]

Rubinfeld and Gal say that the volume of data refers to the exponentially increased amount of data that can be collected and analyzed. They describe volume as the main characteristics of big data. The term velocity refers to the speed of change, which plays a crucial part in dynamic markets. The term variety refers to the number of different sources for the collection of data. Veracity concerns the accuracy of the data. The metadata that is the result of the synthesis can be included in the definition of big data in addition to the data collected.[41]

It is important to realize that companies do not always collect big data by themselves. According to Lerner, data brokers are firms that collect consumer data from many sources both online and offline by e.g. using tracking technologies on certain websites (for instance cookies) and they provide various services to their clients involving the sale of such collected data.[42]

[37] Communication from the Commission (2014), p. 2.
[38] Executive Office of the President (2016), p. 5.
[39] Communication from the Commission (2014), p. 4.
[40] McKinsey Global Institute (2004), p. 1.
[41] Rubinfeld – Gal (2017), pp. 345-347.
[42] Lerner (2014), pp. 8-9.

2.2 The definition of data and the legal framework surrounding data

There are various ways to define the meaning of data. One way is to separate data into personal and non-personal data, however this type of definition fails to define the exact borderline between personal and non-personal involvement in the processing of data.

One key concept in relation to data is that it is non-rivalrous. This means that if one person uses such a good, it can also be used by other persons.[43] While it is relatively easy to see the benefits of big data for companies, society and individuals, it is also necessary to analyze the types of legal protection offered for data in order to understand how companies might seek to protect their valuable asset. It is first however necessary to consider can information as an intangible good even be owned.

In *UsedSoft*[44] the ECJ held that where commercial transactions involve a transfer of the right of ownership of the copy of the computer program, a customer who downloads the copy of the program and concludes a user licence agreement relating to that copy receives a right to use that copy for an unlimited period.[45] The ECJ held that the downloading on to the customer's server of a copy of the computer program on the rightholder's website and the conclusion of a user licence agreement for that copy were a sale.[46] According to Abrahamson the *UsedSoft* decision implies that intangible goods such as software downloaded via the internet could be subject to a specific ownership.[47]

If one assumes that information can indeed be subject to ownership, it is then possible to consider the various ways to protect this data. Ursic and Custers argue that among the various IPRs, copyrights, database rights and trade secrets most closely concern data. For instance, copyright protects the expression or form of a piece of work but not the idea or concept. Hoeren points out that while databases enjoy legal protection under the EU database directive in situations where they have been created as a result of investing substantial amount of time and money, this protection does not extend to the underlying data.[48]

[43] Duch-Brown – Martens (2017), p. 12.
[44] Judgment of the Court (Grand Chamber) 3 July 2012. *UsedSoft GmbH v Oracle International Corp*. Case C-128/11, EU:C:2012:407.
[45] *Ibid*, para. 45.
[46] *Ibid*, para. 84.
[47] Hoeren (2014), p. 753.
[48] Ibid, p. 752.

The Database directive provides for two forms of legal protection for databases. The first form is the protection by copyright and applies to databases which as a result of the selection or arrangement of their contents, constitute the author's own intellectual creation. The second form of protection is based on a sui generis right and applies to databases in cases of qualitatively and/or quantitatively substantial investments made in either the obtaining, verification or presentation of the contents of the database.[49] The owner of a protected database can stop certain acts by others such as reproduction or re-use of the database.[50]

The Database directive states that[51] for the purposes of said directive, database means a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Prima facie this definition includes the types of data sets discussed in this thesis. However, the Database directive only applies to databases which as a result of the selection or arrangement of their contents, constitute the author's own intellectual creation and the protection afforded by the Database directive does not extend to the contents of the database.[52] There are limitations to the protection of a database under the Database directive. In relation to the sui generis protection, the ECJ[53] has held that the expression 'investment in ... the obtaining ... of the contents' of a database in the Database directive refers to the resources used to locate materials that exist and collect them in the database. Resources used for the creation of materials contained in the database are not included in that definition. As a result, the protection is rather limited under the database protection and in any case does not amount to nearly all forms of data collection.

Datasets can also be protected as trade secrets. However, trade secret protection does not extend to information that public or obtained through legitimate means such as discovery or creation.[54] Ghosh points out that privacy and security restrictions may offer protection for

[49] Judgment of the Court (Second Chamber) 15 January 2015. *Ryanair Ltd v PR Aviation BV*. Case C-30/14, EU:C:2015:10, at para. 34.
[50] European Commission, *Commission launches public consultation on Database Directive*. Available at <https://ec.europa.eu/digital-single-market/en/news/commission-launches-public-consultation-database-directive> (accessed 15 March 2018).
[51] Article 1 of the Database Directive.
[52] Article 3 of the Database Directive.
[53] Judgment of the Court (Grand Chamber) of 9 November 2004. *Fixtures Marketing Ltd v Oy Veikkaus Ab*. Case C-46/02, EU:C:2004:694. Para. 49.
[54] Graef (2015), p. 81.

personal and other sensitive types of data. He also says that commercially valuable information is often protected by the measures offered by trade secret law within a company and collection of data by database protection.[55]

Currently there is no uniform legal instrument governing trade secrets in the EU level. However article 39 of the Agreement on Trade-related Aspects of Intellectual Property Rights (''TRIPS'') provides that information amounts to a trade secret where it is not generally known among or readily accessible to persons within the circles that normally deal with that kind of information, has commercial value due it being secret and has been subject to reasonable steps to keep it secret. Cleary big data satisfies the criteria of not being generally known or accessible as well having commercial value, furthermore companies can keep their big data analytics and even data itself secret from other parties to some extent. Finally trade secret regulation seems to fit big data quite well since the TRIPS refers to information. However, once the data has been disclosed to a certain number of parties, it is no longer capable of enjoying protection as a trade secret. This in turn makes it quite challenging for companies to rely on trade secret protection for their big data as they would need to embark on quite burdensome process on keeping their data secret.

There might be little economic interests to disclose big data for companies that do not sell it as a product, however additional reasons such as privacy regulations discourage companies from disclosing their data. Also big data might reveal information such as faults in the products or programmes of the company holding the big data.[56]

As a result of the fact that there are no clear rules on the ownership of data sets, it possible for parties to seek to become the de facto owners of the data by means of data collection and protection technology which are combined with their market power.[57]

[55] Ghosh (2012), p. 202.
[56] Mattioli (2014), p. 549.
[57] Duch-Brown – Martens (2017), p. 18.

2.3 The benefits of big data

According to the Organisation for Economic Co-operation and Development (''OECD'') big data is a core economic asset that has the potential to create significant competitive advantage for companies and drive innovation and growth. The benefits of big data include the development of new goods and services that are based on data, improved production processes, improved marketing through targeted advertisements, improved decision-making and enhanced research and development.[58] Big data leads to more informed decision-making which might enable companies to make more efficient decisions[59]. Rubinfeld and Gal are of the view that having access to data has become a valuable asset and create a competitive advantage.[60]

It has been estimated that big data can result in 60% potential increase in retailers' operating margins.[61] Lerner says that online providers of services can use data to improve the quality of their services in many ways, for instance by reaching customers in a manner that is as efficient as possible.[62] Businesses can gain from using big data as they can improve the efficiency of their production processes, forecast market trends, improve their decision-making processes and enhance the segmentation of their customers.[63]

Companies can utilize user data to improve the targeting of advertisements and sell this service in order to obtain more money to spend on the quality of the service and attracting more users ('monetisation feedback loop'). These loops can make it very difficult for a new company to compete with a company with a large customer base.[64] After all it is marketing what most companies do to maintain their position and increase their profits. The Commission has in its Google/DoubleClick decision noted that online advertising is capable of reaching a more targeted audience in more effective manner as companies can target the audience precisely by combining information concerning geographical location, timing, the customer's areas of interest, the customer's purchase history and search preferences.[65] The Commission

[58] OECD (2013), p. 319.
[59] Rubinfeld – Gal (2017), pp. 347.
[60] Ibid, pp. 342-343.
[61] McKinsey Global Institute (2011), p.2.
[62] Lerner (2014), p. 10.
[63] OECD (2016), p. 8.
[64] Ibid, p. 10.
[65] Case No COMP/M.4731 *Google/ DoubleClick*, Decision of 11 March 2008, para. 45.

further held that the merged entity would be able to combine DoubleClick's and Google's data collections and as a result match records from both databases. This could result in individual users' search histories being linked to that user's past behaviour on the internet, which could be used to better target advertisements.[66]

Indeed big data could be used for private gains for companies[67] and the fact that access to data is often not allowed for competitors, indicates the value of data for companies.[68] However, arguing that big data only benefits companies would be a narrow approach as it leaves out innovation leading to improved quality and better targeted ads for consumers leading to a more informed consumer experience provided that the information is presented in a proper manner. In addition, the importance of big data is not limited to commercial purposes of large companies. Indeed big data can be the factor in improving areas such as medicine, climate food safety and other areas.[69]

Big data does not only produce benefits to companies and society but also to consumers such as the use of so called free services, improvement of quality and increases in innovation. However, here lies a caveat, as the services are not truly free for the consumer as the consumers give up their personal data to the companies.

2.4 The significance of user data for companies

Big data plays a big role in online services such as social media networks in the form of user information. According to Shelanski customer information can enable a company to improve its service offerings and as a result increase the returns. Customer data can also be a strategic asset that allows the company to maintain its position in the market and to curtail entry into the market. User information can also amount to a commodity, which the company sells to other companies.[70] Even at the Commission level there has been acknowledgements concerning the importance of social media as a source of data. Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes in her speech[71] stated that:

[66] Ibid, para. 360.
[67] Ohm (2013), p. 339.
[68] Rubinfeld – Gal (2017), pp. 342-343.
[69] Ohm (2013), p. 339.
[70] Shelanski (2013), p. 1679.
[71] Kroes (2010).

''Many of the "free" services now used by billions on the Internet would not be possible without the income derived from the various forms of online advertising. Advertising revenues – or at least the prospect of such revenues – are the basis of a wave of innovative services that are transforming our economy and society.'' The Commission in *Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV*[72] noted that customers generally tend to give their personal data to many companies who collect and market it and as a result this type of data is generally seen as a commodity.[73] The fact that consumer hand over their personal data for companies has various implications. For instance former Commission Vice-President for Competition Joaquin Almunia has said on June 30, 2014[74]: ''*As to data privacy, it is a fact that Google and other large digital players collect and keep unprecedented amounts of data, including personal data, which can be retrieved and used across their services. This is a legitimate cause for concern which, however, lies beyond the remit of competition policy.*'' The statements by the Commission clearly demonstrate that the significance of big data at least at conceptual level have been noticed by the EU regulator. The emphasis seems to be rather consumer oriented and the conduct of companies from the competition law sense has not been the focus in these arguments. This is understandable as the source of big data often are individuals giving their information online and this tends to shift the focus to the consumer level.

It has not been clear under which area of law and by which authority should the privacy concerns arising from big data be handled. The ECJ has held that any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law and may be handled in accordance with the data protection laws.[75] The Commission analysed the possible concentration of data and whether it was likely to strengthen Facebook's position in the online advertising market or in any sub-segments. The Commission held that any privacy-related concerns resulting from the increased concentration of data within the control of Facebook as a result of the transaction were not within the scope of the EU competition law rules but belong to the scope of the EU data protection rules.[76] Grac-Aubert argues that the

[72] Case No COMP/M.6314 *Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV*, Decision of 4 August 2012 4/09/2012.
[73] Ibid, para. 543.
[74] Speech of Almunia, Joaquin (2014).
[75] *Asnef-Equifax* (see supra note 28), para. 63.
[76] Case No COMP/M.7217 *Facebook/Whatsapp*, Decision of 3 October 2014, para. 164.

Commission choose not to analyse the potential concentration of data which raises implication that the Commission does not have the competence to do so. The result is that the data protection authorities will be the competent authorities.[77] However it is questionable whether any clear implications can be drawn from these statements as the issue as there have not been any consolidating legislation and technologies are rapidly developing leading to the need for the law to adapt to the changes.

[77] Grac-Aubert (2015), p. 227.

3. Competition law

3.1 Background of competition law

Competition law is the branch of law that has as its goal the protection of the process of competition. Competition law is at its fundamental level concerned on the growing market power by companies which can harm consumer welfare for instance by reducing input, reduce quality and innovation.[78]

One form of a harmful practice by a dominant company occurs when the company embarks in abusive behavior towards its competitors.[79] The meaning of dominant position has been clarified in the case law of the ECJ and relates to a position of economic strength that an undertaking has which allows the company to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers.[80] However, a dominant position is the result of a combination of several factors which separately are not necessarily determinative.[81] Market shares in themselves are not solely determinative of dominance, however the longer time and the higher the share, the more credible is the dominance of a company.[82] Other factors such as the constraints from the actual competitors, constraints imposed by the credible threat of future expansion by actual competitors or entry by potential competitors and the countervailing buyer power have to also be taken into consideration when assessing dominance.[83]

The main source of EU competition law is TFEU, which contains various articles governing competition law in the EU. Article 102 TFEU concerns abuses by dominant undertakings. For any undertaking to violate article 102 TFEU, there must be a dominant position, an abuse of that dominant position and an effect on trade between Member States.[84] The concept of abuse is an objective concept relating to the behaviour of an undertaking in a dominant position which has an influence on the structure of a market where, as a result of the presence

[78] Whish (2008), p.1
[79] Ibid, pp. 2-3.
[80] *United Brands* (see supra note 11), para. 65.
[81] *Ibid*, para. 66.
[82] Geradin – Layne-Farrar – Petit (2012), p. 189.
[83] Communication from the Commission (2009), para. 12.
[84] Stothers (2001), p. 256.

of the undertaking, the degree of competition is weakened and which by using methods different from those which condition normal competition has the effect of impeding the maintenance of the degree of competition still existing in the market or the growth of that competition.[85]

Article 102 of the TFEU contains the most important provision for the purposes of dominant companies, namely it provides that among others limiting production, markets or technical development to the prejudice of consumers or applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage amount to an abuse. It is quite obvious why limiting markets or technical development is prohibited from dominant companies, however the second form of abuse concerning 'other trading parties' requires elaboration. The answer to this question becomes clear when taking into consideration that in addition to practices which may cause damage to consumers directly, abuse can also occur when the practices are detrimental to consumers by impacting on the effective competition structure. Abuse may occur if an undertaking in a dominant position strengthens such position in such a way that the degree of dominance reached substantially limits competition, i.e. that only undertakings remain in the market whose behaviour depends on the dominant one.[86] It has been stated in many instances that dominant undertakings have a special responsibility not to engage in conduct that can impair competition.[87]

3.2 Anticompetitive concerns arising from big data

In addition to the possible legal obstacles to sharing of data, companies can also embark on measures that hinder the reuse of data for competitors. Many commentators have argued that it is crucial for the purposes of data reuse for the recipient company to know where the data is coming from, how it has been collected and organized and manipulated. It goes without saying that if companies do not have at their disposal the necessary parameters to further process the data they receive from others, the data loses some or all of its usefulness.

[85] Judgment of the Court of 13 February 1979. Hoffmann-La Roche & Co. AG v the Commission. Case 85/76, EU:C:1979:36, para. 91.
[86] Judgment of the Court of 21 February 1973. *Europemballage Corporation and Continental Can Company Inc. v. the Commission* Case 6/72, EU:C:1973:22, para. 26.
[87] Judgment of the Court of 9 November 1983. *NV Nederlandsche Banden Industrie Michelin v the Commission*. Case 322/81 EU:C:1983:313, para. 57.

Sokol and Comerford introduce an often stated example of anticompetitive situation is where companies cannot compete with larger companies as they lack similar volume of data and this in turn widens the quality gap between the dominant company and its smaller rivals. The larger firm in this situation has no incentives to engage in innovation or to maximize quality of its products. The OECD has noted that market concentration and dominance are favoured by the economics of data. The OECD points out that data-driven markets can lead to a "winner takes all" situation where market success leads to concentration.[88]

The situation is not made easier by the fact that many consumers do not even consider that they trade their information for services from companies. The European Data Protection Supervisor has stated that the markets for personal information are far from being transparent, fair or efficient as the customers are generally not aware of the precise value of the personal data that they give to the companies in exchange for so called free services.[89] According to one research, UK consumers increasingly see their personal data as an asset in data exchanges with organisations. According to the study, the proportion of consumers that hold such a mindset was 56% in 2017.[90] As a result, large companies could invest more on advertisements and on making their services more attractive to gain new users for their services at the expense of smaller rivals.

[88] OECD (2014), p. 7.
[89] EDPS (2015), p. 12.
[90] DMA Group (2018), page 4.

4. Essential facilities

4.1 The background of the essential facilities doctrine

The right to choose the trading partners and freely to dispose of property are generally recognised principles in the Member States laws and incursion on those rights requires justification.[91] On the other hand, it is established legal praxis that companies cannot counter the allegations of anticompetitive conduct by arguing on the freedom to conduct business and the right to property as those principles are subject to public-interest restrictions.[92] Kalimo and Majcher point out that a company with economic strength has a special responsibility to ensure that its conduct does not harm competition, but it's still free to set fair and non-exploitative terms for the dealings.[93] Often essential facilities cases have come up in relation to facilities that had the characteristics of a natural monopoly. It is difficult or economically wasteful to duplicate the facility due to high fixed costs and low marginal costs and that is why natural monopolies are existing.[94]

Against this background it seems clear and reasonable that companies can be forced to share access to their facilities in some instances. The essential facilities doctrine is a more specialised form of the dominant company's duty to deal with its competitors. The classic case of essential facilities is a situation where a competitor wants to become a new customer of the dominant company and seeks access to a physical resource controlled by the dominant company by offering remuneration. The refusing dominant company may then be forced to share its infrastructural resources, networks or other facilities with a competitor which is unable to function in the market without such access.[95]

The Commission has noted in its Guidelines, that the concept of refusal to supply covers a broad range of practices, such as when the dominant company refuses to supply products to existing or new customers, intellectual property rights related refusals to supply, or refusal

[91] Opinion of Advocate General Jacobs delivered on 28 May 1998. *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and Others*. Case C-7/97, EU:C:1998:264, para. 56.
[92] Judgment of the Court (Second Chamber) of 29 June 2006. *SGL Carbon v Commission*. Case C-308/04 P, EU:C:2006:433, para. 108.
[93] Kalimo – Majcher (2017), p. 228.
[94] Polonetsky – Tene (2013-2014), p. 2013.
[95] Ong (2005), p. 217.

to grant access to an essential facility or a network.[96] However, the essential facilities doctrine cannot be applicable to mere processes even if these production processes result in competitors' activities uneconomic.[97] O'Donoghue and Padilla prefer the interpretation that essential facilities concern 'stage of production' meaning something that is capable of being sold or licensed and resembles real market.[98]

According to the Commission's Guidelines, competition problems typically arise when the dominant undertaking and the buyer whom it refuses to supply compete on the downstream markets. The Commission defines the term 'downstream market' as the market for which the refused input is needed in order to manufacture a product or provide a service.[99] This is not always the case with data intense markets as companies often need the data to develop their services and products. The companies' products and services in these cases compete at the same level of the market. As a result, the conventional market analysis might not be the most suitable tool to assess the market for companies' products that rely on big data.

4.2 The requirements for the essential facilities doctrine

One of the first cases of essential facilities in the EU was the *Sea Containers v. Stena Sealink*[100], where the Commission held that where an undertaking has a dominant position in the provision of an essential facility and does not grant access to competitors (who cannot provide services to their customers without such facility), without objective justification or grants access to competitors only on terms less favourable than those which it gives its own services, infringes EU competition law.[101] The *Bronner*[102] case was about a nationwide home-delivery scheme consisting of delivering the newspapers directly to subscribers. Eagles points out that the distribution system in *Bronner* case was in strict legal terms nothing more than a network of interlocking contracts and was not a form of property, intellectual or otherwise.[103] This supports the argument that even data itself could be an essential facility if one considers whether data is capable of being an asset without which the competitors of a

[96] Communication from the Commission (2009), para. 78.
[97] O'Donoghue – Padilla (2006), p. 438.
[98] Ibid, p. 439.
[99] Communication from the Commission (2009), para. 76.
[100] Case COMP IV/34.689 *Sea Containers v. Stena Sealink*, Decision of 21 December 1993.
[101] *Sea Containers v. Stena Sealink (Commission)* (supra note 17), para. 66.
[102] *Oscar Bronner* (see supra note 18).
[103] Eagles (2006), p. 409.

dominant company could not conduct business. Waller and Tasch argue that in addition to traditional infrastructure, a variety of resources including certain software platforms, and the internet satisfy the criteria for essential facilities.[104]

One of the most best known EU cases dealing with refusal to supply is the Magill case[105], in which the court laid out the principle that in order for the refusal to be abusive. First of all, the refusal has to prevent the appearance of a new product, which the requesting party does not offer and for which there is a potential consumer demand. Second, there should be no justification for such refusal. These requirements have been developed in subsequent case law of the ECJ, which will be discussed below. It is interesting to compare the Magill criteria to the views of the Commission. The Commission considers the following criteria when determining whether an obligation to deal should be imposed on an undertaking: the refusal has to relate to a product or service that is objectively necessary to be able to compete effectively on a downstream market, the refusal is likely to cause the elimination of effective competition on the downstream market, and the refusal is likely to result in consumer harm.[106] Both approaches emphasize the indispensability of the facility and consumer perspective. These criteria will be discussed in detail below.

4.2.1 The indispensability requirement

In the *Bronner* case the ECJ noted that it is necessary, not only that the refusal of the service bis likely to eliminate all competition in the relevant market of the party requesting the service and that such refusal cannot be objectively justified, but also that the service in itself is indispensable to carrying on the requesting party's business, to the extent that there is no actual or potential substitute in existence for the required facility.[107] The *Bronner* case concerned the distribution system for newspapers and the ECJ noted that alternative methods of distributing daily newspapers, even though possibly less advantageous for the distribution of certain newspapers, exist and were used by the publishers of those daily newspapers.[108] The ECJ also pointed out that there were not any technical, legal or economic obstacles

[104] Waller – Tasch (2010), p. 764.
[105] Judgment of the Court of 6 April 1995. *Radio Telefis Eireann (RTE) and others v the Commission*. Joined Cases C-241/91 P and C-242/91 P, at paras. 54-55.
[106] Communication from the Commission (2009), para. 81
[107] *Oscar Bronner* (see supra note 18), para. 41.
[108] *Ibid*, para. 43.

making it impossible, or even unreasonably difficult, for any other publisher of daily newspapers to establish, alone or with other publishers, its own nationwide home-delivery scheme and use it to distribute its own daily newspapers.[109] Finally the ECJ noted that access can be only indispensable, if at the very least it can be established that it is not economically viable to create a second home delivery scheme for the distribution of daily newspapers providing the circulation comparable to that of the daily newspapers distributed by the existing scheme.[110]

O'Donoghue and Padilla point out that the question therefore is whether a company operating on the same scale as the dominant firm could develop its own facilities, not whether the requesting party can.[111] It follows that the facility has to be crucial not only to requesting company's activities but also for the larger and hence more competitive entrants. Eagles is of the opinion that this distinction recognizes in an implied manner that it is not the role of an economically rational competition law to encourage inefficient entry or assist companies simply because they are small.[112] Stothers points out that there are views that in markets where the parties do not sell products or services directly to the consumer, some stricter analysis should be applied than the one considered in the *Bronner* case.[113] This would be an important factor in order to avoid free riding from companies that only use data as a raw material to improve their services and enhance their own data.

Advocate General Jacobs was of the opinion in the *Bronner* case that the application of the essential facilities doctrine is justifiable only in cases in which the dominant company has a position on the market amounting to a genuine stranglehold. This could happen for instance where duplication of the facility is impossible or extremely difficult due to physical, geographical or legal constraints or is highly undesirable for reasons of public policy. Furthermore, it is not sufficient that the control of a facility gives the undertaking a competitive advantage.[114] For the cost of duplicating the facility alone to amount to a barrier to entry, the cost must be at such a level as to prevent any prudent undertaking from entering the market.[115]

[109] Ibid, para 44.
[110] Ibid, para 46.
[111] O'Donoghue – Padilla (2006), p. 426.
[112] Eagles (2006), pp. 409-410.
[113] Stothers (2001), p. 260.
[114] Opinion of Advocate General Jacobs in *Oscar Bronner* (supra note 91), para. 65.
[115] Ibid, para. 66.

Graef argues that in *Microsoft*, the Court lowered the indispensability standard by concluding that in order to be able to compete viably, competitors should be able to interoperate with the Windows domain architecture at an equal level with the Microsoft systems.[116] He compares this judgment to the *Bronner* case, where it was held that it is not decisive whether the product that is demanded is the most advantageous possibility, as long as there are alternatives which are economically viable for competitors.[117] He concludes that according to the Microsoft judgment, as long as the alternatives do not put the competitor at an equal level, the product amounts to an indispensable product.[118]

In order for the indispensability requirement to be satisfied, there should be no effective substitutes available.[119] However, as has been noted in relation to the nature of data, there are very few situations in which data is not available from another source than from the company refusing access as data is often non-rivalrous. It might prove to be challenging however to analyze what other sources of data are sufficiently similar to be effective substitutes, but this does not in my opinion change the fact that the substitutability of data is in general quite feasible.

4.2.2 The new product requirement

According to the Commission, it is not necessary that without the refused input, no competitor could ever enter or survive on the downstream market. Rather, an input is indispensable where there is no actual or potential substitute on downstream competitors can rely so as to counter at least in the long-term the negative consequences arising from the refusal. The Commission will in these instances make an assessment of whether it is possible and feasible for competitors to effectively duplicate the input of the dominant undertaking in the foreseeable future.[120]

When the requested facility is instead an intellectual property right, the focus turns on the nature of the requesting party's own product and on the potential consumer demand of such

[116] Graef (2011), pp. 6-7.
[117] Ibid, pp. 6-7.
[118] Ibid, p. 7.
[119] Hou (2012), p. 460.
[120] Communication from the Commission (2009), para. 83.

a product. This is demonstrated in the *IMS* case[121], where it was held that the refusal by a dominant undertaking to allow access to an indispensable product protected by an intellectual property right may be regarded as abusive only where the requesting undertaking does not limit itself essentially to duplicating the goods or services already offered on the secondary market by the owner of the intellectual property right, but intends to produce new goods or services that are not offered by the right owner and for which there is a potential consumer demand.[122] Ezrachi and Maggiolino see this problematic as by stripping IMS of its main asset, the Court challenged not only the alleged abuse, but also the dominant position of IMS itself.[123]

The Commission and the ECJ in the case of *Microsoft* extended the requirement for a new product to that of follow-on innovation. The Commission went beyond a mere analysis of the 'new product' criterion as defined in IMS Health and concluded that Microsoft's refusal was a 'refusal to allow follow-on innovation', in other words, the development of new products, and not a mere refusal to allow copying.[124] The General Court held that the circumstance relating to the appearance of a new product, as envisaged in *Magill* and *IMS Health*, cannot be the only parameter which determines whether a refusal to license an intellectual property right is capable of causing prejudice to consumers and that such prejudice may arise where there is a limitation not only of production or markets, but also of technical development.[125]

Ezrachi and Maggiolino argue that in the Microsoft case, the Court used Article 102(b) of the TFEU to expand the Magill criteria by adding innovation into it and thus lowered the threshold for refusals to license to be abusive. This development has introduced legal uncertainty.[126] Ezrachi and Maggiolino also argue that in *Microsoft*, the CFI introduced the idea of economic indispensability by holding that although access to the market might have been technically possible, Microsoft's refusal to license the interoperability information eliminated the economic viability of any entry into the market.[127]

---

[121] Judgment of the Court (Fifth Chamber) of 29 April 2004. *IMS Health GmbH & Co. OHG and others v. the Commission*. Case C-418/01, EU:C:2004:257.
[122] Ibid, paras. 48-49.
[123] Ezrachi – Maggiolino (2012), p. 605.
[124] *Microsoft Corp v. the Commission* (see supra note 18), para. 457.
[125] Ibid, para. 647.
[126] Ezrachi – Maggiolino (2012), p. 602.
[127] Ibid, p. 603.

4.2.3 The elimination of competition requirement

One question arising in relation to the requirements of essential facilities is whether competition has to be eliminated immediately or is it sufficient that there is a threat of such an elimination. The Commission and the ECJ in the *Microsoft* case clarified that there is no need to establish that competition has already been eliminated or, at least, that its elimination is imminent.[128] According to the Commission, the likelihood of effective competition being eliminated is affected by factors such as the size of the market share of the dominant undertaking in the downstream market. The likelihood of effective competition being eliminated is in general increased when the market share of the dominant undertaking in the downstream market grows. The less capacity-constraints the dominant undertaking faces compared to competitors in the downstream market, the closer the substitutability between the dominant undertaking's output and that of its competitors in the downstream market, the greater the proportion of competitors in the downstream market that are affected, and the more likely the demand that could be served by the foreclosed competitors would be diverted away from these competitors to the benefit of the dominant company.[129] In relation to big data, there are unlikely to be capacity constraints as data is a non-tangible good, however it is difficult to say what level of substitutability each data set has and what the likelihood is that the demand could be diverted from foreclosed competitors to the dominant company.

4.3 Potential justifications for refusal to supply

The duty to deal is not automatically imposed on an undertaking even in situations where the above requirements of the essential facility doctrine are met as the Commission will look into whether from consumer perspective, the likely negative consequences of the refusal to supply are greater over time compared to the negative consequences of imposing an obligation to supply.[130] According to the Commission, a refusal to supply might be necessary to allow the dominant undertaking to receive an adequate return on the investments made in order to develop its business, thus creating incentives to continue to invest in the future, while acknowledging the risk that projects do not always succeed. The dominant undertaking is free to assert that its own innovation will be negatively affected by the obligation to supply,

[128] *Microsoft Corp v. the Commission* (see supra note 18), para. 457.
[129] Communication from the Commission (2009), para. 85.
[130] Ibid, para. 86.

or by the structural changes in the market conditions that imposing such an obligation will bring about, including the development of follow-on innovation by competitors.[131] However the dominant undertaking has to demonstrate any negative impact which an obligation to supply is likely to have on its innovation. If a dominant undertaking has supplied the input to the companies before, this can be relevant for the assessment of any efficiency based justification claims.[132]

The Commission will consider the possible claims made by the dominant undertaking that said undertaking's conduct is justified in the way that the conduct is objectively necessary or that the conduct produces substantial efficiencies which outweigh the anticompetitive effects produced on consumers. The Commission will assess whether the conduct is indispensable and proportionate to the dominant undertaking's claimed goal.[133] According to the Commission, factors outside of the dominant undertaking are used to determine the question of whether the conduct is objectively necessary and proportionate.[134] However, even technical and commercial reasons can be taken into consideration.[135]

In order to succeed in justifying its refusal to supply the Commission states that the dominant undertaking has to show that four cumulative conditions are fulfilled.[136] First, the efficiencies have been, or are likely to be, realised as a result of the conduct (for example improved quality of goods, or a reduction in the cost of production or distribution of the goods). It is not enough that there is an increase in the total wealth of the society, but the benefits arising from the increased efficiencies have to be received by the consumers and not remain at the company's disposal.[137] Second, the conduct has to be indispensable in order to acquire the efficiencies so that there must be no less anti-competitive alternatives to the conduct capable of producing the same efficiencies. Third, the likely efficiencies resulting from the conduct have to outweigh any likely negative effects on competition and consumer welfare in the markets affected. Finally, the conduct should not result in total elimination of effective competition. According to the Commission, exclusionary conduct which maintains, creates or

[131] Ibid, para. 89.
[132] Ibid, para. 90.
[133] Ibid, para. 28.
[134] Ibid, para. 29.
[135] Judgment of the Court (Fifth Chamber) of 3 October 1985 *Centre belge d'études de marché — Télémarketing (CBEM) SA and Compagnie luxembourgeoise de télédiffusion SA Information publicité Benelux SA*. Case 311/84, EU:C:1985:394, at para. 26.
[136] Communication from the Commission (2009), para. 30.
[137] Geradin – Layne-Farrar – Petit (2012), p. 22.

strengthens a market position and is close to a monopoly cannot be justified in normal cases by arguing that it also creates efficiency gains.[138]

Applying the above Commission's criteria to refusals to supply data to competitors demonstrates the complexity of the issue. The dominant company must be able demonstrate that its conduct is done in order contribute to improve the production or distribution of products or to promote technical or economic progress.[139] The dominant company has the burden to raise any plea of objective justification.[140] It might prove quite challenging for companies to demonstrate just how the refusal to share data might achieve these requirements.

The company would have to demonstrate efficiencies resulting from such a refusal. Efficiencies on the contrary seem to be more readily realized when more companies have access to data that enables them to produce better products and services. The second requirement is the indispensability to achieve the alleged efficiencies requirement which is for the dominant company to demonstrate. Therefore, the dominant company must be able to demonstrate why alternatives for the conduct would be significantly less efficient.[141] It is hard to see how the refusal could be indispensable to realizing such efficiencies for the company as the company is still able to keep the data to itself and keep analyzing it further due to its non-rivalrous nature. Finally the balancing act between the efficiencies and negative effects could prove to be very challenging.

[138] Communication from the Commission (2009), para. 30.
[139] DG Competition discussion paper (2005), para. 85.
[140] *Microsoft Corp v. the Commission* (see supra note 18), para. 688.
[141] DG Competition discussion paper (2005), para. 86.

5. Big data and the essential facilities doctrine

5.1 Data as an essential facility

Companies can have strong incentives to engage in certain conduct in order to maintain their competitive advantage in relation to data such as limiting other companies' access to data, preventing the sharing of the data, and opposing data-portability policies.[142] Ursic and Custers are of the view that liability under Article 102 TFEU appears to be most likely in situations where a party seeking access needs the user data as an input for a new product that would not be in direct competition with the main product of the online platform provider's.[143] Even at the regulatory level, there have been concerns over the use of personal data to facilitate the infringement of competition law. Vice President of the European Commission responsible for Competition Policy, Joaquín Almunia has said[144] that: *''the commercial value of personal data has grown exponentially. In spite of this, DG Competition has yet to handle a case in which personal data were used to breach EU competition law. But we cannot rule out this eventuality. In time, personal data may well become a competition issue; for instance, if customers were prevented from switching from a company to another because they cannot carry their data along.''*

Having considered the nature of data and the prerequisites for the essential facilities doctrine, it is possible to embark on an analysis on some of the cases that have dealt with refusal to grant access to data by companies.

In the English case of *Attheraces*[145], the court was of the opinion that pre-race data held by the party responsible for the administration of British racing, was essential to the business of a party who used the information to maintain his services. There was no substitute for the information with the administrator being the only supplier of said data in the market. It would have been prohibitively expensive and difficult and rather impractical for any other person to process and supply the same data.[146] The court held that the control of the pre-race data

[142] Stucke – Grunes (2015), p. 3.
[143] Ursic (2016), p. 230.
[144] Speech of Almunia, Joaquin (2012).
[145] Judgment of 21 December 2005. *Attheraces Ltd & Anr and The British Horseracing Board & Anr* [2005] EWHC 3015 (Ch).
[146] Ibid, p. 39.

was an essential facility and that the refusal to supply the data amounted to an abuse of dominance.[147] Interestingly the judge in the case was of the opinion that it did not matter whether the parties are in competition or potential competition for an unreasonable refusal to supply to amount to an abuse of a dominant position within Article 102 TFEU.[148] According to the Court, the effect may be for example to deter the market entry of other companies, or to encourage the purchaser to exit the market, or to limit the purchaser's activities within the market.[149]

The Finnish Supreme Administrative Court has ruled on a case concerning abuse of dominance in relation to data. The case was an appeal by Suomen Numeropalvelu Oy (''Numeropalvelu'') after the Market Court had ruled that Numeropalvelu had abused its dominant position by refusing to give certain information to Eniro Finland Ab (''Eniro'') on the grounds that due to data privacy laws, the service providers are not allowed to offer their services for free and without registration on the internet to end users.[150] Numeropalvelu had terminated its contract with Eniro and notified Enrio that it would no longer update Eniro's electronic database used for search.[151] According to the then Finnish Competition Authority, Numeropalvelu had breached Finnish competition law by refusing to conduct business without adequate reason and had applied unreasonable terms.[152] The market could held that Numeropalvelu's claimed justification for refusal based on data privacy laws was not adequate. Numeropalvelu argued that the subscribers should have been informed about the use of the contact details in Eniro's service or that consent should have been acquired, however according to Market Court, this was not a factor to be taken into consideration in these types of situations.[153]

These cases demonstrate how national courts have been able to recognize situations in which data sets can amount to essential facilities and furthermore have been able to consider whether the refusal to deal amounts to an abuse. The Numeropalvelu case demonstrates how the collision between the essential facilities doctrine and data privacy have been dealt with by the Court, although in that case the Court choose to disregard the data privacy concerns

[147] Waller – Tasch (2010), p. 747.
[148] *Attheraces* (supra note 145), p. 38.
[149] Ibid, p. 38.
[150] The Finnish Competition and Consumer Authority (2013).
[151] Market Court Judgment of 6 April 2009. Case *MAO:178-179/09,* para. 4.
[152] Ibid, para. 306.
[153] Ibid, para. 253.

as a valid argument for the refusal to share the data. However, this is a case decided before the GDPR and furthermore is at the national level. As a result no conclusions should be drawn from it concerning the collision of data privacy and competition law.

5.2 Characteristics of big data that support the application of the essential facility doctrine

Stucke and Grunes argue that if big data was truly ubiquitous, low cost and widely available as often claimed, then companies would not waste money and time by offering ''free'' services in order to gain the personal data of their users.[154] The Franco-German competition report notes that the collection and the ways in which data are used could be a factor that raises entry barriers and be a source of market power.[155] In relation to data, the barriers can be technological, legal, or behavioral with often the combination of both. However, there are barriers that are not unique to data such as barriers arising from two-sided markets or network economies.[156]

Rubinfeld and Gal argue that certain entry barriers are unique to big data, such as storage of large volumes of data. Furthermore, the specific characteristics of the data necessary for a particular market in which the data serve as an input can have an influence on the intensity and type of entry barriers.[157]

The non-rivalrous nature of big data basically means that technology wise it can be easily and cheaply copied and shared for instance by selling and licensing their data sets to multiple users. However with big data one must keep in mind that not only its collection is relevant, but also the organization, storage, and analysis which can be said to transform data into a private good.[158] Despite the fact that data is said to be non-rivalrous, whether one data set is necessary for all companies to operate will depend on whether it is a replicable or non-replicable asset. This depends how the particular data is used and why it is processed.[159] Even

[154] Stucke – Grunes (2016), p. 42.
[155] Autorité de la Concurrence and Bundeskartellamt (2016), p. 11.
[156] Rubinfeld – Gal (2017), p. 369.
[157] Ibid, p. 349.
[158] Ibid, p. 373.
[159] Cowen (2016), p. 16.

if particular data set can be copied, this does not mean it will remain as valuable.[160] Furthermore, the value of data for companies relates more to the need to be able to understand the changing customer needs instead of using historical past data.[161] Big data requires the capacity to analyse largely unstructured data sets from diverse sources which is only possible by linking data sets. This type of data is highly context-dependent and may be of no value outside the exact context. Some estimations state that the amount of unstructured data in businesses could amount to 80% to 85% of the amount of data.[162]

Rubinfeld and Gal have identified three types of barriers to entry at the stage of collection of big data. The first one is that of technological barriers, which refer to situations, where data cannot be easily replicated. This might be the case if the data were created as a result of a distinctive interaction. Another barrier relates to the point in time that a certain company has started gathering data. Finally, the whole system for data collection may also create technological entry barriers.[163] Rubinfeld and Gal argue that a barrier related to technological supply-side can arise where companies have achieved substantial economies of scale or scope through investments which are partially or wholly sunk. Therefore, where economies of scope are large, this might create entry barriers to companies that have access to merely one source of data.[164]

According to the Franco-German competition report, due to the sheer size of an incumbent's data set, it might not be possible for competitors to simply buy the data from a third party. This is especially so where the incumbent has a large customer base and offers free services to consumers who generate large number of data.[165] The Franco-German competition report states that the collection of data could result in entry barriers in cases where entrants cannot collect the data or buy the same kind of data when it comes to the volume and variety of the data.[166] Even the Commission has noted in the *Google/DoubleClick* decision that competition based on the quality of collected data does not simply depend on the size of the database, but also depends on the variety of data that competitors have access to and whether it will

[160] Stucke – Grunes (2016), p. 44.
[161] Lambrecht – Tucker (2015), p. 16.
[162] OECD (2013) p. 325.
[163] Rubinfeld – Gal (2017), p. 350-351.
[164] Ibid, p. 352.
[165] Autorité de la Concurrence and Bundeskartellamt (2016), p. 12.
[166] Ibid, p. 11.

be useful for conducting internet advertising.[167] The Franco-German competition report states that the non-rivalrous nature of data does not mean that all companies have access to data or able to collect data on an equal footing. These issues should be dealt on a case-by-case analysis.[168]

Stucke and Grunes argue that the authorities and courts will not be focusing on important entry barriers, namely network effects, if they focus on traditional entry barriers in relation to data.[169] Free entry of companies to the market might not decrease the market power of an incumbent company where there are consumer switching costs and learning costs resulting in changing to the competitors' products.[170] Sokol & Comerford explain that network effects are present in online platforms meaning that a service becomes more valuable to its user when more people use the same service. Indirect network effects refer to uses not being in direct contact with each other.[171] Sokol & Comerford are of the opinion that users may switch companies simply due to an innovative product regardless of the existence of network effect enjoyed by the larger company.[172]

However this statement might be too bold as even innovative products require marketing and economies of scale thus placing larger companies at an advantage. Rubinfeld and Gal argue that network effects can create a barrier to entry in the context of data, where the quality of the product is influenced by the quality of the data and the quality of the data is in its turn influenced by the number of data entries, their variety, and how up to date they are.[173] The Franco-German competition report notes that smaller competitors may be marginalized due to data access becoming differentiated as the larger amount of data a company has, the more it can support its services and attract more customers and data. The company holding large amounts of data can afford even better data analytics tools and by using them, attract even more customers.[174] The loss of users will likely result in the decrease in the quality of the company's products and result in less people using the products.[175]

[167] *Google/DoubleClick* (supra note 65), para. 273.
[168] Autorité de la Concurrence and Bundeskartellamt (2016), p. 42.
[169] Stucke – Grunes (2016), p. 160.
[170] Motta (2008), p. 79.
[171] Sokol – Comerford (2016), p. 1148.
[172] Ibid, p. 1149.
[173] Rubinfeld – Gal (2017), p. 355.
[174] Autorité de la Concurrence and Bundeskartellamt (2016), p. 13.
[175] Stucke – Grunes (2016), p. 201.

The Franco-German competition report points out that even in so called free services, consumers might not necessarily multi-home that readily as switching costs can prevent consumers from using various providers in equal proportions especially where the quality is the only parameter for competition.[176] The Franco-German competition report points out that multi-homing by consumers and diversification of services by a company might not be that simple as access to data might depend on the capacity of the company to build a customer base that is sufficiently large. This depends on the presence of network and experience effects and economies of scale as entry barriers.[177]

Another factor to consider are industries where data is used to deliver a personalized experience for the user, and plays an important role in customer experience. In such industries, there might be few substitutes for big data.[178]

The intensity of the barrier to entry also depends on the consumers' switching costs. However, two-sided markets do not necessarily mean that entry barriers are high. The switching costs and lock in effects manifest themselves in the investment of time needed for the consumer to learn to use a platform, the number of complementary products available to the consumer, or the fact that the consumer's friends use the same platform.[179] Koponen and Mangiaracina argue that if customers are locked in and it is not possible for them to make use of other service offerings, or their ability to do this is reduced significantly, competitors may be foreclosed. As a result the control of personal data is a way of excluding rivals.[180] As already discussed, consumers can give their personal data to many companies simultaneously, however the incentive to do this might be diminished if the consumer simply cannot change to another service provider due to technical or contractual obstacles.

[176] Autorité de la Concurrence and Bundeskartellamt (2016), pp. 27-29.
[177] Ibid, p. 53.
[178] Lambrecht – Tucker (2015), p. 13.
[179] Stucke – Grunes (Research paper) (2015), p. 8.
[180] Koponen, Jonas – Mangiaracina, Annamaria, 2013 ''No Free Lunch: Personal Data and Privacy in EU Competition Law''. In *Competition Law International*, Vol. 9(2), p. 190.

5.2.1 The uses of data

The Finnish Competition and Consumer authority has noted that even if data bases were public, the established companies might have at their disposal advanced analytical techniques or a reputation as a trusted company causing new entrants to be marginalized. In situations where the data are not public, the established actors in the market can have a significant advantage in the market rendering it difficult, costly and time consuming to meet the offers made by the incumbents.[181] Rubinfeld and Gal argue that the value of data itself is often low and only becomes valuable through analysis that alters unstructured pieces of data into information and derived information i.e. creating new information that cannot be acquired from data directly. This data-based information allows companies to embark on product improvement and to better target consumers as well as to have an improved knowledge of different parties among other things. Data-based information can also benefit individuals enabling them to enjoy better products for instance.[182]

Cowen criticizes the part of the Commission's decision in *Facebook/Whatsapp* merger, where it referred to the generic collection of data and took no account of the unique nature of user data held by WhatsApp on its users. He argues that if the alternative sources of raw data do not create same or similar knowledge then the accumulation of knowledge than that the combined entity cannot be replicated. According to Cowen the Commission probably failed to consider that data about one consumer preference collected by one company in one situation is not much use as a substitute for data concerning something else collected by another company. Cowen argues that the competition authorities have not properly considered the situation in which datasets of companies form unique collections of data making them unique as a result, and whether they can be competitive advantages.[183] The Commission has in *TomTom/Tele Atlas*[184] analyzed the degree of demand-side substitutability between digital map databases for navigation purposes and for non-navigation purposes and held that the substitutability is limited, because the quality requirements differ very much in

[181] Statement of the Finnish Competition and Consumer Authority (2016).
[182] Rubinfeld – Gal (2017), p. 342.
[183] Cowen (2016), p. 22.
[184] Case No COMP/M.4854 *TomTom/Tele Atlas* Case of 14 May 2008.

detail, accuracy and level of update as well as in the amount of attributes and add-on layers.[185] This is an ample example of how the Commission is able to analyze the different levels of substitutability of data, even though this case was a merger decision.

5.2.2 The freshness of data

As has been discussed already, data is most useful when it is fresh. Therefore information on past behavior is not sufficient and even if companies purchase data from data providers, the companies with established user base enjoy advantages over such companies.[186] Margrethe Vestager has in her speech said that it might not be easy to build a strong market position by utilizing data that goes out of date quickly. She pointed out that it is important to analyze the type of data to see whether it stays valuable. Vestager also pointed out that is necessary to look at what are the reasons that hinder companies from collecting the same data from their own customers than another company is already doing.[187] However, as discussed previously, it may not be the collection of the data, as much as the capability of a company to extract useful information in a timely manner from a large volume and variety of data resulting in a competitive advantage.[188]

5.2.3 The economic costs of creating data assets

The economics aspect also plays its part in the analysis as potential entrants do not constrain the dominant companies in markets with high fixed sunk costs such as requiring high and risky investment before entry.[189] The Franco-German report notes that the costs of collection of data can be significant for instance in the form of fixed costs in setting up data centres. Furthermore a new entrant would have to set up platform that can provide services that enable the collection of data from a sufficiently large number of users that also increase the quality of the service. It might be challenging for companies to convince the customers to give their personal data.[190] If a company has the capability to further process the data and maintain its utility, then such dataset might prove to be a larger barrier for new entrants. Despite the general view that data itself is non-rivalrous, the Franco-German competition

[185] Ibid, para. 22.
[186] Graef (2015), p. 488.
[187] Speech of Vestager, Margrethe (2016).
[188] OECD (2016), p. 22.
[189] Motta (2008), p. 75.
[190] Autorité de la Concurrence and Bundeskartellamt (2016), p. 38.

report notes that there might be limits on the possibility to access data. Furthermore, the Franco-German competition report points out that the scope of data that data brokers can sell to a company could be limited both in volume and in variety.[191]

5.3 Characteristics of big data that do not support the application of the essential facilities doctrine

This part of the essay will analyze the arguments against big data being a barrier to entry for competitors. It will largely draw on the nature of big data as discussed earlier. The nature of data plays a crucial part in analyzing the possible competitive constraints that can relate to data. From the point of view of competition law it should be noted that being big is not as such an offence under competition law.[192] Even if a large company has a large set of data at its possession this does not at least prima facie lead to competition concerns, especially where competitors can collect this data somehow themselves.[193]

While it is relatively easy to perceive that infrastructures such as transport, communication or energy facility networks are not feasible to duplicate,[194] data itself is not a tangible good meaning that, once recorded, it can be re-used many times without loss of fidelity.[195] It is obviously non-feasible to duplicate infrastructures such as transport, communication or energy facility networks.[196] However in contrast to physical structures mentioned above, data itself is intangible. Lerner argues that the claims that competitors can be foreclosed through the collection of user data are based on assumptions that user data is an essential input, large amounts of such data are needed to compete efficiently and that large companies foreclose smaller competitors from access to this data. However, online providers in reality do not have actual exclusivity over user data and its nature is non-rivalrous meaning that websites are free to collect the same data from a same user for same types of activities. In relation to user data, there are usually no exclusive contracts with users preventing them from parting their personal details or user data to competitors, no loyalty discounts that lock users into certain platforms.[197] Kennedy argues that the possession of data can be compared to the

[191] Ibid, p. 39.
[192] Sokol – Comerford (2016), p. 1130.
[193] Ibid, p. 1135.
[194] Raspaud (2014), pp. 71-72.
[195] Communication from the Commission (2014), p. 4.
[196] Raspaud (2014) pp. 71-72.
[197] Lerner (2014), p. 20.

situation where a company builds an expensive factory before it sells a single product or collects a large amount of workers. In these situations the factory or the workers are not barriers to entry as such. Furthermore collecting data is relatively cheap.[198]

The Commission has considered the nature of data in various merger decisions in the past. Margrete Vestager pointed out that the Commission has looked at similar issues in Google's acquisition of DoubleClick and Facebook's purchase of WhatsApp. The Commission did not see any concerns in these mergers as post mergers, other companies would have access to many sources of useful data.[199] The Franco-German competition report is of the view that the Commission in the *Google/DoubleClick* decision took into account the possibility for competitors to access similar data as the merged entity.[200] Furthermore the amount of available data could increase due to the presence of data brokers and the nature of digital markets where data collection is particularly common.[201]

After these preliminary points on the nature of data and its relation to the essential facilities doctrine this thesis will move on to discuss and analyze whether the requirements of the essential facilities doctrine are satisfied in relation to big data.

5.3.1 Indispensability

As has been discussed above, one of the core requirements for the application of the essential facilities doctrine is the indispensability of the facility meaning that the service in itself has to be indispensable to for the business in the way that there is no actual or potential substitute available for it.[202] Lambrecht and Catherine E. Tucker argue that widely available free open source technologies allows companies to analyze large datasets and consumers leave traces of their information to the internet increasingly thus making it possible for companies to obtain useful data for business purposes.[203]

---

[198] Kennedy (2017), p. 8.
[199] Speech by Margrethe Vestager, 2016 ‘’Competition in a big data world’’. Available at <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en> (accessed on 19 March 2018).
[200] Autorité de la Concurrence and Bundeskartellamt (2016), p. 34.
[201] Ibid, p. 36.
[202] *Oscar Bronner* (see supra note 18), para. 41.
[203] Lambrecht – Tucker (2015), p. 7.

The Commission has in some merger decisions analyzed the indispensability related nature of data. For instance in the *Facebook/Whatsapp* merger, the Commission held that the use of one consumer communications app does not exclude the use of apps made by competitors by the same user.[204] Furthermore the Commission stated that users of consumer communications apps are not locked-in to any particular physical network, hardware solution or anything else requiring replacement if one wishes to chance the service provider.[205] According to the Commission regardless of whether the merged entity would use WhatsApp user data for the purpose of targeted advertising on Facebook's social network, there will remain a large amount of Internet user data that Facebook does not have exclusive control over.[206] While these arguments seem quite well justified, it is still necessary to point out that they concern specific case and specific market, but the Commission will likely consider these factors in other similar cases as well. As has been mentioned earlier, data is often simply an input for other products rather than being a product of its own. As a result, entry barriers should be analyzed beyond the specific market to cover the related parts forming the data-value chain.[207]

In relation to markets that utilize user data, it has to be emphasized that consumers often multihome, meaning that they use various service providers and share their data to different parties instead of just one company. Multihoming is a factor that reduces the market power of companies.[208] The Commission held in *Facebook/Whatsapp*[209] that consumer communications applications are a sector that develops rapidly and is characterized by low switching costs and barriers to entry/expansion. Furthermore leading market positions even if supported by network effects could be challenged by competitors and there had been entry by new players. The threat from new companies is a significant disciplining factor for the merged entity, no matter how large its network is.[210]

In *Telefonica UK/Vodafone UK/Everything Everywhere/JV*[211], the Commission concluded that the joint venture could collect a wide range of consumer information in the possible sub-

[204] *Facebook/Whatsapp* (supra note 76), para 133.
[205] Ibid, para. 134.
[206] Ibid, para. 189.
[207] Rubinfeld – Gal (2017), p. 375.
[208] Sokol – Comerford (2016), p. 1137.
[209] *Facebook/Whatsapp* (supra note 76).
[210] Ibid, para. 132.
[211] *Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV* (supra note 72).

markets, but that there were other strong and established competitors that could also offer comparable solutions. The Commission held as a result that other providers of advertising services would not be foreclosed from an essential input.[212] The Commission held there were no entry barriers due to the facts of the case, but the analysis confirmed that personal data could be used for anticompetitive means in order to exclude rivals from the market.[213] The Franco-German competition report notes in relation to essential facilities that the requirements of essential facilities are only satisfied where the incumbent's data is truly unique and that there is no possibility for the competitor to have possession of the data it needs to perform its services.[214]

5.3.2 New product

As has been discussed in relation to the requirements of the essential facilities doctrine above, the refusal by a dominant company to license its data to its competitor should prevent the development of new products or follow-on innovation. In relation to data driven markets, it is relatively easy to conclude that companies can through the use of big data innovate and develop new products and services. For instance, in the online environment market players do not merely compete by lower prices and improved products but also by introducing new products and services affecting consumer demand.[215] There are various industries that use large data sets to improve operations, for instance communications firms and gaming industries.[216]

One situation where the new product requirement is unlikely to be satisfied is where a competitor seeks to gain access to the dominant company's data set simply to target its own customers with more efficient advertisement or to draw more new customers. These activities are not in any way innovative and are a form of free-riding. This raises the issue of how the regulators and courts can truly differentiate claims for access from genuine innovative

[212] Ibid, para. 557.
[213] Koponen, Jonas – Mangiaracina, Annamaria, 2013 ''No Free Lunch: Personal Data and Privacy in EU Competition Law''. In *Competition Law International*, Vol. 9(2), p. 189.
[214] Autorité de la Concurrence and Bundeskartellamt (2016), p. 18.
[215] Graef (2015), pp. 494-495.
[216] Lambrecht – Tucker (2015), p. 12.

motivations and free riding as it is possible that a company attempts to hide its true intentions. Therefore the new product or innovation should be assessed with utmost care and should not be assumed too readily.

O'Donoghue and Padilla argue that a sensible approach would be to have the party requesting access to the facility to provide its plans on new product, the product should actually be a new kind of product for which there exists a consumer demand and which meets the needs of consumers in ways the old product did not.[217] This would arguably place the burden on the party seeking access to competitors' data set to demonstrate how this access would support in the creation of a new product or follow-on innovation. As a result groundless claims for access can be recognized and dealt with early on.

5.4 Concluding remarks on whether data can be held to amount to an essential facility

Big data could amount to an essential facility in very limited circumstances. Such circumstances are present when in order to function in a market, a company would have to have a data mass so wide and large that no alternatives to it are available.[218]

The Franco-German competition report points out that the ECJ has in *Bronner*, *IMS Health* and *Microsoft* limited the applicability and scope of the essential facility doctrine. Basically an undertaking can request access to a facility or where the dominant company refuses to grant access to a product which is indispensable for carrying on the business, if as a result of the refusal, the emergence of a new product for which there is a potential consumer demand is prevented (this condition being applicable to intellectual property rights), if it is not justified by objective considerations and if it is likely to exclude all competition in the secondary market. Furthermore, in *Bronner*, the ECJ ruled that a product is indispensable only if there are no alternative products and there are technical, legal or economic obstacles that make it impossible or unreasonably difficult for any company wanting to operate on the downstream market to develop, possibly in cooperation with other companies, products or services. These requirements will only be satisfied if it is demonstrated that the data owned by the dominant company is truly unique and that there is no possibility for the competitor to obtain the data that it needs to perform its services. An important point is that a more

[217] O'Donoghue – Padilla (2006), p. 447.
[218] Warma – Nieminen (2016), p. 565.

liberal data access regime may also lessen incentives for competitors to develop their own sources of data. Finally, forced access to data may raise privacy concerns as forced sharing of user data could violate privacy laws if companies exchange data without their consumers' consent.[219] The privacy concerns arising from the forced sharing of data will be discussed below.

[219] Autorité de la Concurrence and Bundeskartellamt (2016), pp. 17-18.

6. Application of the essential facilities doctrine in relation to big data

6.1 Forced sharing of data as a remedy under competition law and the GDPR

As has been described above, under certain circumstances, a dominant company can be forced to share its facility with a competitor. The remedy of forced sharing is however not the only type of remedy under competition law. Indeed the Commission has the power to impose a fine of up to 10% of the company's total turnover under certain conditions.[220] The EU data privacy laws do not contain structural remedies in comparison to EU competition law.[221] This is understandable as structural remedies do not as such play such a role in the processing of data by companies as opposed to the role they play in regulating how companies conduct business and compete. Stucke and Grunes say that despite the fact that fines available under both EU competition law and GDPR, competition law remedies are superior to data privacy remedies in controlling monopolies.[222] It is true that forced sharing of a data set is more efficient remedy than fining a company as the company could simply pay the fine and continue to refuse access. The GDRP provides for a different solution for the sharing of data between companies in the form of data portability contained in article 20 of the GDPR. According to this article, the data subject has the right to receive his personal data in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller if certain conditions are satisfied (these will be discussed below).

The remedy that competition law provides in the form of forced sharing of data has implications on the data privacy of the users whose personal data is being transferred from the dominant company to another company. On the other hand the concept of data portability is essentially designed to strengthen the control of the data subject over his or her own data[223] and not to maintain or improve the competitive situation. The implications of forced sharing and data portability will be discussed in the next part. The company subject to a forced sharing remedy could in theory invoke certain measures in order to avoid sharing the personal

[220] Commission ''Fines for breaking EU Competition Law''. Available at <http://ec.europa.eu/competition/cartels/overview/factsheet_fines_en.pdf> (accessed 20 March 2018).
[221] Stucke – Grunes (2016), p. 255.
[222] Ibid, pp. 254-255.
[223] GDPR recital 68.

data of its users. According to the ECJ[224], the protection of fundamental rights is a legitimate interest which, in principle, justifies a restriction of the obligations arising from Community law, including the fundamental freedoms contained in the Treaty. Therefore in principle a company could argue that the refusal to share its data would be justified by the fundamental freedoms of the citizens in relation to the protection of their privacy contained in various EU legal instruments. For instance under the Charter of Fundamental Rights of the European Union, everyone has the right to the protection of personal data concerning him or her.[225] As has been stated earlier in this thesis, the purpose of data privacy regulation is to secure the protection of privacy and other fundamental rights and therefore a company could in theory base its refusal to share data containing personal data based on this fundamental right of protection of privacy. Even the data portability right is not absolute as the GDPR provides that the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.[226] Therefore the technical limits could release the company from providing the data portability. The various aspects of both forms of data sharing will be discussed next.

6.2 Administrative problems of forced sharing of data under competition law

The remedy of forced sharing requires some form of intervention by the courts in the form of a judgment as otherwise the parties would have simply reached an agreement on the sharing of the data and no court intervention would have been required. Administrability problems concern the management of the access.[227] It has been argued that courts are able to administer access to data more easily than access to physical facilities.[228] Antitrust remedies in the form of essential facilities usually require the court to engage in supervision as simply forcing the monopolist to share the facility might not suffice in terms of for instance ensuring reasonable access price.[229]

[224] Judgment of the Court (First Chamber) of 14 October 2004. *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*. Case C-36/02 Omega, ECLI:EU:C:2004:614, para. 35.Para. 35.
[225] Article 8 of the Charter of Fundamental Rights of the European Union.
[226] Article 20(2) of the GDPR.
[227] Ezrachi – Maggiolino (2012), p. 612.
[228] Abrahamson (2014), p. 872.
[229] Choi (2010), p. 77.

One particular difficulty surrounding the forced sharing of data is that there is no single way to define the access terms for data. The OECD for instance has concluded that when it comes to the value of personal data, there is no single, perfect measure for it.[230] Abrahamson points out that critics of the essential facilities doctrine argue that the courts are not necessarily capable of identifying and remedying refusals to deal.[231] Abrahamson points out that the costs of sharing the data are likely near zero and as a result there is no need for judicial inquiry into the special characteristics of the industry or exact estimations necessary to determine the costs of sharing.[232] Piraino argues that the courts could make a rather general order stating that the monopolist make available its essential facility in a nondiscriminatory manner to its competitors instead of specifying the precise terms of access.[233]

Choi argues that competition authorities do not have the necessary information and expertise to determine the optimal level of the access price especially due to the changing environment of dynamic industries. According to Choi, the application of essential facilities doctrine for promoting ex post static efficiency has the negative consequence of decreasing ex ante investment incentives, which can lead to a serious loss of dynamic efficiency.[234] As has been described earlier about the nature of data, there are considerable variations on the use of data and on the value of data for companies. In addition the exact nature of how the companies use data is context dependent and thus difficult for courts or administrators to define in terms of access remedies. It is completely different thing from the point of view of supervision and oversight to force a company to share its physical facility than its intangible data assets. Furthermore the access should in theory be continuous as due to the fast moving nature of data, historical data is of little significance. One could argue that in relation to physical infrastructure the access is also continuous as the competitor in normal cases would be granted access more than once. However the physical infrastructure remains the same unlike the data set that is continuously altered by the dominant company. Furthermore, is impossible to define the exact point when the data set is no longer the one that the court initially held to be essential for the other company. It is akin to saying that instead of a full cinematic piece, a company would only acquire one screen shot of the film. Big data just does not function that way in real life. Thus there exist considerable obstacles to the administrability of the access

[230] OECD Digital Economy Papers (2013), p. 19.
[231] Zachary Abrahamson, Zachary ''Essential Data'' In *Yale Law Journal*, Vol. 124, 2014, p. 872.
[232] Abrahamson (2014), pp. 877-878.
[233] Piraino (2000), p. 883.
[234] Choi (2010), p. 77.

remedy rendering it questionable whether this type of remedy is suitable to deal with the possible issues arising from the accumulation of data by dominant companies.

Finally forced sharing can decrease legal certainty since the limits of the essential facilities doctrine are not clear.[235] Therefore at the level of legal rules, the doctrine of essential facilities introduces legal uncertainty for companies utilizing big data in their operation. Furthermore even at the level of the remedy itself, namely forced sharing of the data, there are legal uncertainty related factors present. Hellstrom, Maier-Rigaud and Wenzel Bulst point out that a Commission decision has to be in accordance with the principle of legal certainty meaning that it must be clear and precise so that companies subject to such decisions know their rights and obligations and can act accordingly.[236] The requirement that the decision to impose a duty to share access to data has to be clear and precise can turn out to be difficult to attain as the nature of big data itself imposes challenges on making precise definitions on the nature of the data and how access should be provided.

6.3 Harmful effects on innovation from forced sharing of data

In addition to the practical difficulties arising from forced sharing of data, there are also possible concerns arising in the form of decreased incentives for companies as there would be no reason for companies to invest in the big data asset in the first place if they were not allowed to benefit from their investment due to being forced to share this data set with a competitor. As a result companies might seek to use aggregated data and invest less on the data related analysis. Such a scenario will lead to consumers not benefiting from lower costs, new products and better quality.[237] If competition law is to intervene on the process of a company choosing its trading partners, such an intervention requires careful consideration where the application of Article 102 would lead to the imposition of an obligation to supply on the dominant undertaking. The Commission has noted that the existence of such an obligation may make it less desirable for the undertakings' to invest and innovate and, thereby, can cause consumer harm even if fair remuneration is offered to the dominant company.[238]

[235] Graef (2011), p. 18.
[236] Hellstrom – Maier-Rigard – Wenzel (2009), p. 51.
[237] Motta (2008), p. 39.
[238] DG Competition discussion paper (2005), para. 75.

Arguably collecting and analyzing data sets requires costs and is time consuming and companies' incentives to embark on such procedures would be diminished if their data sets were subject to forced sharing.

In certain specific cases, the Commission considers that it may be clear that imposing an obligation to supply is not capable of having negative effects on the dominant company's incentives to invest and innovate upstream. This is particularly likely to be the case where a regulation already imposes an obligation to supply on the dominant undertaking and the necessary balancing of incentives has already been made by the public authority before imposing a duty to supply. This is also the case where the upstream market position of the dominant undertaking has been developed under the protection of special or exclusive rights or has been supported by the state financially.[239] It is quite likely however, that companies that use big data in their business have not done so by the special protection of the state or similar circumstances.

Furthermore, it is not universally accepted that forced sharing of a facility will automatically decrease incentives to invest and innovate. Ideally there should be some sort of a tradeoff between the ex-ante efficiency (the preservation of companies' interests to invest) and ex-post efficiency (after a company has innovated, all companies should have access to the innovation).[240] Stothers is of the view that the argument that access to the product or service will reduce the future incentive to create essential facilities is highly misleading. He argues that access only stops the dominant undertaking from charging monopoly prices and so long as access is paid for at a competitive market rate, normal incentives exist to create the facility[241]. However, even a monopoly can result in less innovation as the company has less incentives to adopt the most efficient technologies.[242] On the other hand effective competition will cause the inefficient firms to exit and allow the efficient ones to remain[243]. Therefore the most suitable level for innovations and productive efficiency might lie in the intermediate level of competition.[244]

[239] Ibid, para 82.
[240] Motta (2008), p. 65.
[241] Stothers (2001), p. 260
[242] Motta (2008), 47-48.
[243] Ibid, p. 50.
[244] Ibid, p. 57.

This type of balancing exercise is demonstrated by the Commission's Microsoft decision[245], where the Commission embarked on a balancing exercise and held that the possible negative impact of an order to supply on Microsoft's incentives to innovate was outweighed by the positive impact that the supply will have on the level of innovation for the entire industry in question.[246] Ezrachi and Maggiolino argue that dominant undertaking not protected by network effects face ongoing challenges caused by possible new entries and as a result are likely to engage in innovation in order to maintain their market position. However it is the perception of over-enforcement that might chill innovation.[247] Sokol & Comerford say that smaller companies will maintain the incentive and ability to compete if smaller companies are well funded and have innovative products that cause consumers and advertisers to switch from larger companies.[248] Smaller companies might even have larger incentives to invest in quality as they have more users to gain than the larger company with an existing large amount of users.[249] Therefore the nature of the market is crucial factor and forced sharing might be more suitable where there are substantial entry barriers.

The specific nature of data has to be taken into consideration here too. As Graef points out, the IT sector is not similar from other sectors in the economy as there exist very high entry barriers due to network effects, switching costs and economies of scale. According to Graef, due to the dynamic nature of the IT sector, compulsory licenses do not necessarily have a negative effect on innovation.[250] However, big data is used in other sectors besides the IT sector and as a result it cannot be categorically stated that all markets in the sectors with big data have these features.

Especially the fast moving nature of big data makes it difficult to justify why a company cannot simply continue collecting and analyzing data despite having to share its data set with a competitor if the company is capable of maintaining its user base by offering superior services. Again it is also crucial to note that the data itself is not the end product in these cases. To take a more traditional example, a company operating train service on its train

[245] Case COMP/C-3/37.792 *Microsoft* Decision of 24 March 2004.
[246] Ibid, para. 783.
[247] Ezrachi – Maggiolino (2012), p. 610.
[248] Sokol – Comerford (2016), p. 1150.
[249] Ibid, pp. 1150-1151.
[250] Graef (2011), p. 2.

tracks would find it difficult to argue that it would not have built the tracks if another company could use the tracks for it is the quality of the train service that the companies should be competing, not the infrastructure itself. On the other hand it is always possible to counter these arguments by saying that if data is so easy to obtain and analyze, then the smaller rivals could access this data by offering superior services themselves without having to obtain the data set from competitors. At least some form of free riding could possibly result in the forced sharing of data which is bound to have a negative influence on the overall attitude of market players. As a result the forced sharing of data is likely to raise at least some concerns over the incentives for the companies subject to such an obligation to innovate and invest. However, a case-by-case analysis is necessary before one concludes that this is the case.

7. The privacy implication arising from forced sharing of data

7.1 The legal framework surrounding personal data in the EU

This part of the thesis will focus on the privacy of personal data. The reason for this is that users' data can and often does contain their person data. As has been discussed above, the dominant company could, under certain circumstances, be forced to share this data set under the essential facilities doctrine (in this case its data set comprising the personal data of its users) to its competitors. It is therefore necessary to consider how this is dealt with by the laws that govern data privacy at the EU level and what implications this might have on the sharing of these types of data sets.

To begin with, the individuals whose data is being collected are often unaware of the processing of their data as the collection of big data is based on so many different and sources which can be unexpected to them.[251] Competition law involvement through forced sharing of the data can create privacy related concerns as the users in most cases have not consented to the sharing of their data to other parties and to the possible other uses made by those parties of the data.[252] This means that the starting point on the sharing of user data between companies is problematic from the perspective of transparency as the users might not even realize that their data is shared.

The EU adopted the General Data Protection Regulation (''GDPR'') in 2016. The GDPR replaces the Data Protection Directive and its application will commence on the 25th of May 2018.[253] The GDPR acknowledges that the fast moving technological developments and globalisation have brought with them new challenges to data protection as the scale of the collection and sharing of personal data has been increased significantly by the technological development. Furthermore people increasingly make personal information available publicly.[254] The GDPR has certain key principles such as the transparency principle according to which the processing of peoples' personal data should be transparent. The principle of transparency requires information concerning the processing to be easily accessible and easy

[251] ENISA (2015), p. 13.
[252] Sokol – Comerford (2016), p. 1159.
[253] European Data Protection Supervisor ''The History of the General Data Protection Regulation''. Available at <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> (accessed 20 March 2018).
[254] GDPR recital 6.

to understand.[255] It is particularly important to inform the data subject on the identity of the controller[256] and the purposes of the processing of the data.[257] Furthermore, data protection laws allow data subjects to enforce a remedy in courts and entitling them to compensation in cases of violations of privacy.[258]

Data privacy laws are enforced at national level by the national authorities and at the EU level by the European Data Protection Supervisor (the "EDPS"). The EDPS is entitled to carry out investigations and can issue warnings or order that the controller complies with the requests of the data subjects concerning their rights under the data privacy, order the rectification, blocking, erasure or destruction of data and impose a ban on processing of data.[259]

The GDPR contains provisions on the lawfulness of processing of personal data. The most relevant provisions concerning the lawful basis of processing of personal data for the purposes of this topic are:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) the processing is necessary for the performance of a contract concerning the data subject;
c) the processing is necessary for compliance with a legal obligation to which the controller is subject;
d) the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.[260]

[255] GDPR recital 39.
[256] According to article 4 of the GDPR, controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the why and how data is collected.
[257] GDPR recital 39.
[258] Kuschewsky – Geradin (2013), p. 7.
[259] Ibid, p. 8.
[260] GDPR Article 6.

The GDPR provides that the data has to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[261]. In addition to having a lawful basis on processing, companies must inform the data subject of the recipients of their data i.e. who will receive the data.[262]

Based on the above considerations it is clear that the processing of personal data is heavily regulated in the EU under the GDPR and companies are not able to process data without having regard to the requirements of the GDPR.

7.2 What type of data amounts to personal data

Not all type of information qualifies as personal data and fall under the GDPR. According to the GDPR, personal data encompasses any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[263] This provision demonstrates how wide ranging the definition of personal data under the GDPR is.

Even information such as an individual's search history is personal data if the individual to which it relates, is identifiable. Though IP addresses in most cases are not directly identifiable through the use of search engines, identification is possible by a third party. Internet access providers have IP address related data at their possession. As a result, in most cases the data can be used to identify the user of the IP address.[264]

It can be argued that the data sets of companies' that contain user data will almost certainly contain personal data as defined under the provisions of the GDPR. As a result the GDPR is applicable to the processing of this data.

[261] GDPR Article 5 1(b).
[262] See for instance GDPR Articles 13, 14 and 30 on the information duties of the controller.
[263] GDPR art. 4.
[264] WP 29 (2008), p. 8.

7.3 The lawful basis under the GDPR for the sharing of personal data contained in data sets under the essential facilities doctrine

The objectives of competition law and data privacy do not always co-exist in harmony as Warma and Nieminen point out that there could be a situation in which a dominant company violates either the data privacy laws by sharing its data containing personal data or competition law by refusing to share such data to a competitor.[265] This part of the thesis will analyze whether the forced sharing of personal data contained in the data sets of a company is possible under the GDPR. For the purposes of this essay it is assumed that the recipient companies are private companies and will use the data sets containing personal data for business purposes. The purpose of this part of the thesis is to demonstrate that despite the fact that there is a court ordered remedy forcing the dominant company to share its data set to a competitor, the GDPR will place additional requirements for the company to justify the processing of personal data in the form of transferring said data to the competitor.

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes

According to the GDPR, consent should be freely given. Furthermore in order for the consent to be informed, it is necessary that the data subject is being informed of certain aspects such as the controller's identity and the purpose of each of the processing operations for which the consent of the data subject is being sought.[266] These facts highlight the importance of informing the users on how their personal data will be processed and by whom.

Taking into consideration the strict criteria for valid consent for processing of personal data, it seems unlikely that this basis is feasible for justifying the processing of the data subject's personal information as the dominant company would have to acquire consent from all of the data subjects whose personal data it would transfer to its competitor. Furthermore due to the strict information requirements it is not possible to acquire the consent in advance for possible future purposes contained in the further processing by the recipient of the data.

[265] Warma – Nieminen (2016), p. 550.
[266] WP 29 (2016), p. 13.

b) The processing is necessary for the performance of a contract concerning the data subject

A processor can rely on the lawful basis of contract where the processor has to process personal data in order to fulfil the processor's contractual obligation to a person or where a person has asked the processor to complete a task before entering a contract. The processing should be necessary, meaning that there are no other ways to achieve the aims of the person.[267] This legal basis seems unlikely to apply to a situation where a company shares its data set to another company as it is difficult to see where a contract between the data subject and the dominant company would require the sharing of data based on the request of another company. As a result this basis is unlikely to be applicable for the present purposes.

c) The processing is necessary for compliance with a legal obligation to which the controller is subject

The GDPR also contains a provision which allows processors to process personal data based on legal obligation to do so. Article 6(3) of the GDPR requires that the legal obligation must be laid down by national or EU law. The obligation does not have to be in the form of an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it.[268] The jurisprudence of the ECJ can form a sufficient legal basis too. There does not have to be an explicit legal provision providing for the activity, but the legal obligation has to have a sufficiently clear basis in either common law or statute. A court order requiring the processing of personal data for a particular purpose qualifies for legal obligation as well as regulatory requirements where there is a statutory basis for the regulatory regime and the organisations must comply with this obligation. One example of this could be a national authority having authority to remedy adverse effects on competition by way of forced disclosure of data.[269] Furthermore in order to comply with a legal obligation, companies subject to such obligation can process personal data if it is necessary. For instance

[267] Information Commissioner's Office ''Guide to the General Data Protection Regulation''. Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/> (accessed 21 March 2018).
[268] Recital 41 of the GDPR.
[269] Information Commissioner's Office ''Guide to the General Data Protection Regulation''. Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation//> (accessed 21 March 2018).

where documents in the possession of the company have to be produced in response to a mandatory request for information or a court order.[270]

The legal obligation basis relies on the regulator's or court's orders and is a more secure basis than legitimate interest which requires the balancing of interests. Furthermore the legal obligation basis seems applicable as even though there are no explicit provisions in the TFEU concerning the sharing of personal data in abuse of dominance situations, such an obligation can be inferred from art. 102 TFEU and through the case law of the ECJ concerning essential facilities. What this basically means is that the legal basis to transfer the data to the competitor would be based on article 102 TFEU that lays down the basis for the sanctioning of abuse of dominance. Furthermore Regulation 1/2003 contains the provisions for the structural remedies including forced sharing of facilities such as data. Finally the case law of the EU Courts and particularly the essential facilities doctrine form the legal basis for the transfer of the personal data in cases of forced sharing. However, this interpretation is quite broad as there is not a clear piece of legislation enabling companies to transfer data on the basis of a dominant position. Therefore whether the legal obligation basis is applicable depends on whether the regulators and courts adopt a broad or narrow interpretation of the meaning of legal basis in this context. Naturally it would be preferable for legal certainty if there would be more express legal provision for this sort of disclosure.

d) The processing is necessary in order to protect the vital interests of the data subject or of another natural person

The vital interest covers processing that is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.[271] This legal basis seems unlikely to apply to user data in relation to business purposes as the data for the purposes of commercial activities is unlikely to concern the vital interests of the data subjects.

e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

[270] Kuschewsky – Geradin (2013), p. 12.
[271] The GDPR recital 46.

This basis will apply if the data is being processed in relation to either carrying out a specific task in the public interest which is laid down by law or in the exercise of official authority. The processing has to be necessary in the sense that the processing must be a targeted and proportionate way to achieve the aimed purpose.[272] It is unlikely that companies using their users' personal data in for business purposes could rely on this basis as they are private businesses instead of public authorities.

f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

Legitimate interests require that the personal data is used in ways that people would reasonably expect with minimal privacy impact, or where there is a compelling justification for the processing. Commercial interests of a company can be part of legitimate interest. The processing must be necessary with no other less intrusive ways available. It is also possible to justify processing in the form of lawfully disclosing personal data to a third party. In this case the party disclosing the information should consider why the other party wants the information, does the other party actually need it, and what the other party will do with it. The disclosing party has to demonstrate that the disclosure is justified and the receiving party has to determine their lawful basis for their own processing.[273] As a result the legitimate interest basis is applicable to processing even before a possible court decision to transfer the data has been made. However, in this case the dominant company transferring the data should be very cautious in balancing its own interests and the interests of the data subject.

Conclusions on the legal basis for the processing of personal data

The only feasible legal basis for the sharing of personal data seems to be limited to the legal obligation or the legitimate interest. However the problem with the legal obligation is that it

[272] Information Commissioner's Office ''Guide to the General Data Protection Regulation''. Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/ > (accessed 21 March 2018).
[273] Ibid.

is uncertain whether there will be a broad enough interpretation by the regulators and courts should the processing come under question. For the basis of legitimate interest, the biggest obstacle lies in the fact that the interests of the data subject should be balanced against the interests of the dominant company and in particular it is questionable whether the data subject could have expected his or her data to be shared in such a manner when providing the data to the dominant company in the first place.

As a conclusion on the lawful basis for processing it can be said that the GDPR does not automatically prohibit the disclosure of personal data to competitors, however the legal bases available are limited and should be assessed on a case-by-case basis in order to ensure that the processing complies with the data privacy laws. In any case simply transferring a data set containing personal data to competitors following negotiations or a remedy imposed by a court would place the transferring company in risk of violating the GDPR and incurring a substantial fine[274] as a result.

7.4 Purpose limits to the reuse of personal data

In addition to the legal bases for the processing of personal data described above, personal data can only be processed for new purposes if the controller asks for the data subject's consent.[275] The data reuse activities that might happen in the future can be described and communicated to the data subject before the collection of his personal or the data subject may be asked to renew his consent each time his personal data is used for a new purpose.[276] However, according to Ursic and Custers it may challenging to predict all the purposes for data reuse that may arise in the future and it may be nearly impossible to contact all data subjects and to secure their valid consent. The idea behind conveying adequate information to an individual is not only to comply with the fairness of processing but also enable the data subject to invoke his core rights such as right to access, erase and object.[277] Stucke and

[274] The GDPR provides for two levels of fines in article 83. The first category provides for administrative fines up to 10 000 000 euros, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The second and more severe category provides for administrative fines up to 20 000 000 euros, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The failure to comply with the requirement of lawful basis falls under the second category of fines.
[275] Article 29 Data Protection Working Party17/EN WP259 Guidelines on Consent under Regulation 2016/679 p. 12.
[276] Ursic (2016), p. 212.
[277] Ibid, p. 213.

Grunes point out that consumers often are unaware of the party who has access to their personal information, what data is actually being utilized, how and when such utilization is taking place and finally on the entire

7.5 Possible solutions to avoid data privacy rules in relation to sharing of personal data

As has been demonstrated above, there is an inherent tension between the sharing of data from the procompetitive perspective and the protection of the privacy of personal data. There are however situations where the data might not fall under the provisions of the GDPR. The principles of data protection apply only to information concerning an identified or identifiable natural person. The principles of data protection on the other hand do not apply to anonymous information, which means information which does not relate to an identified or identifiable natural person or to personal data made anonymous so that the data subject can no longer be identified.[278] Anonymisation can be used by companies to comply with the data protection obligations and also make it possible for companies to share information with the public. In general, it is easier to disclose anonymised data than personal data as there are less legal restrictions to this. It is also easier to use anonymised data in different ways as the data can be then used for different purposes.[279] According to the Finnish Data Ombudsman, the anonymisation of personal data refers to the technical and other measures through which personal data is irrevocably altered into such a form that the data subject cannot be directly or indirectly identified from them by anyone. The anonymization is a form of processing of data. The processor has to evaluate the anonymity of the data at certain intervals even after the data has been anonymized. Even if the processor is of the view that the data is anonymized, it could happen that a third party is nonetheless able to identify the person by using techniques or otherwise process the data in a manner that enables the identification.[280]

Not all measures aimed at making the personal data less identifiable amount to anonymization. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. However such additional information have to be kept separately and be

[278] Recital 26 of the GDPR.
[279] Information Commissioner's Office ''Anonymisation: managing data protection risk code of practice''. Available at <https://ico.org.uk/media/1061/anonymisation-code.pdf> (accessed 21 March 2018), p. 12.
[280] The Finnish Data Protection Ombudsman (2015).

subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[281] Recital 26 of GDPR provides that in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person to identify the person directly or indirectly. In order to define whether means are reasonably likely to be used to identify the person, factors such as the costs of and the amount of time required for identification should be considered, taking into consideration the available technology at the time of the processing and technological developments should be considered.

However while anonymization might be useful in avoiding the applicability of the GDPR, it has other problems for companies. Namely as Stalla-Bourdillon and Knight point out, the fact that the value of datasets is maximized when patterns are discovered and linking relationships between data points and anonymization delinks relationships that can be discovered about peoples' identities. The question for companies surrounding anonymization is therefore, how can the companies embark on data anonymization and still retain the utility of the data for a future third party with whom the data is shared subsequently?[282] In addition, there is the problem with defining the value of the data set to the competitor if it has been anonymized only after the court has ordered the sharing of said data. Where completely anonymized data is processed for business purposes and transferred between companies, then there are no foreseeable problems with the GDPR. In any case companies should not assume that by simply removing certain features of the data sets, the data would automatically be rendered anonymous and thus outside the scope of the GDPR.

7.5.1 The forced sharing of data under the GDPR in the form of data portability

As has been discussed above, the GDPR offers an alternative approach to the sharing of user data (provided this data is personal data within the meaning of the GDPR), namely the data portability. Indeed data portability can prevent abuse of dominance and consumers from being locked into services. Also data portability could make it easier for consumers to benefit from value-added services from third parties and creating more access to the market for other companies.[283] The EDPS is of the opinion that remedies should be subject to strict conditions

[281] Article 4 of the GDPR.
[282] Stalla-Bourdillon – Knight (2016), p. 285.
[283] EDPS (2014) para. 83.

and safeguards following the principle of data minimization, which holds that only strictly necessary personal information should be processed. The EDPS has suggested that data portability should be implemented by way of giving the users an opportunity to withdraw their personal information and to transfer it to another company, which would benefit the competitive market structure.[284] Data portability could release synergies between competition law and data protection law by preventing abuse of dominance and empower consumers to benefit from other companies' services while making it easier for access to the market by competitors.[285] However, Stucke and Grunes point out that data portability could reduce incentives for the companies forced to hand over their users' data to conduct business. On the other hand, it should be borne in mind that the users' 'own' their personal data.[286]

The use of data portability is however limited as it applies only to situations where the processing is based on consent or on a contract and the processing is carried out by automated means.[287] Nonetheless the processing of personal data for the purposes of user data among companies seems to fit quite perfectly for the above requirements as the initial processing is often based on the user's consent or on the contract (for instance contract for service or goods) between the user and the company. In addition the collection and analysis of big data in most cases require automated processing. It could be said then that there are no legal obstacles in the application of the data portability to the personal data processed as part of a data set of a company.

Companies might be sanctioned under the GDPR if they refuse to allow their customers to port their data to another company.[288] However, restrictions on data portability can probably only be justified by technical difficulties.[289] Furthermore there seems to be consensus at the Commission level on the need to promote the sharing of data as the Commission is of the view that in order to facilitate exploitation and reduce transaction costs there should be less restrictions and more harmonised rules on data re-use.[290]

[284] Ibid, para. 72.
[285] Ibid, para. 83.
[286] Stucke – Grunes (2016), p. 332.
[287] GDPR Art. 20 1(b).
[288] See article 83 of the GDPR for the setting of fines.
[289] Geradin – Kuschewsky (2013), p. 11.
[290] Communication from the Commission (2014), p. 5.

An interesting example of data portability related issues related to Google. In March 2013, the Commission formally informed Google of its preliminary conclusion[291] that certain business practices by Google may violate EU antitrust rules prohibiting the abuse of a dominant position. Among the concerns of the Commission were the contractual restrictions on the transferability of online search advertising campaigns to search advertising platforms maintained by Google's rivals and the management of such campaigns across Google's Adwords and rival search advertising platforms. Vanberg and Bilal Ünver are of the opinion that the Google case demonstrates the importance of data portability in order to avoid consumer lock-in in concentrated markets. They argue that Google has in its possession a vast amount of personal data allowing it to deliver relevant and high quality search results. Thus Google prevents other search engines from effectively competing with it by not sharing this data with its competitors.[292]

Data portability has not been welcomed without criticism. Kallasvuo points out that the right to portability can be criticized for its ambiguous wording as the GDPR does not clarify the situations in which the portability is technically possible. Kallasvuo argues that the wording of the GPDR does not seem to require that the controller has to alter the data in such a form that allows the data subject to port his or her data to another system. On the other hand, Article 18 of the GDPR can also be interpreted as precluding the processor from willfully hindering the portability from one system to another. This view is supported by the fact that the processor is under a duty to facilitate the fulfilment of the data subjects' rights under Article 12 paragraph 1a of the GDPR.[293]

However, consumers need to be aware of other service providers in order to be able to port their data to them in the first place. The EDPS is of the view that when consumers are better informed, they should be more capable to choose between competing online services.[294] It is thus clear that in order for the data portability to function properly, the principle of transparency is of utmost importance. It seems that not all of the consumers are aware of the GDPR and the related rights. For instance only 29% of the Finnish consumers had even

[291] European Commission ''Commission seeks feedback on commitments offered by Google to address competition concerns''. 2014, Available at <http://europa.eu/rapid/press-release_IP-13-371_en.htm> (accessed 23 March 2018).
[292] Diker – Ünver (2017).
[293] Kallasvuo (2015), p. 154.
[294] EDPS (2014), para. 82.

heard of the GDPR. Of those who are aware of the GDPR, only 9% will use the right to access to their personal data. However the amount of consumers who will seek access to the personal data stored by social media services is 33%, which signals that consumers are more concerned about the data that social media companies store of them.[295]

Users might be aware of the company to whom the users first gave their personal information, however the users most likely are not aware of the subsequent recipient companies that process their information. Even if companies offered transparent information about the recipients of the personal data, it is questionable whether the users would in fact read these statements.

As a result the data portability is dependent first on the users being informed, and second that the users actually understand where their personal data is being transferred. Finally the users have to actually be willing to request their data to be transferred.

7.6 Concluding remarks on court ordered forced sharing and data portability

Both the court ordered remedy under the essential facilities doctrine and the data portability under the GDPR result in the personal data of the user being transferred between the initial data processor (the dominant company for the purposes of this thesis). There are nonetheless various differences between these two measures. First of all the data portability applies to companies regardless of their size, whereas the forced sharing remedy is applicable to dominant companies within the meaning of EU competition law. Another key difference is the fact that it is the user (data subject) who initiates the transfer of his or her data under the data portability right envisaged in the GDPR, whereas the competition law remedy of forced sharing is the result of a regulator or court based finding of an abuse of dominance and the users whose personal data is involved are not the parties to these proceedings albeit they certainly are an important stakeholder group. On the procedural side, the competition law remedy requires the finding of a dominant position which might be a lengthy process with both the regulator investigating and the parties appealing to the Courts. On the other hand the data portability right is a mere technical process albeit it has its implications on the companies having to be able to carry out the transfer of the data in the required format.

[295] Metsämäki (2017).

The court ordered sharing poses privacy concerns and requires careful analysis of the justifications for the processing of personal data as has been described above. Data portability is only possible where the users truly wish to transfer their data to competitor, thus it means that the companies should seek to offer better services and products in order to have the consumer port their data to them. On the other hand there are various obstacles to data portability, for instance the information problems associated with the lack of transparency of the data processing.

Finally forced sharing ordered by the court and the data portability both contain unclear parts which raise legal certainty problems for companies. Both can also act to reduce the incentives for companies to innovate and invest. However, it seems that for the data portability the case is not that strong as consumers in fact own their personal data and are free to make the decision on whom to transfer the data.

Warma and Nieminen are of the opinion that transferring the data of each individual at a time is not a satisfactory solution from the view point of competition compared to the transfer of large data masses.[296] Indeed this is a strong argument as the sharing of data based on data portability only concerns the data of a single individual and not a data set itself. Furthermore, the problems associated with data portability mentioned above limit the usability of data portability.

[296] Warma – Nieminen (2016), p. 558.

8. Conclusions

This thesis has analysed the implications arising from the accumulation of large datasets with personal information from the point of view of competition law and data privacy regulations. The main question of this thesis was whether big data containing personal information can be regarded as an essential facility under the competition law. As a result of the analysis, it can be concluded that big data as a non-tangible asset cannot be compared with traditional infrastructure such as power lines or railroads. Despite this fact, the accumulation of big data can in practice increase the market power and be used to exclude companies from the market.

The essential facility doctrine focuses on the indispensability of the facility and whether the facility will be used to introduce a new product to the market or follow-on innovation. No clear conclusion can be made whether big data amounts to an indispensable facility without which companies could not compete. The reasons for this are multifold among them the fact that big data in most cases is non-rivalrous meaning that it is possible for companies to acquire the same set of data from the users despite the fact that a company already possess that data. However, this is not always the case as some types of data can be rivalrous, such as data that goes out of date quickly or data that is highly personalized. As a result, regulators and courts should take a case-by-case approach. Furthermore it might not be feasible for companies to acquire a certain data set from third parties despite the fact that there are data brokers selling certain data to companies. Especially in consumer markets, the accumulation of data can cause a snowball effect with the dominant company being able to improve its services by the use of the user data and attract even more users as a result. For the new product requirement it is challenging for companies seeking access to data to demonstrate what they will in fact do with the data and what type of new product or innovation they will introduce instead of simply using the data to improve their marketing.

On a more fundamental basis, compelling companies to share their data assets could reduce their incentives to innovate and invest and as a result the benefits of big data would not be realized. Indeed the role of competition law is not to assist inefficient market entrants wishing to gain the assets of more efficient companies. Another harm arising from forced sharing

of big data concerns the administrability problem associated with the remedy of forced sharing. Especially the problem of quantifying a fair remuneration and access terms to the data raise obstacles to the use of the access remedy.

The structure of the market plays a crucial part in the analysis of whether big data can result in dominance and become an essential facility. This thesis has brought forward the idea that competition law should only intervene in situations where the data asset forms a genuine barrier to entry such as where there are network effects and locked in consumers or the data set is truly unique and cannot be copied under any circumstances. While this is no doubt challenging for the regulators and courts to do, it is no reason why it should not be done.

In cases of traditional facilities such as railroads and powerlines, there are no other stakeholders with their personal data being transferred as is the case with the sharing of big data containing the data of the users. While competition law regime is concerned with well-functioning competition and consumer welfare, the aim of data privacy regulations including the GDPR is the protection of personal data. Forced sharing of data can thus serve the goals of competition law by enabling well-functioning competition but at the same time collide with data privacy regulations by making the personal data of the users' subject to the processing by the recipient company without a legal basis contained in the GDPR. In some cases there can be a legal basis for the processing of the personal data by the recipient company for instance when the sharing is based on the court ordered remedy and on the broad interpretation of the legal basis of legal obligation. However even if there is a legal basis for the processing of the information, the data subject should be informed of the sharing of the data according to the GDPR. In practice, this could turn out to be a heavy burden on companies and even impossible as companies cannot be aware of possible future requests to share data with competitors. Furthermore if the purpose for which the data was originally collected and processed changes, then consent should be acquired from the data subjects, which can be truly challenging.

An alternative approach to the data sharing is the data portability right contained in the GDPR. This right allows for the data subjects to ask for the company to transfer the user's personal data to a competitor under certain circumstances. However this right is only applicable under limited circumstances, such as where the data is processed in order to fulfil a

contract between the data subject and the company. Besides this right differs from the competition law remedy of forced sharing in that the data portability is dependent on the will and activity of the data subjects whereas the competition law remedy of forced sharing is dependent on the ruling of the court or the decision of the regulator. The personal data of a single user is in addition not nearly as useful for companies as full data sets made available through forced sharing. As a result data portability can hardly be a useful tool in tackling disruptions in the competitive process.

As a conclusion big data containing personal data can in some circumstances form an essential facility capable of being the subject of the court ordered forced sharing remedy. In theory data portability right has less concerns for the incentives of companies to innovate and invest in big data as the personal data belongs to the user and he or she has the right to decide what to do with the personal data. On the other hand the data sets subject to forced sharing could contain the data of multiple users and even other data than the mere user data, which makes this form of data more useful for companies.

The key point is that while big data can result in market power and possible competitive disruptions, its benefits are in most cases short lived in the fast moving IT sector. Therefore there is a need for sector specific regulation that takes into consideration both the efficient functioning of markets as well as the data privacy aspects.