Protecting Non-personal Data in the Framework of the Legislation of the European Union

Ville Mustila
Faculty of Law
University of Turku
May 2020

UNIVERSITY OF TURKU
FACULTY OF LAW

Ville Mustila: Protecting Non-personal Data in the Framework of the Legislation of the European Union

Thesis, 57 pages, attachments, xiii pages
Commercial Law
May 2020
The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

Data has become one of the most valued resources in today's economy. With the introduction of Big Data analytics and the Internet of Things, it is vital for businesses of all sizes to gain access and benefit from non-personal data. While personal data is governed by the GDPR, non-personal data does not currently have any catch-all regulation within the EU. The majority of protection is brought by a combination of contract law and technological means. This Master's thesis aims to explore the current EU legislation in order to determine whether or not there are ways to protect non-personal data within the EU, and how this protection could be developed.

The thesis is mostly legal dogmatic in nature, but some comparative and critical legal perspectives are also taken. Additionally, some technological terminology and economic theories of value are used.

Conclusion is that some EU legislation, namely the Database Directive and the Trade Secrets Directive could offer protection to non-personal data that falls within their scope. This, however, is not necessarily a very significant portion of the data. In the U.S. trade secrets protection, the civil law regulations seem to be even stricter on what can benefit from trade secrets protection. Data ownership and non-legislative measures are explored as possible avenues forward, but in the end, there are benefits to both legislating and using non-binding measures. It is concluded that the best solution would likely involve a combination of both, in addition to the development of technical means of protection. Further research in the area is required.

Keywords: EU law, non-personal data, trade secrets, data rights, Internet of Things, Big Data

TURUN YLIOPISTO
OIKEUSTIETEELLINEN TIEDEKUNTA

Ville Mustila: Protecting Non-personal Data in the Framework of the Legislation of the European Union

Tutkielma, 57 sivua, liitteet, xiii sivua
Kauppaoikeus
Toukokuu 2020
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -järjestelmällä.

Datasta on tullut yksi taloutemme ja yhteiskuntamme tärkeimmistä resursseista. Big Datan ja esineiden internetin (Internet of Things) vallankumouksen myötä Big Data analytiikasta on tullut tärkeää myös sellaisille yrityksille, joiden liiketoiminta ei suoraan liity dataan. Vaikka EU:n alueella Tietosuoja-asetus sääntelee henkilötietoja hyvin pitkälle, ei muun tyyppisiä tietoja koskevaa sääntelyä ole juuri lainkaan. Tämän pro gradu -tutkielman tarkoituksena on kartoittaa EU:n nykyisen lainsäädännön sisältöä, sekä arvioida miten sitä voisi hyödyntää yritysten dataomaisuuden suojelussa. Lisäksi se tutkii mahdollisuuksia lainsäädännön kehittämiseksi tällä alueella.

Tutkielman metodi on pitkälti oikeusdogmaattinen, vaikkakin jonkin verran oikeusvertailua ja oikeuskriittistäkin näkökulmaa on hyödynnetty. Myös teknologista termistöä ja taloustieteen arvoteorioita käytetään hyödyksi.

Tutkielman tulosten perusteella voidaan todeta, että sekä EU:n Tietokantadirektiivi, että Liikesalaisuusdirektiivi voivat olla hyödyksi datan suojelemisessa. Direktiivien asettamien vaatimusten vuoksi niiden kattavuus jättää kuitenkin toivomisen varaa, eikä Yhdysvaltojenkaan liikesalaisuuslainsäädännön tarkastelu tuottanut laajempaa tulosta. Toimivin tulevaisuuden ratkaisu datalainsäädännön alalla tulee todennäköisesti olemaan jonkinlainen yhdistelmä datan omistajanoikeuksia, ei-lainsäädännöllisiä keinoja ja teknologisten suojausmuotojen kehittämistä. Selkeiden vastausten saamiseksi tarvitaan lisää tutkimusta.

Avainsanat: data, liikesalaisuudet, EU-oikeus, muut kuin henkilötiedot, Big Data, Internet of Things, teollisuusdata, datan määrittely

Table of Contents

References

Literature

Argento, Zoe: *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation* (July 21, 2014). 16 Yale Journal of Law & Technology 172 (2014); Roger Williams Univ. Legal Studies Paper No. 150.
Available online: https://ssrn.com/abstract=2469220 accessed 1.5.2020.

Arrow, Kenneth: *Economic Welfare and the Allocation of Resources for Invention*, in Universities-National Bureau Committee for Economic Research, Committee on Economic Growth of the Social Science Research Council: *The Rate and Direction of Inventive Activity: Economic and Social Factors* [Princeton, New Jersey]: Princeton University Press, 1962, pages 609-627.

Baker McKenzie & Euromoney: *Protect and Preserve: The Rising Importance of Trade Secrets*, 2017.
Available online: http://www.bakermckenzie.com/-/media/files/insight/publications/2017/tradesecrets.pdf?la¼en accessed 11.5.2020.

Broy, Dominic: *The European Commission's Proposal for a Framework for the Free Flow of Non-Personal Data in the EU*, European Data Protection Law Review (EDPL), vol. 3, no. 3, 2017, pages 380-383.

Chandler, D., & Munday, R: API. In *A Dictionary of Social Media*: Oxford University Press. Accessed 11.5. 2020.

Cohen, Bret A. and Renaud, Michael T. and Armington, Nicholas W.: *Explaining the Defend Trade Secrets Act* Business Law Today 1 (2016).

Dapp, Thomas F. and Heine, Veronika: *Big Data – The Untamed Force*, Deutsche Bank Research, 2014.
Available online: https://www.dbresearch.com/PROD/RPS_EN-PROD/Big_data_%C2%96_the_untamed_force/RPS_EN_DOC_VIEW.calias?rwnode=PROD0000000000435629&ProdCollection=PROD0000000000451930 accessed 4.5.2020.

De Franceschi, Alberto and Lehmann, Michael: *Data as Tradeable Commodity and New Measures for Their Protection*, The Italian Law Journal, 51, 2016, pages 51-72.
Available online: https://italian-law-journal.scholasticahq.com/article/592-data-as-tradeable-commodity-and-new-measures-for-their-protection accessed 10.5.2020.

de Werra, Jacques: *How to Protect Trade Secrets in High-Tech Sports? An Intellectual Property Analysis Based on the Experiences at the America's Cup and in the Formula One Championship* (June 20, 2010). European Intellectual Property Review, Volume 32, Issue 4, 2010, page 155.
Available online: https://ssrn.com/abstract=2149767 accessed 11.5.2020.

Derclaye, Estelle: *Research Handbook on the Future of EU Copyright*, [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2009.

Desai, Shreya: *Shhh - It's a Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive*, Georgia Journal of International and Comparative Law, volume 46, issue no. 2 (2018) pages 481-514.

Drexl, Josef: *Designing Competitive Markets for Industrial Data,* Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 8, no. 4, 2017, pages 257-292.

Drexl, Josef and Hilty, Reto M. and Desaunettes, Luc and Greiner, Franziska and Kim, Daria and Richter, Heiko and Surblytė, Gintarė and Wiedemann, Klaus: *Data Ownership and Access to Data*, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, 2016.

Goldman, Eric: *The New 'Defend Trade Secrets Act' Is the Biggest IP Development in Years*, FORBES (Apr. 28, 2016).
available online: https://www.forbes.com/sites/ericgoldman/2016/04/28/the-new-defend-trade-secrets-act-is-the-biggest-ip-development-in-years/#334e1b934261 accessed 1.5.2020.

Gordon, Keith: *What is Big Data?*, ITNOW, Volume 55, Issue 3, Autumn 2013, Pages 12–13.
available online: https://doi.org/10.1093/itnow/bwt037 accessed 10.5.2020

Graef, Inge and Gellert, Raphael and Purtova, Nadezhda and Husovec, Martin: *Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data* (January 22, 2018).
Available online: https://ssrn.com/abstract=3106791 accessed 29.4.2020.

Green, Jonathan: *Trade Secrets and Data Security: A Proposed Minimum Standard of Reasonable Data Security Efforts When Seeking Trade Secret Protection for Consumer Information,* Cumberland Law Review, vol. 46, no. 1, 2015-2016, pages 181-218.

Halligan, R. Mark, and Richard F. Weyand: *The Economic Valuation of Trade Secret Assets*. Journal of Internet Law 9 (8) 2006, pages 19-24.

Hartzog, Woodrow: *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, [Cambridge, Massachusetts]: Harvard University Press, 2018.

Hilty, Reto *Big Data: Ownership and Use in the Digital Age* in Seuba, Xavier and Geiger, Christophe and Penin, Julien (eds), *Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data*, Global Perspectives for the Intellectual Property System, CEIPI-ICTSD, Issue 5, 2018, pages 85-94.

Hugenholtz, Bernt P.: *Data Property: Unwelcome Guest in the House of IP.* Paper presented at *Trading Data in the Digital Economy: Legal Concepts and Tools*, [Münster, Germany], 2017.

Johnson, E. Eric, *Trade Secret Subject Matter*, (2010) Hamline Law Review, 33, Summer, 545-581 in Sandeen, K. Sharon, and Rowe, A. Elizabeth: *Trade Secrets and Undisclosed Information* [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2014, pages 422-458.

Kaur, Gurjit and Tomar, Pradeep: *Handbook of Research on Big Data and the IoT*, [Hershey, Pennsylvania]: IGI Global, 2019.

Kerber, Wolfgang, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection* (April 26, 2016). Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int) 2016, pages 639-647 (Kerber 2016a).
Available online: https://ssrn.com/abstract=2770479 accessed 4.5.2020.

Kerber, Wolfgang: *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, (October 24, 2016), Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 11/2016, pages 989-999 (Kerber 2016b).
Available online: https://ssrn.com/abstract=2858171 accessed 11.5.2020.

King, J.E. and McLure, Michael: *History of the Concept of Value*, 2014
Available online: http://www.business.uwa.edu.au/__data/assets/pdf_file/0004/2478883/14-06-History-of-the-Concept-of-Value.pdf accessed 12.5.2020.

Kitch, Edmund W.: *The Nature and Function of the Patent System*, The Journal of Law & Economics, volume 20, issue no. 2, 1977, pp. 265–290.
Available online: www.jstor.org/stable/725193 accessed 8.5.2020.

Landes, William M., and Posner, Richard A: *The Economic Structure of Intellectual Property Law* [Cambridge, Massachusetts]: Harvard University Press, 2003.

Leistner, Matthias *The Protection of Databases* in Derclaye, Estelle: *Research Handbook on the Future of EU Copyright* [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2009, pages 427-456.

Merrill, Thomas W.: *Property and sovereignty, information and audience*, Theoretical Inquiries in Law, 18(2), pages 417-445.

OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, [Paris, France]: OECD Publishing, 2015.
Available online: https://doi.org/10.1787/9789264229358-en accessed 10.5.2020.

Penner, J., *The 'Bundle of Rights' Picture of Property*, UCLA Law Review 43.3 (1996): 711.

Pingo, Zablon and Narayan, Bhuva: *Big Data and the Internet of Things: Current Industry Practices and Their Implications for Consumer Privacy and Privacy Literacy* in Kaur, Gurjit and Tomar, Pradeep: *Handbook of Research on Big Data and the IoT*, [Hershey, Pennsylvania]: IGI Global, 2019, pages 55-76.

Rifkin, Jeremy: *The Age of Access*, [New York, New York]: Tarcher/Putnam, 2000.

Sandeen, Sharon K.: *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 2010, Hamline Law Review, 33, Summer, 493-543 in Sandeen, K. Sharon, and Rowe, A. Elizabeth: *Trade Secrets and Undisclosed Information* [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2014, pages 3-53.

Sandeen, Sharon K.: *The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is* Based, 2011, in Sandeen, K. Sharon, and Rowe, A. Elizabeth: *Trade Secrets and Undisclosed Information* [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2014, pages 797-827.

Sandeen, K. Sharon, and Rowe, A. Elizabeth: *Trade Secrets and Undisclosed Information* [Cheltenham, United Kingdom]: Edward Elgar Publishing Ltd, 2014.

Selamat, Siti Aishah Mohd and Prakoonwit, Simant and Shandi, Reza and Khan, Wajid: *Big Data and IoT Opportunities for Small and Medium-Sized Enterprises (SMEs)*, Bournemouth University, 2019 in Kaur, Gurjit and Tomar, Pradeep: *Handbook of Research on Big Data and the IoT*, [Hershey, Pennsylvania]: IGI Global, 2019, pages 77-88.

Seppälä, Timo and Juhanko, Jari and Mattila, Juri: *Data Ownership and Governance – Finnish Law Perspective*, ETLA Brief 71 2018.

Shapiro, Carl. and Hal R. Varian: *Information Rules: a Strategic Guide to the Network Economy*, [Boston, Massachusetts]: Harvard Business School Press, 1998.

Sibble, Joshua. *International Trend Toward Strengthening Trade Secret Law* Intellectual Property & Technology Law Journal 26, no. 4 (2014), pages 18-20.

Silva, Nuno Sousa e, *What Exactly is a Trade Secret Under the Proposed Directive?,* Journal of Intellectual Property Law & Practice, Volume 9, Issue 11, November 2014, pages 923–932.
Available online: https://doi.org/10.1093/jiplp/jpu179 accessed 2.5.2020.

Slaby, David W. and Chapman, James C. and O'Hara, Gregory P.: *Trade Secret Protection: An Analysis of the Concept Efforts Reasonable Under the Circumstances to Maintain Secrecy*, 5 Santa Clara High Tech. L.J. 321 (1989).
Available online: https://digitalcommons.law.scu.edu/chtlj/vol5/iss2/4 accessed 12.5.2020

Smith, Henry E.: *Property Is Not Just a Bundle of Rights*, Intellectual Tyranny of the Status Quo, volume 8(3), 2011, pages 279-291.
Available online: https://econjwatch.org/articles/property-is-not-just-a-bundle-of-rights accessed 11.5.2020.

Spulber, Daniel F.: *How Patents Provide the Foundation of The Market for Inventions*, Journal of Competition Law & Economics, Volume 11, Issue 2, June 2015, Pages 271–316.

Statista Research Department: *Internet of Things - number of connected devices worldwide 2015-2025*, published 27.11.2016.

Stepanov, Ivan: *Introducing a property right over data in the EU: the data producer's right – an evaluation*, International Review of Law, Computers & Technology, Volume 34, 1/2020, pages 65-86.
Available online:
https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621?scroll=top&needAccess=true accessed 10.5.2020.

Tantleff, Aaron: *Considerations on Big Data Licensing*, Managing Intellectual Property, 246, 2015, pages 14-17.

Universities-National Bureau Committee for Economic Research, Committee on Economic Growth of the Social Science Research Council: *The Rate and Direction of Inventive Activity: Economic and Social Factors*, [Princeton, New Jersey]: Princeton University Press, 1962 pages 609-627.
Available online: http://www.nber.org/books/univ62-1 accessed 7.5.2020.

Vapaavuori, Tom: *Liikesalaisuudet ja salassapitosopimukset*, 3rd edition. [Helsinki, Finland]: Alma Talent Oy, 2019.

Ward, John S. and Barker, Adam: *Undefined By Data: A Survey on Big Data Definitions*, School of Computer Science, University of St Andrews, United Kingdom 2013.

Wiebe, Andreas, Protection of industrial data – *A New Property Right for the Digital Economy?,* Journal of Intellectual Property Law & Practice, Volume 12, Issue 1, January 2017, pages 62–71.
Available online https://doi.org/10.1093/jiplp/jpw175 accessed 6.5.2020.

Willems, Heiko: *Trading in Data: An Industry Perspective,* 2017 in: Lohsse, Sebastian and Schulze, Reiner and Staudenmayer, Dirk: *Trading Data in the Digital Economy: Legal Concepts and Tools* [Baden-Baden, Germany]: Nomos 2017.

Zech, Herbert, *A legal framework for a data economy in the European Digital Single Market: rights to use data*, Journal of Intellectual Property Law & Practice*,* Volume 11, Issue 6, June 2016, pages 460–470.
Available online https://doi.org/10.1093/jiplp/jpw049 accessed 7.5.2020.

Zech, Herbert, *Data as a Tradeable Commodity – Implications for Contract Law* (September 2017). Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: *The New Data Economy between Data Ownership, Privacy and Safeguarding Competition*, Edward Elgar Publishing, Forthcoming.
Available online: https://ssrn.com/abstract=3063153 accessed 10.5.2020.

Zech, Herbert, *Information as Property*, JIPITEC 6 (3) 2015, 192.
Available online: https://ssrn.com/abstract=2731076 accessed 27.4.2020.

Yu, Peter K., *Data Producer's Right and the Protection of Machine-Generated Data,*
Tulane Law Review, vol. 93, no. 4, April 2019, pages 859-930.

Official Publications

A Digital Single Market Strategy for Europe, COM(2015) 192 final.

Building a European Data Economy, COM/2017/09 final (COM2017a).

COMMISSION STAFF WORKING DOCUMENT: on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication: Building a European data economy COM/2017/09 final (COM2017b).

A European Strategy on Data, COM(2020) 66 final (COM2020).

Court of Justice of the European Union, PRESS RELEASE NO 39/19.

EU Legislation

Treaty on the European Union (TEU)

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Not yet in force as of May 2019) (Copyright Directive).

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive).

Regulation (EU) 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 (General Data Protection Regulation).

Directive (EU) 2009/24 of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Computer Programs Directive).

Directive (EU) 96/9 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive).

International Treaties

Trade-Related Aspects of Intellectual Property Rights Agreement (TRIPS).

United States Law

Uniform Trade Secrets Act of 1979 with 1985 amendments.

Economic Espionage Act of 1996.

Defend Trade Secrets Act.

EU Case Law

C-338/02 *BHB v. William*
ECLI:EU:C:2004:695

C-46/02 *Fixtures Marketing Ltd v. Oy Veikkaus Ab*
ECLI:EU:C:2004:694

C-128/11 *UsedSoft GmbH. v. Oracle International Corp.*
ECLI:EU:C:2012:407

C-30/14 *Ryanair v. PV Aviation*
ECLI:EU:C:2015:10

C-166/15 *Ranks and Vasiļevičs*
ECLI:EU:C:2016:762

United States Case Law

Compco Corp. v. Day-Brite Lighting, Inc., 376 U. S. 234 (1964)

Sears, Roebuck & Co. v. Stiffel Co., 376 U. S. 225 (1964)

Erie R. Co. v. Tompkins, 304 U. S. 64 (1938)

Finnish Case Law

Helsingin HO 16.2.2018, dnro R 16/1956.

List of Abbreviations

B2B	Business-to-Business
ECJ	Court of Justice of the European Union
EEA	Economic Espionage Act
EU	European Union
GDPR	General Data Protection Directive
IoT	Internet of Things
OECD	Organisation for Economic Co-operation and Development
SME	Small and Medium Enterprise
TEU	Treaty on European Union
TRIPS	Trade-Related Aspects of Intellectual Property Rights
U.S.	United States
UTSA	Uniform Trade Secrets Act
WTO	World Trade Organisation

1. Introduction

1.1. General

Data is something none of us can avoid. Most of us know what it means, or what at least we think we do. It is likely, however, that the majority of us do not truly comprehend the vastness of the amount of information that is collected from every single one of us every day. Because that is what data in its core is; it is information, no matter how irrelevant it may seem to us at the time of collection.

Of course, data is completely necessary. It is an old concept, born with the surfacing of first written markings. In today's world, though, it has a different meaning. Data is everywhere, in everything we do. Each of us carries the knowledge of the whole world in our pockets or bags in the form of a smartphone, computer, or any other device with internet access. It is simply not feasible to think that a person could be a part of modern society, go about their daily business, work, shop, or quite literally live without leaving some traces of data in their wake. It is not completely impossible, but the tradeoffs are something that most of us would not be willing to make anymore.

What makes the world today different? Why should it suddenly matter? It is not the existence of data, but the efficiency in both acquiring and processing it that makes the difference. These facts coupled with the consideration that most of our data does not go to a well-regulated, government-run databank, but to the big tech giants, such as Google and Amazon, or the social media companies, such as Facebook and Twitter, are what separates the current environment from the past. In the "data-driven economy"[1], these titans of the industry run the show for less-pronounced companies and small-and-medium enterprises (SMEs).

However, digital data and its collection are often not harmful, but a necessity. In fact, many governmental functions rely on data collection to be able to work efficiently. Examples of this would be healthcare and taxation. Often it is to make our life more convenient, streamlined, and simple. It is much more convenient and faster when Google Chrome auto-fills our personal information in yet another job application, or when Netflix suggests to us a TV-series that we are interested in. A little bit of offered convenience, and we give our personal and less-personal data away willingly. And this does not even begin to touch on the gigantic passive data streams

[1] OECD, 2015 pp.

that are constantly being fed to various servers from our appliances at home, work, or on our person.

In short, data may just be the single most valuable resource in today's business world and the technologically driven markets. It simply cannot be overstated; the value of information is immense.

What differentiates data from other resources, such as oil, gold, coal, or wood, is that its value is not the same in the hands of every person, natural or legal. For example, consider sensor data from an appliance that monitors and records the amount of rain in a certain area of farmland. Firstly, this data is obviously useful to the farmers, as they have to regulate the amount of water their crops get to grow and yield a profitable harvest. They are also likely the ones who purchased and installed these appliances. Secondly, the same data can be incredibly useful for the company that made it, and is most likely stored on their servers; in times of localized draughts, for example, the company might be able to focus its marketing on these areas towards different watering solutions or nutrients necessary for crops to survive such draughts. Third, as mostly a curiosity, we can consider for example an environmental researcher, that could use the data from these sensors towards their research. And these are only the three most obvious beneficiaries, and without considering the combining of this information.

This topic is discussed further in chapter 2.2.1, in which we take a look at different ways of interpreting the value of information.

1.2. Structure and Research questions

This study will focus primarily on the value of data that would interest the manufacturer of the sensors in the above example, the potential commercial applications of non-personal information. More precisely, this study will explore the different legal options a company has to protect this kind of data from its competitors within the EU, and whether or not this kind of protection is warranted at all. Focus will be on protection through the use of trade secrets, as well as in the recent Trade Protection Secrets Directive, with a light touch on the possibility of using the Database Directive.

The study is structured in following way: first, the study will take a look at data, it's the difficulties surrounding it and what arguments exist in favor of enacting specific legal protection for industrial data, and what speaks against it; second, the study will examine current legislation in the EU, Finland and as a point of comparison, the U.S. Finally, possible measures to be taken

to protect industrial data by means of specific legislation or by further developing certain legal constructs will be considered.

The research questions are formulated as follows: Is industrial data protected by the legislation within the sphere of EU law? Can this kind of non-personal, sensor derived data hope for protection under the Trade Secrets Directive, or the Database Directive, and are the remedies derived from these directives effective in case of data? Does it require protection at all? What could be done to further the protective measures, if society deems it worth protecting?

1.3. Method and Literature Review

The method used in this study is largely dogmatic, as it aims to form a coherent understanding of protecting non-personal data on EU-level, though some comparative approaches have been taken to study the trade secrets legislation within Finland and the United States. Some remarks and subchapters could be interpreted to be critical of the current legislative approaches, though the chapter seeking solutions will focus on finding and compiling existing ideas rather than criticizing the current legislation. Some computer science terminology is used, mainly to explain different concepts that the study comes across regarding data, its storage, and handling.

Due to the modern nature of the research subject, relevant books written in the area are somewhat scarce, especially those concerning the newest developments, such as the implementation of the Trade Secrets Directive. Scientific articles, however, are in abundance, and the study relies heavily on information found in different journals and collections. While a large portion of the literature is European, some American articles and collections were utilized.

There is also a multitude of internet sources that can be utilized in a study that aims to explore modern technology; while the pickings for reliable information on the legal side of the study are slim outside official and peer-reviewed journals and literature, for technical knowledge there exists a trove of information on the internet for the curious.

Lastly, many official documents and court cases have been explored, most of these originating from the different officials of the European Union. Some legislation from the United States, as well as a few relevant court cases have been considered.

2. Defining Data and Its Worth

Discussed in this chapter are the most essential definitions when considering data as a whole, Big Data analytics, and the Internet of Things. It aims to shed light on the complex terminology and different ways of interpreting the word "data", and to provide tools needed to navigate the later chapters. The second part is dedicated to the discussion around the deceptively simple question: is the legal protection of this kind of non-personal data necessary?

2.1. What We Mean by Data, and Why Is It So Complicated

The first step in regulating data is to, naturally, understand how to define data. It is not a clean-cut definition; as we will discover, it is sometimes incredibly difficult or even impossible to determine with any kind of certainty which legislation a piece of information falls under.

Data is, essentially, information. At its most basic definition, what we mean by data is machine-readable, encoded information. It is the basis of life today, and indeed modern society is often referred to as "information society". To understand the legal issues arising from the use, storage, and movement of data, we must first understand what we mean by "data" when talking about it in the context of industrial data. This requires understanding two key terms, Big Data and the Internet of Things (IoT), and how they interact with each other to fuel the modern data economy.

To better understand information, and data as an object, it can be separated into three levels; semantic, syntactic, and structural information.[2] At the semantic level is the meaning of a certain bit of information. For example, the information or the data that would be considered know-how, or the content of a book. [3] In terms of legislation, this level would be protected by, for example, patent or trade secret laws. The syntactic information would, then, be the writing itself that makes up the content of the book, or in the case of data, the 0s and 1s that make up the information on the device. This is what would be protected by, for example, copyrights or design protection. Finally, the structural information is the book, or for data, a flash drive or a DVD itself, the "physical carrier" of the information. This is what would be protected by traditional property rights. This classification is important because it allows potential data-centric legislation and contracts to specify which level of information, or data, they seek to protect.

[2] See e.g. Zech, 2015 pp. 194, Zech, 2016 pp. 462-463.
[3] Zech, 2015 pp. 194.

"In the world of Big Data, more is always better."[4]. Big Data is raw, partially processed and processed data that is defined to be simply too vast in scale for either humans or conventional algorithms to process. In terms of levels of data, it falls, usually, to the syntactic level. It is, perhaps, best described by the three V's that originally were the key attributes that were used to define Big Data; volume, velocity, and variety.[5] Lately, a fourth[6] and a fifth[7] V have been added; veracity and value. In other words: big data contains massive amounts of data from all parts of the spectrum, and it moves incredibly quickly.

Internet of Things (IoT) refers to the communication that happens between our smart devices, such as cars, smartphones, tablets, TVs, or more lately, kettles, washing machines or really any appliance that is somehow connected to others, be it through a wireless network, Bluetooth or physical cables. This information is collected by the device using either physical sensors, such as those that regulate the thermostat in a modern smart home, or by the device itself, such as the digital information produced by using a smart device i.e. cookies, browsing habits or data usage.

Big Data analytics are the tools that are used to tackle the massive flow of information produced by the IoT, and to tap the massive potential carried by this non-personal data. Needing a working solution for Big Data to benefit from the data flows produced by the IoT is one of the fundamental reasons why big tech corporations have an edge over SMEs; Big Data analytics requires substantial investment in know-how, hardware, software, and facilities.[8] The lack of existing Big Data structures might be the reason why a large portion of SMEs may not be equipped to benefit from the rise of IoT and the massive amounts of raw data it brings with it, even if they produce the devices that gather this information.[9]

2.2. Personal or non-personal?

Data can be divided roughly into two types: personal data, and non-personal data. Drawing the line can sometimes be challenging, as the type of a piece of information can change over time, especially if it can be combined with some other information to draw a connection with a single person. In the clear majority of cases, this change will occur from non-personal to personal.

[4] Hartzog, 2018 pp. 51.
[5] Ward, Barker, 2013 pp. 1.
[6] Pigon, Narayan, 2019 pp. 59.
[7] Gordon, 2013 pp. 12.
[8] Selamat et al., 2019 pp. 79.
[9] ibid., pp. 78.

Defining personal data is quite simple; we can, for example, take one of the most recent definitions available in legislation, the one used in the European Union's General Data Protection Regulation (GDPR). It's article 4 states the following:

> *"'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"*[10]

In other words, anything that can be used to positively, directly or indirectly, identify a natural person, is personal data. This may sound simple, but in practice it can be very complicated, or nearly impossible, to determine the threshold between what is possible to use in the identification of a natural person.[11] Due to the dynamic wording of the definition, it is also possible for a piece of data to transform between personal and non-personal, depending on the processing and the available context.[12] Personal data is on the semantic level, as its definition relies on its ability to convey content that allows identification of a natural person.

Regarding non-personal data, in theory the aforementioned definition makes it quite simple, as the definition for non-personal data can be derived from it by using it as means to rule out all data that would fall under the definition of personal data. Non-personal data would then, in short, be all that is left. In other words, all data that cannot be considered personal, is non-personal. This has been also used in EU legislation, for example in the Framework for the Free Flow of Non-Personal Data in the European Union regulation.[13] This kind of information comes from many sources.[14] Good examples of this type of data would be different instances of sensory data collected by our modern appliances. Such data can be described in many ways. The most common used seems to be "industrial data"[15].

[10] Regulation (EU) 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 (General Data Protection Regulation) Art. 4.
[11] Graef et al., 2018 pp. 4.
[12] ibid., pp. 1-3.
[13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union Art. 3 (1).
[14] See e.g. Kerber, 2016a pp. 2.
[15] See e.g. Wiebe, 2017.

Finally, another, third grouping of data has been suggested[16], a group that would be situated somewhere between the personal and non-personal data. While the information in this group is not personal on its own, "… the relation to the person could (more or less) easily be produced."[17]. This is the data that most significant applications would be interested in, as it is the fuel for all kinds of connections which can be made about a user by combining a multitude of different sources.

This study will focus on non-personal, industrial data, and mostly disregard personal data, as it falls outside of the scope of interest in this study.

2.3. Why Should Industrial Data Be Regulated?

2.3.1. The Value of Industrial Data

It seems to be a fact that almost all data have some value, at least to someone. While the actual monetary value and even the person/entity who can derive it may vary based on which piece of information is being discussed, the fact remains the same; information is valuable. Take, for example, the speed and performance data recorded by the sensors of a modern smart car. It can, first and foremost, be valuable to the manufacturer who produced the car; it can lead to innovation and further streamlining of their manufacturing process. Secondly, it can be valuable to the vendor who sold the car, to give more precise information on the performance and safety of the vehicle to cement further sales. Third, the data can obviously be valuable to the competitors of the manufacturer, to give them a competitive edge, or to be quick to expose any faults in the design of the vehicle to try and damage the reputation of the original manufacturer.

Aside of these rather clear avenues of exploitation for this particular data set, others can be found as well; researchers may be interested in the data to further their projects, insurance companies to determine the premiums charged from the owner of the vehicle, or in a case of an accident to possibly try to determine their liability to reimburse the driver through the insurance. Even government officials could be interested in the data, if it can help to clear up accident investigations, make sure the vehicle is up to the current safety standards, or, for example, determine the tax class of the model in question.[18]

[16] Hilty, 2018 pp. 91.
[17] ibid. Hilty uses an example of traffic flow data – data that is collected from the location data of the users of various navigation applications and could be used to identify a single user when compiled, for instance, with the data from their smart car.
[18] For more on the economic value of data, see e.g. Dapp, Heine, 2014 pp. 17-20

Of course, the value of data is not as easily determined as is the case with physical goods or one's labor. Traditional value theories often fall short when trying to assign value to digital information[19]. Traditional goods pull added economic value from each step of the rather vertical chain, starting from the manufacturer of the raw materials and ending at the distribution step on a retailer's shelf. Naturally information cannot be treated the same way, as digital information can be copied and re-copied without reducing the value of the original copy of the piece of information, as is the case with any digital good. As such, data can be said to be "expensive to produce, but cheap to reproduce."[20] Smart devices and data generated by the Internet of Things gather their value in more complex networks[21], through extensive information collecting and sharing between different connected devices. In the case of Internet of Things, data is usually not seen as expensive to produce – the production often happens almost accidentally, collected by the ambient sensors, the purpose of which may not even be to collect and store that particular information, but the device needs it to fulfill its primary function, e.g. keeping the room temperature at a certain level.

The amount of data collected by the Internet of Things is massive, as the number of connected devices is increasing exponentially across the globe. A study estimates that that number could be as high as 42 billion devices worldwide in 2022.[22] In 2019, the same number was 26.6 billion, while in 2015 it was 15.4 billion.[23] EU Commission estimated the value of European data economy to have been EUR 257 billion in 2014, and that it would grow to be over double that at EUR 643 billion in 2020.[24] With numbers like these, that are difficult even fully to comprehend, it is no wonder that the legislative bodies around the world are lagging behind. Needless to say, the potential value from the network-linked devices expands with the quantity of these devices available, and it is not unreasonable to assume that the quality of the data collected in this manner is going to keep improving in both precision and readability. As this can hardly be expected to lower the value of the data collected by the Internet of Things, it seems safe to expect this data to have significant value in the future.

2.3.2. A Stable Legal Framework for Industrial Data

Regulating the use, ownership, and protection of the industrial data has benefits outside of just ensuring that businesses' valuable data is protected; it can create stability and transparency in

[19] King, McLure, 2014 pp.10.
[20] Shapiro, Varian, 1998 pp. 3.
[21] Drexl 2017 pp. 266.
[22] Statista, 2016.
[23] ibid.
[24] COM/9/2017 final "Building a European Data Economy".

this legislative sphere, which in turn can, in theory, lead to growing trust between both the consumers and the companies themselves.

Investing in new and enhanced technologies is one of the cornerstones of the modern industrial market. Since investors tend to favor stable investments, a safer legislative framework can lead to larger investments in areas and technologies that might be deemed too risky in the current legal vacuum; this being doubly true for small businesses and start-ups. While it may be completely possible for big tech giants such as Google, Facebook or Amazon to ensure that their data is protected through contracts, it is difficult for a small start-up, often consisting only of a single natural person, to be in a good or even equal position when dealing with the industry giants – which often is necessary when reliance on the distribution, component or raw material networks of others is the lifeblood of most young start-up companies. Investing, of course, is not merely consideration for young or small businesses, but an important part of the growth underlining any healthy corporation. Not having to rely on the protection provided purely on contractual basis could help push medium-sized companies to invest in different kinds of projects spanning industrial data collection, storage, and infrastructure, boosting the economic growth on the Union area.

2.3.3. Clarifying Data Ownership

Ownership of data, particularly industrial, machine-generated data, is not a clear-cut issue. There are arguments for and against many different approaches as to who is the rightful owner of certain data produced by a sensor in a smart device. This has become increasingly more difficult as the vast majority of data in the world is now stored not necessarily on physical devices or hard drives, but on cloud services[25] and in data banks. The information has to always go *somewhere*. Even when it is in the "cloud", it is stored on a physical server in some corner of the world. The difference between having your information stored in a physical "carrier" (such as a flash drive, a physical disk, be it DVD, CD or even an old-school floppy) and in a data bank or cloud service is that the owner of the latter two is often an independent third party. Maintaining storage for massive amounts of raw data can get expensive, as it requires specific facilities, know-how, and constant investments and upkeep that a lot of SMEs might not be willing or able to justify.

[25] Cloud services (also referred to as cloud-computing) are essentially a form of offering software, infrastructure or platforms as a service. In the case of data by "cloud" we mean infrastructure-as-a-service, which, for example, boils down to someone offering to store your data for you on their server, while you maintain full access to it through the internet.

As such, another important feature of enacting legal protections for industrial data is that legislators would be forced to clarify questions concerning the legal ownership of such data – As it stands right now, it is difficult to say for certain who owns machine-generated data. Is it the manufacturer of the sensory equipment on whose servers the data most likely is stored – or is it the consumer who uses the equipment and does the actual "data collecting", or at least whose activity leads to the data being collected and transmitted, even if as a byproduct of use. And what rights, if any, possess the data service providers who own the physical piece of technology containing the said information?

Non-personal data does not lend itself well to the conventional means of defining the ownership of objects, nor does it work with intellectual property rights. It seems, in fact, that data itself cannot be "owned" in the traditional sense.[26] While you can, and all of us most definitely do, own a physical representation or storage that contains certain information, the difficulty comes with the ownership of information itself. In classic interpretation of intellectual property rights, this has been attempted to solve by giving the rights to the information to the person who created said information. With machine-generated data, the problem is that the entity creating the information is not a legal or natural person, but a machine.

One way to solve this issue has been proposed in the EU. On October 1st, 2017 European Commission gave a communication titled "Building a European Data Economy"[27] in which it suggested so-called "Data Producer's Right", which would essentially give ownership rights to the "data producers", which in this case means the owner of the device or the long-term user (i.e. licensee) of the device.[28] The idea has been met with criticism both inside and outside of Europe and has not been officially put in motion even within the EU. This idea will be discussed and explored further in chapter 5.

2.4. Arguments Against Legislative Measures

2.4.1. Free Flow of Data

While it is imperative to recognize the value found within industrial data, and that the benefits of a clearer legislative framework could be substantial, it is equally mandatory to explore the possible boons of not using hard legislation. First and foremost, too restrictive legislation could serve as a gigantic impediment for innovation and slow the advancement of technology down

[26] Seppälä et al., 2018 pp. 1.
[27] COM/2017/09 final, "Building a European Data Economy".
[28] ibid., at 3.5.

needlessly. EU Commission has been on a mission to improve the technological capabilities of the EU to an internationally top-level, both with its legislative endeavors and softer, non-binding recommendations for contract terms and self-regulating entities for the data market.[29]

In 2018, the EU passed a regulation concerning the free flow of non-personal data, that came into force on May 29th, 2019.[30] This regulation strives to ensure the free flow of non-personal data within the EU, but it does not provide much in the way of protection; it is, however, notable due to its definition of the non-personal data; even if it merely uses the GDPR definition of personal data to lump up everything else as non-personal.

2.4.1.1. Impediment of Innovation

While the adoption of legislation to control the use (or access) and ownership of non-personal data can serve by reinforcing the trust in the legal environment around it, it may also cause some unwanted effects on the market as a whole. Restrictions in access to data could mean life or death to many different innovations derived from existing information.[31] Inhibiting access to already existing information could cause many SMEs, especially start-ups, to topple before even getting a proper chance to enter the market. As discussed briefly, SMEs are in a somewhat vulnerable position when it comes to non-personal data and Big Data analytics, and consequently reaping the rewards of the information flow that accompanies IoT. They often do not possess the necessary workforce or even the know-how, which in the area of Big Data analytics is quite specific, to handle the requirements of benefitting from a Big Data stream of their own. While using external consultation services or even businesses that would analyze the Big Data for SMEs is possible in theory, it is costly, and so it would likely not be an option for most SMEs due to budgetary reasons.

It is curious to note that the argument to benefit SMEs and innovation could be reasonably spun either way; on the one hand, clarifying the protection of non-personal data assets could lead to SMEs and start-ups being braver to innovate new business models and data collection methods if there was a way to ensure the protection of their innovations. On the other hand, it is as discussed above; restricting access to already existing information could seriously hamper the ability to innovate based on it. It is difficult to say for certain which side of the argument would,

[29] See e.g. COM/2017/09 final Building a European Data Economy.
[30] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.
[31] See e.g. Hilty 92-93, Drexl et al. 2016 pp. 2.

in the end, weigh more. These are the dilemmas that make data such a complicated object to regulate efficiently.

2.4.1.2. Impediment on Competition

Similar to innovation, the competitive integrity of the EU internal market may suffer from too stiff regulation of non-personal data. It can reasonably be seen to create market entry barriers[32], making it more difficult or even impossible for new market operators and start-ups to enter certain fields. The cost of entry to an existing market might be simply too high for simple SMEs or start-ups to bear when the expenses surrounding Big Data analytics are taken into account. Moreover, certain markets would be nearly impossible to get into if the non-personal data was locked behind strict regulation.

Another point having to do with competition is that when assessing the need for the regulating of non-personal data, the competitiveness of the EU against its main rivals, namely the U.S. and China, could suffer greatly if the EU were to enact regulation of non-personal data. While the EU Commission has pondered the adoption of certain rights for data producers[33] in October of 2017, in the U.S., for example, there has not yet been any proposals or serious discussion that would have made their way through the legislative system to mirror the proposal in the EU.[34] The question then rightfully becomes, why should the EU be the first to dull its competitive edge in relation to the other industry-leading regimes around the globe?[35]

2.4.2. Sufficiency of the Current Environment

Lastly, it would seem proper to ask if we need to change anything at all. Does there not currently exist a flourishing data economy within the EU, with multiple working business models that are based on information alone? The current trend is to deal with the access to and the use of information using technical means, protecting any data deemed worth it and seeking to ensure the interests of the company through contractual means.

Technical protection often seems to lead to at least some level of factual exclusivity[36], that keeps the data in the hands of the company that "owns" it. The problems arise when this technical protection fails for one reason or another. But should that be a reason to regulate data?

[32] Drexl et al., 2016 pp. 2.
[33] COM2017a " at 13.
[34] Yu, 2019 pp. 864.
[35] Hilty, 2019 pp. 9.
[36] Drex et al., 2016 pp. 3.

Many companies seem to navigate the data economy quite proficiently, and thus it might seem like an exaggeration to create new ownership rights or try to conclusively define data to regulate it, as this would certainly cause a massive ripple across existing regulation and contractual environment.

With the freedom of contract being one of the chief principles in contract law, companies that deal with Big Data often seek to offer special licensing contracts, also known as data licensing agreements. The Court of Justice of the European Union (ECJ) ruled in its decision on *Ryanair v. PV Aviation*[37] in 2014 that the legal owner of a database that is protected under the *sui generis* right of the Database Directive has the right to control the "…purposes and the way of using that database or a copy thereof."[38]. However, licensing the use of Big Data is extremely tricky, and as such it often requires contracts beyond the traditional licensing agreements. Issues stem, for example, from the fact that it is often impossible to discern all the ways the data can be used, and what other data the licensee possesses and how that interacts with the licensed information.[39] Not only does the company have to be cautious not to give birth to a possible, more proficient competitor, but also be way of the licensing of information that would, after analyzing and combining, lead to personalization or re-personalization of the data, which could cause a potential disaster in public relations.

According to Aaron Tantleff, for example, the special provisions required from data licensing agreements should allow at least the following on the side of the licensor[40]:

1) Limiting the use of the database to include only anonymized data;
2) prohibiting the re-identification of any individual or combining data with any such database that would allow identifying individuals;
3) prohibiting the licensee from taking any actions based on the re-identified information or any other unwanted use;
4) requiring the licensee to give notification on any case of re-identification or the risk of thereof, and;
5) the ability to halt any activities involving the database immediately.

[37] Case C-30/14 *Ryanair v. PV Aviation*.
[38] ibid., para 43.
[39] Tantleff, 2015 pp. 14.
[40] ibid., pp. 15.

Whereas for licensees the main concern is their liability in case of any unwanted re-identification, and they should strive to make sure that the licensing agreement[41]:

1) Concerns only properly de-identified data, and complies with all the applicable privacy legislation;
2) has the rights to use the data in all the ways it deems necessary, and;
3) stipulates the possibility of the licensee to give a notification in case it discovers any re-identified data or suspects that, given the ways it aims to use the data, such re-identification would be at least highly probable.

It is important to include confidentiality clauses in such contracts, to ensure that the data remains undisclosed outside of the intended use of the licensee, and to keep any possible trade secrets under the (possible) protection of the Trade Secrets Directive.

2.4.3. The Difficulty of Defining Data

As was briefly discussed above, defining data in any meaningful way in legislation can be very complicated. We have the definition of both personal and non-personal data, courtesy of the EU. However, if the EU or any other legislative body would want to create rules concerning the ownership and B2B (Business-to-Business) protection of data, there would have to be clear definitions on what kind of data would demand ownership and protection. Clearly, it is not sensible to assume that all non-personal data should be owned or would benefit from some kind of protection of those ownership rights.

First of all, any legislation aiming to protect information, be it data or a more traditional form of information, should consider which levels of information does it seek to protect.[42] Traditionally, the structural level, or the "physical carrier" is protected already by traditional property rights, and as such, usually, by criminal law. Semantic data can fall within the parameters of database, trade secret, or patent protection. The syntactic level of data seems to be in the need of the most attention; outside of copyrights there does not seem to be many ways to protect the level of information most Big Data consists of. The choice of whether to protect data on the semantic or the syntactic level seems to depend on the context of both the data and the situation itself.[43]

[41] ibid.
[42] See e.g. Drexl, 2017 pp. 263.
[43] ibid.

Even within the level of data there should be some lines; not all syntactic data can or should receive protection or be the object of property rights. At best, it seems that these lines would be arbitrary and forced; at worst they would be meaningless compromises. On the one hand, creating too flexible legislation could, and most likely would, lead to courts spending the next decades pondering the exact categories of data that would qualify for protection. Meanwhile, new forms of data would be constantly being created. On the other hand, creating too complex, precise, and exhaustive legislation would most likely lead to confusion and market disturbances. Additionally, it would only be a matter of time until someone finds a technical way to circumvent exhaustive legislation, and it would most likely happen very rapidly; it seems impossible to create wordings that would account for all the possibilities within our current technical capability, let alone a few years from now. Impossible, that is, without creating blanket restrictions that would lead to their own issues, likely hampering many legitimate business models that depend on data as the basis for their commerce. Fascinatingly, it seems to always boil down to a very simple issue when discussing enacting technical legislation; developing legislation is slow, and technology develops very rapidly. This is why rules on the use of technology should always try to find a balance between what is a problem now, and what will most likely be a problem in the future. This, along with the fact that legislation often comes out as a result of political compromise, makes it very, very difficult to enact effective legislation when considering something as complex as a modern digital, data-driven society.

3. Protecting Industrial Data: The Current Legislation

This chapter goes over the current legislation available on the level of the European Union that concerns non-personal data directly or could be used to indirectly protect data that fulfills certain legal requirements. The last subchapter will try to give a more concrete example of how the EU legislation presents itself on the national level by going over the current Finnish implementation of the EU rules.

3.1. Brief Overview of the EU Framework

Industrial data, and non-personal data in general, is tricky. Since its ownership does not directly fall into a category of neither traditional property rights nor intellectual property rights, as it stands, there currently does not seem to be any protection for this kind of data as a whole.

In contracts and standardized terms and conditions this kind of data is often treated as an intellectual property right.[44] This, however, does not automatically place it within the scope of relevant protective legislation, such as the brand-new Copyright directive[45] or the older Database Directive[46] and Trade Secrets Directive[47]. As copyright is traditionally seen to only apply to "human-made" content, most of the industrial data will fall outside of the scope of these rules. The majority of the data available is generated as so-called "raw data", which has not and might not see a human interaction during the entirety of its life span.

However, it should be, in theory, possible for this kind of data to receive protection to some degree. Both the Trade Secrets Directive and the *sui generis*[48] -right of the Database Directive could, in certain situations and certain phases of the life cycle of the data, offer at least limited protection to industrial data. The next subchapters will discuss the possibility of protection under different options in the current legal framework of the EU, and finally taking an example from Finnish law.

3.2. The Database Directive

3.2.1. Scope and Industrial Data

Database Directive holds in its scope any information that is "…a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means."[49] A significant portion of the industrial data falls into this category; it is often stored in a cloud server or physical hard drives, in a way that allows a certain person, a customer, or the company holding the data to access parts of it individually. Whether or not the data is stored by the same party that produces it or the devices collecting the information, however, is a different matter.

While the database itself may qualify for copyright protection, it may not be relevant for the protection of the information stored within those databases. Moreover, these databases, mostly consisting of massive amounts of numbers, serial codes, and lines of code, are not usually

[44] Wiebe, 2017 pp. 63.
[45] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Not yet in force as of May 2019).
[46] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[47] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
[48] Database Directive, Art. 7.
[49] Database Directive, Article 1 para. 2.

compiled in a unique way. It is not cost-effective to come up with new ways to present data and store data in databases that are used daily. This does not, however, necessarily mean that the entirety of the Database Directive would be completely unusable in protecting industrial data.

3.2.2. The *Sui Generis* right

The true test for the industrial data comes with the conditions for the *sui generis* right laid out in the first paragraph of Article 7 of the Database Directive. It gives database owners the right to prevent re-use and acquisition of information from their databases. It reads as follows:

> *"Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."*[50]

The first obstacle is the requirement of a "substantial investment". While it can certainly be seen that a large amount of this kind of data would not exist without the vast amount of money poured into manufacturing and innovating the tools and devices that collect the data, it may not be enough. The Court of Justice of the European Union has held that the resources spent into the creating and generation of this kind of data are to be excluded when considering the substantiality of the investment.[51] This makes overcoming the substantiality requirement difficult in some cases, where the main part of the investment has been directed towards the "invention" of the data, such as calculating gambling odds.[52] However, it seems that the investment made to collect already existing information through, for example, sensors and other measurement devices, can be taken into account when considering substantiality.[53] It seems that ECJ wants to differentiate between completely "making up" data, and collecting and extracting data from a phenomenon that would be "free" for anyone in the right conditions and with the right tools. This puts industrial data, once again, in an awkward middle ground. On the other hand, it is mostly generated from existing natural phenomena such as weather, temperature, or even bodily functions. Yet, at the same time, a large portion of these phenomena are generated by human-made devices, such as vehicles, machines, and technology. If using the argument of "freely"

[50] ibid., Article 7 para. 1.
[51] e.g. ECJ C-338/02 *BHB v. William Hill* para. 31.
[52] See e.g. ECJ C-46/02 *Fixtures Marketing Ltd v. Oy Veikkaus Ab* paras. 34-49.
[53] Leistner, 2009 pp. 438.

available, existing data, such as temperature, should it make a difference if the sensors are on an open field, or inside someone's personal vehicle?

Secondly, the *sui generis* protection only applies if someone is re-using or extracting a *substantial* part of a database. It seems that protection provided by this article can be very limited, or even non-existent if the target of the data breach is only a small part of the database. Luckily, the provision allows for either quantitative or qualitative evaluation of the substantiality in this case. This essentially means, that the Court, when pondering the seriousness of the breach, can take into account not only *how large of a part* of the information was extracted, but *what* that part of the information was. In cases where a company that keeps vast databases of Big Data, most of which has value that is often difficult to determine, can get protection under the *sui generis* right. This would require the company to be the victim of a heavily targeted breach, extracting a handful of valuable data amounting to a fraction of the total volume of the database, if this information was the most crucial part of the database.

As with all things data, we have to consider the fact that the protection provided by the Database Directive will only apply to data stored within the confines of the EU. And while a healthy amount of data resides within the EU, the vast majority of company-controlled data is stored in "data havens", places which have a laxer regulatory environment. Today's reality is, that data moves around the globe in fractions of a second. It will be challenging to navigate a global legal framework, while in one part of the world a certain data set is protected, and in another it is not. A good example of this would be today's China and copyrights.

3.3. Trade Secrets and Know-How

3.3.1. Definition of the Trade Secret Directive

In June of 2016, the European Union passed the new Trade Secrets Directive[54]. This piece of legislation is a part of a larger operation undertaken by the EU Commission to create a better, more stable, and open Digital Single Market[55]. This has been an on-going trend internationally for several years, as all major economical players rush to ensure a safe environment for innovation.[56] Defining a trade secret is tricky. It is not an immaterial property right, yet neither is it a traditional property right.[57] One widely accepted definition is found in the treaties for Trade-

[54] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
[55] COM(2015) 192 final "Digital Single Market Initiative".
[56] Siebe, 2014 pp. 19.
[57] See e.g. Vapaavuori, 2019 pp. 38.

Related Aspects of Intellectual Property Rights (TRIPS) made by the World Trade Organization.[58] In fact, this definition was copied word for word in the new Trade Secrets Directive, as many other states have seen fit to do in the past.[59]

The new directive defines a trade secret in its article 2 as follows:

> "*(1) 'trade secret' means information which meets all of the following requirements:*
>
> *(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
>
> *(b) it has commercial value because it is secret;*
>
> *(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;"*[60]

As we are discussing the possibility of commercial sensory data receiving protection under the aforementioned directive, it is imperative to dig into the definition. Any data that fulfills these three requirements, should be and is considered a trade secret, and therefore it receives all of the relevant benefits. The next parts will consider each part of the definition in its turn.

3.3.2. Secrecy of the Information

The first requirement for the data to be defined as a trade secret is, that it is indeed a secret. This alone is not a difficult requirement – after all, that is why companies want their data protected. In an old, yet often cited case from 1969, *Coco v* Clark, the High Court of England and Wales stipulated that trade secret would need to be unknown, even if all its parts were known.[61] This sounds more complicated than it is. A simple example would be a recipe; anyone can reverse-engineer a product and know its contents, yet the recipe itself can still stay a secret. The requirement of secrecy also seems to be of a relative nature[62], which means that companies are still free to license their trade secrets, without losing the protection granted by the legislation. However, it seems that there would be a certain number of licenses to trade: At some point if

[58] TRIPS Article 39.
[59] Silva 2014, pp. 924.
[60] Trade Secrets Directive, art 2 (1).
[61] *Coco v. Clark,* 420.
[62] Silva 2014, pp. 928.

enough people become aware of it, the secret will enter the public domain and become generally known.[63]

All in all, the secrecy of the information is rarely an issue, as the assumption is that in order to need protection, you need to have something you want protected. In the case of data, specifically, right now it will not be unnecessarily difficult to reach the level of secrecy necessary to fulfill the first requirement of the Trade Secrets Directive. However, it will get more and more complicated to keep information secret, as our networking technologies and exposure on the internet will get more profound.[64] This could speed up the process of data being "generally known", without companies over-licensing their trade secrets.

3.3.3. Commercial Value that is Based on Secrecy

The second requirement of article 2 of the Trade Secrets Directive states, that in order to be considered a trade secret, information must possess commercial value due to the fact that it is kept secret. This imposes two separate requirements for any information looking for protection under this Directive; firstly, it must have commercial value, and secondly, this value must derive from the fact that this information is a secret.[65] The first of these criteria is not a great obstacle to the interpretation of industrial data as a trade secret, as aligning to what was stated earlier in this study, most data can be seen to have value.[66] Information is valuable; even if it is readily available, to those who wish to exploit it, often value can derive from the fact that someone has invested into gathering, organizing, and checking this information.

The latter of the two, however, cause some concern and lead to some data being restricted outside of the scope of this Directive. There are different ways to convey value; it can either be potential, or actual.[67] It feels quite redundant to only require potential value, however. Most existing information can be conceived to have at least some *potential* value, and thus it would in practice lead to not requiring any value at all.[68]

While there are no explicit mentions in the Directive on what the factual value for something to be considered a trade secret is, it can be assumed to be quite low, seeing as it fails to provide a description of the attached value. The courts seem to have accepted the *prima facie* evidence

[63] Silva 2014, pp. 929.
[64] See e.g. Wiebe, 2017 pp.65.
[65] See e.g. de Werra, 2010 pp. 158.
[66] See 2.2.1.
[67] Silva 2014, pp. 929.
[68] ibid.

of someone being willing to fight to protect their secrets to be enough to establish some value.[69] It seems that the monetary value of information is not supposed to be a significant hurdle in seeking protection against competitors in economic struggles.

3.3.4. Reasonable Steps to Keep the Secret

The third and final requirement posed by the Trade Secrets Directive states that in order for information to be considered a trade secret, the legal owner of the piece of information must have taken reasonable steps to keep it a secret from the parties who would seek to use it for their own ends. This seems to require that the legal owner actively is trying to hide the information from its competitors, and is quite vague in its wording, leaving a lot of room for interpretation. What exactly are "…*reasonable steps under the circumstances*…"[70]? It seems to strongly convey that some sort of a test of proportionality is in order to determine which measures fulfill these criteria, and which are found insufficient.[71] It would thus seem, that not all information requires equal effort for secrecy.

In the case of industrial data, this requirement can bring complications. As most of the Big Data and sensory data is merely kept on a server, secure or not, it may be deemed too frail an attempt to hold this information close. What could then be seen as a sufficient effort to keep the secret? Maybe the companies should restrict access to only internal networks. If that would be the case, the data that is stored on a cloud service would be in an awkward position. Would it then require a certain level of security on behalf of the service provider, or is the company expected not to store information on an external cloud service? All of these notions are interesting, and unfortunately as of now there is no detailed, comprehensive case law to support an opinion in either direction.

While there are no cases from the ECJ regarding the Trade Secrets Directive, it being a relatively young piece of legislation and the court system being relatively slow, there are some cases that bring guidance on what kind of measures could considered reasonable. Since the definition of the Trade Secrets Directive is merely a reflection of the much older TRIPS article, we can look for a direction in older literature. It seems that the protection of the trade secret must in fact be actual, and effective.[72] Therefore measures that have no actual effect on the secrecy of the information, regardless of their scale and investments made, are not enough to

[69] See e.g. Silva, 2014 pp. 930.
[70] Trade Secrets Directive, art 2 para. 1 (c).
[71] de Werra, 2010 pp. 159.
[72] Slaby et al., 1989 pp. 327.

warrant protection. It is not reasonable to expect companies to invest more in protecting a trade secret than the value of its secrecy.[73] In other words, if the damage of the secret getting out is measured to be a certain sum, the company cannot reasonably be asked to use more than that sum to keep the secret.

This requirement, while seeming rather ambiguous and open for interpretation, can play an important role as a filter through which the information has to go through to gain any type of protection. After all, not all company-owned data can be considered a trade secret[74], and it is sensible to limit the scope of the directive to information that the company actively tries to keep secret.

3.3.5. Sanctions under the Directive

Section 3 of the Trade Secrets Directive covers the repercussions that member states should make available in cases of misappropriation of trade secrets. Article 12 stipulates the requirement of having the possibility for the judicial authorities to order an injunction or other corrective measures. At the very least, according to the parts 1. and 2. of the article, member states need to ensure that the courts have the possibility to: a) halt the illicit use or disclosure of the protected information; b) prohibit the manufacturing, offering, use and sales of infringing goods; c) to recall, remove from the market or destroy the infringing goods, or to deprive them of their infringing properties, and; d) to order destruction, or delivery to the applicant, of the infringing documentation that holds the undisclosed information. Part 3. of the article holds and intriguing little detail, where it notes that the infringing goods can be ordered to be delivered either to the trade secret holder or to *charitable organizations*. The 4th part of the article states that the infringer will be the one bearing the cost of measures meant in points c) and d) of the first part. This should be without prejudice to any damages the infringing party is liable to pay for the illicit acquisition, use, or disclosing of the trade secret.[75]

Article 13 seeks to ensure that any measures taken by the authorities are proportional, as is traditional in any piece of EU legislation. It states that the authorities should take into account the following points when considering the proper measures: a) the value of the trade secret; b) measures taken to protect the secret; c) the way the infringer got hold of, used or disclosed the secret; d) the impact the illicit disclosure or use had; e) the current state of the parties and the impact the decision would have on them; f) interests of possible third parties; g) public interest

[73] Landes, Posner, 2003 pp. 369.
[74] See e.g. Halligan, Weynad, 2006 pp. 21.
[75] Trade Secrets Directive, article 12.

and h) fundamental rights.[76] All in all, the requirements are quite standard in any court consideration, with maybe the exception of point f).

Finally, article 14 considers damages. The judicial authorities in the member states will have the opportunity to order the infringing party to pay damages suffered by the injured party from the illicit use, disclosure, or acquisition of the trade secret. A requirement for the damages is that the infringer knew or should have known that they are acquiring the information illegally. The text notes that the member states may lower the liability of the employees working for the infringed party if the act was done unintentionally. Additionally, the amount of damages is subject to a consideration of all appropriate factors, also interestingly mentioning any "moral prejudice" caused to the legitimate trade secret holder. Authorities may also order the damages to be paid as a lump sum based on the situation where the infringer would have asked for a legitimate authorization to use the trade secret, mentioning at minimum any fees or royalties that the legitimate holder would have collected for the use.[77]

The sanctions imposed by the Trade Secrets Directive have been discussed further in the chapters 3.5.2 and 3.5.3 in the light of the Finnish implementation of the directive. The discussion is centered around the concept of using these sanctions to combat illicit use in the area of data.

3.4. Framework for the Free Flow of Non-personal Data Regulation

In October of 2018, the European Union passed the Framework for the Free Flow of Non-personal Data Regulation.[78] In its first article, it states that it "…aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localization requirements, the availability of data to competent authorities and the porting of data for professional users.".[79]

The regulation applies to the use of data other than personal data within the EU if it is;

1. Provided as a service to users that reside or have established within the EU, regardless of where the service provider is established or;
2. done by a natural or legal person residing or having established within the EU for its own needs.

[76] ibid., article 13.
[77] ibid., article 14.
[78] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.
[79] ibid., article 1.

In the case of a dataset consisting of both personal and non-personal data, the regulation only applies to the non-personal part of the dataset.[80] This is interesting, as it seems to imply that it would be easy, or even possible to separate such a dataset, as drawing a line between personal and non-personal information is often complicated, if not impossible.[81] The Framework for the Free Flow of Non-personal Data Regulation seems to err on the side of caution, however, as it stipulates that "…where personal and non-personal data are in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679."[82]. The mentioned Regulation (EU) 2016/679 is, of course, the General Data Protection Regulation (GDPR). However, this may cause its own issues. There are scenarios in which, for example, a piece of data changes from non-personal to personal. Are the relevant parties supposed to determine when, precisely, the information changed from non-personal to personal, and apply the relevant regime from that point onwards? It seems even more complex than conclusively identifying personal information amidst non-personal, especially given the dynamic nature of the definition of personal data.[83]

Another intriguing point in this regulation is found in the definition of non-personal data, where it opts to only refer to the "...data other than personal data as defined in point (1) of Regulation (EU) 2016/679.".[84] Another reference to the GDPR, and while it is elegant and completely feasible, it is still slightly surprising that the legislators would opt to use a negative, excluding definition.

In article 4 the regulation seeks to ensure the free movement of data within the Union by prohibiting data localization requirements, unless deemed necessary for public security and are in accordance with the principle of proportionality.

Article 5 stipulates that such data should be available for competent authorities, regardless of whether or not it resides in the same member state where the information is stored. It also ensures the possibility of obtaining such data, with the assistance of the competent authority in the relevant member state, as well as the possibility to impose repercussions for non-compliance.

[80] Article 2 (2).
[81] Graef et al. 2019 pp. 1.
[82] Article 2 (2).
[83] Graef et al. 2019 pp. 4.
[84] Article 3 (1).

The sixth article seems to be the most interesting one, at least from the perspective of businesses' interests. It lays down the rules concerning Porting of Data, also known as "data migration"[85]. The article states that the Commission will "encourage" and "facilitate" the adoption of self-regulating "codes of conduct" among the data service providers to ensure that "professional users", meaning both natural or legal persons (including public authorities) who use that information professionally, have the option to switch and compare between service providers, regardless of in which member state the service provider is established. The article calls for the codes of conduct to be effectively implemented by May 29th, 2020. This article is clearly meant to both increase the efficiency of the European data economy, and simultaneously to motivate service providers to invest and develop their products and infrastructure by allowing easy comparisons and the possibilities of shopping outside of your own member state.

By removing barriers between the member states, the commission seeks to ensure that the European data economy will remain competitive and streamlined while trying to maintain the "level playing field" the European Union is known to value within its borders. The effects of this regulation are yet to be seen, but at the time of the proposal, there were doubts as to its effectiveness, mainly concerning the attitude of the businesses.[86] Businesses like to keep their data as close to them geographically as possible. If there was trust in storing data beyond the borders of your home state, would it not already be the case? Only time will tell whether or not this along with other parts of the Digital Single Market Strategy will be enough to create a truly integrated European Data Economy.

3.5. Options Within the Finnish IPR Legislation

3.5.1. Introducing the Finnish Framework

While the Database Directive and Trade Secrets Directive do not directly provide us with remedies against unlawful breach of these intellectual property rights, they do require the Member States to provide such remedies in their respective national legislation.[87] While the implementation of Trade Secrets Directive is still in progress in many Member States, several have already enacted corresponding legislation. As a reference point, the Trade Secrets Act of Finland[88], which was enacted in August of 2018, will provide some insight into what these

[85] Data porting essentially means the process of selecting, extracting, preparing and transforming information, while permanently moving it to a new location.
[86] Broy, 2017 pp. 383.
[87] Database Directive, art 12, Trade Secrets Directive, art. 6 para 1.
[88] Liikesalaisuuslaki 595/2018.

remedies could look like. In the case of databases, the remedies are stipulated by the Finnish Copyright Act[89] , which will be reasonable to use as an example alongside the Trade Secrets Act.

Both the Trade Secrets Act and Copyright Act have divided the available remedies to civil law remedies, stated in the respective codes themselves, and criminal repercussions found in the Criminal Code of Finland. In this study, the criminal side of the possible outcomes will be left unconsidered, as the punishments listed in the Criminal Code are rather obvious and similar to the common criminal law repercussions. In the two acts, however, two of the basic civil law remedies seem to be available, and they are remarkably similar; injunctions against the continued use and spreading of the information[90], and damages and reimbursement[91]. In the Trade Secrets Act, there are a few more options than in the Copyright Act, mainly the possibility of a temporary injunction[92], and the possibility of collecting compensation for the illegal use of a trade secret.[93] As the remedies under the two Acts are quite similar, apart from the few peculiarities of the new Trade Secrets Act, it seems reasonable to not go through the remedies from the Acts separately, but to bundle them into holistic pictures under each remedy.

3.5.2. Injunctions Against the Illicit Use in Data Breaches

A classic among intellectual property remedies, the possibility of requesting an injunction from a court is an essential tool to combat the illicit use of the intellectual property.[94] It allows the plaintiff to request that the court issues an order to stop the misuse of the property and to refrain from engaging in it in the future. The provision of the Trade Secrets Act also includes the possibility of remedial actions to limit the damage done by illicit use of the trade secret.

In a recent study[95], at least one in five of the responding companies said that they have been the victims of corporate espionage or a cyber-attack. Chances are that the real numbers are higher, as getting companies to admit their vulnerability can be challenging. As useful as injunctions are in cases of misuse of the traditional intellectual property rights, it may not serve as well in a situation that involves a data breach. There are several reasons why this kind of remedy would be less effective in cases of cyber-attacks and thefts.

[89] Tekijänoikeuslaki 8.7.1961/404.
[90] Tekijänoikeuslaki 56g §, Liikesalaisuuslaki 8 §.
[91] Tekijänoikeuslaki 57 §, Liikesalaisuuslaki 11 §.
[92] Liikesalaisuuslaki 9 §.
[93] ibid., 10 §.
[94] See e.g. Vapaavuori, 2019 pp. 170.
[95] Baker McKenzie & Euromoney, 2017 pp. 3.

Firstly. it takes sometimes hours if not days for a company to notice that they have been a victim of corporate espionage or cyber-attacks.[96] It is not all flashing red lights, sirens, and pixelated skulls appearing on the company monitors, as Hollywood would have us believe. Sometimes these attacks are not noticed for months if at all. And months, days, and even hours might as well be years in today's world, where it takes mere seconds to transfer even massive amounts of data from one device or even continent to another. When the data breach is noticed, it is often too late to make use of an injunction; everything useful that a competitor could possibly extract from the data has already been taken, copied, re-copied and sent to a part of the world where there are very few, if any, rules against the misuse of intellectual property.

The second issue with injunctions against data theft is the same as in all things data; enforcing the decision once it's been made. How does a court make sure that the culprit has turned over and stopped using any and all parts of the illicitly gained data? In this day and age, it does not even take a physical device anymore; having sent the data to a secure location far outside of the jurisdiction of the competent court, the illicit user does not even need to physically hide a hard- or a flash drive. Naturally, the act of transferring the data is possible to detect using computer forensics, as the offenders are not the only ones who possess advanced modern-day technology. But how does the residing EU court force the data holders in another country, and possibly completely different legal system, to hand over the illegally obtained data and stop them from making copies of it? The answer usually is: with great difficulty.

In addition, there are multiple other reasons why companies would not pursue litigation in cyber-theft, such as embarrassment or like Zoe Argento put it in the title of her article in 2014, they simply do not want to "kill the golden goose"[97], and risk their trade secrets being made public in response to legal action. Furthermore, while the new EU Trade Secrets Directive demands secrecy in trade secret proceedings, it is not difficult to imagine mismanagement that would lead to accidental exposure of confidential information.

All of this is not to say that injunctions in data breaches would be a completely useless and antiquated tool; they can still bring the victim solace from many inconveniences. If the breach is detected quickly, and the perpetrator acts sluggishly, it is possible to stuff the proverbial cat back into the bag. An injunction against spreading the information can also be useful if done in time. And that is what matters; providing viable options for all severities of data breaches.

[96] Argento 2014 pp. 214.
[97] See title of Argento 2014.

The Finnish Trade Secrets Act, in addition to the traditional injunction, provides an opportunity to file for a temporary injunction. While the aforementioned typical injunction requires the breach of the right to have already happened, its temporary counterpart is more flexible; it allows the plaintiff to apply for an injunction against a breach that has either happened or is *imminent*. The provision gives more breathing room in other areas as well; it only requires the plaintiff to show that it is *probable* that the trade secret exists and that they are the legal owner of the information.[98] Needless to say, in cases of data breaches, that were discussed to be extremely time-sensitive, the possibility of seeking an injunction against an imminent threat can make all the difference. Temporary injunctions are meant to serve as a quick remedy during the legal proceedings, after which they are either lifted or changed into a regular injunction. The need for this type of speedy action is brought up in recital 26 of the Trade Secrets Directive.

3.5.3. Damages and reimbursement in Data Breaches

Damages are another classic form of civil law remedy. Intellectual property rights, in this case database holders' rights and trade secrets, are no exception; it is possible to seek damages for the financial losses suffered as the result of the illicit use and reimbursement for the use of the secret information.

The Finnish Trade Secrets Act allows the collection of compensation for the illicit use of the secret information. It is a new remedy in Finnish law, and quite irregular.[99] It is found in the Trade Secrets Directive, and thus required to be implemented into national law.[100] It requires that the defendant has already used the secret, and that they have done so in good faith; not knowing and not even being supposed to know, that what they were engaging in was illegal. It also requires separate consideration of discretion from the court. This provision allows the defendant, provided that all the aforementioned conditions are fulfilled, to demand that they are allowed to continue using the information that has been defined as a trade secret, provided that they pay the plaintiff reasonable compensation for the use of the said information. Here we have a kind of forced license[101], a counter-remedy, or maybe even a defense, that is supposed to protect a defendant who acted in good faith. One has to imagine, that the situations in which this provision would apply, are rare; it is difficult to come across secret information, in good faith, that would be readily available to be exploited unknowingly. Even after checking all the

[98] Vapaavuori 2019, pp. 174.
[99] ibid.
[100] Trade Secrets Directive article 14.
[101] Vapaavuori, 2019 pp 174.

boxes in the Act provides, it is still up to the court, which makes a decision based on the holistic deliberation on the facts in every individual case.[102]

In terms of being useful in cases of data breaches, damages are somewhat more consistent than injunctions. After all, it is often easy to see that some form of damage has been done. As is often the case with damages, the issues stem from the specific amount of damages granted. It is often difficult or even impossible to evaluate the damage caused by a data breach or the loss or spreading of a certain trade secret; after all, the information does not usually have an exact monetary value. There are naturally methods to estimate its value[103], but they will most likely be just that: estimations. And estimations are often subject to interpretation, which is even more true in the case of data; what is one bit worth? Data breaches will most likely benefit from a qualitative rather than quantitative approach when it comes to the estimation of monetary value; *how much* often matters less than *what*.

It is worth noting that national courts and even the ECJ often lack the authority to enforce damages outside of their jurisdiction; in this regard, the issues mirror those discussed regarding injunctions.

As injunctions, damages are nowhere near useless in cases of data breaches. While the largest issue might be the evaluation of the damage caused by the data breach, it is still preferable to receiving nothing at all. Damages and injunctions often go hand in hand in the legal proceedings, the plaintiffs usually opting to apply for both. While the injunctions are highly time-sensitive in cases involving data breaches, the damages are often more lenient in this regard; when it is too late for an injunction to grant any benefits, damages might help to mitigate the financial loss.

3.6. Concluding on the Current Situation

As it stands, there are no real catch-all mechanisms in place to protect non-personal data in the European Union. It is difficult to say for certain whether or not data qualify to receive any kind of protection in the current sphere of EU legislation, and it seems that the only way to be positive is to test the data in court.

While both the Database Directive and the Trade Secrets Directive may offer limited protection in some cases, neither of them is excellently equipped to handle data breaches and cyber-

[102] ibid.
[103] See for example the Cash Flow Method in Halligen, 2006 pp. 19.

attacks. More hope seems to be found in the direction of trade secrets, and indeed it seems like non-personal data might find some moderate protection in some cases, provided that it is seen to fit the definition of a trade secret in the under the new directive.

Meeting the requirements for trade secret protection for non-personal data may prove challenging. For those seeking to protect their industrial data, the main causes of headache are the requirement of commercial value due to secrecy and the requirement of taking reasonable steps to keep the information secret. It should, however, be noted, that the directive is not aimed to provide data protection or to affect specifically the data economy in any way.[104]

If the information is seen to fall under the umbrella of trade secret protection, the remedies may still not prove effective at containing the damage caused by the misappropriation. Injunctions will often be too little too late, even though there is some hope if the breach is detected quickly and the perpetrator resides within the victim's domicile, or the vicinity of, and is acting somewhat slowly. In cases like these threatening legal action is often enough, and the incident is handled outside of the courtroom, usually by parties' respective lawyers.

Damages seem to be a somewhat more useful tool for acquiring back some of the lost value caused by misappropriation of a trade secret. Under the new directive, it is possible for the courts to order the illicit user to pay for the use of the information, akin to any royalties or fees that would have to have been paid in a legitimate scenario. This kind of "forced leasing" would likely not be a popular demand by the injured party, but its existence is an indication that legislators are trying to make intellectual property remedies more flexible.

Within the EU legal sphere, the Framework for the Free Flow of Non-personal Data in the European Union regulation seems to offer a source to find definitions for when trying to nail down what is non-personal data. This directive faces the same issue that has been around since the dawn of popularization of the internet; what is and what is not, in fact, personal data? The directive seeks to use a negative definition, ruling out all the data that falls into the definition found in GDPR as personal. However, it seems that the fluidity of data and the fact that context can make certain data personal despite its inherently non-personal nature, this will not be an easy question to solve. In this regard it is like many other dilemmas surrounding information in the modern digital age.

[104] Drexl et al., 2016 pp. 7.

4. Comparing EU and U.S. Approaches: A Short Review

This chapter takes the issues discussed in the previous chapters across the pond and aims to provide a brief overview of the current workings and simplified history of trade secrets legislation in the United States and to compare it to the situation in the EU. Trade secrets were chosen as the focal point of the comparison, because out of the current EU legislation the Trade Secrets Directive seems to be the best bet to protect the kind of data explored in this study, and it could be beneficial to seek inspiration from across the Atlantic.

4.1.A Brief History of Trade Secret Legislation in the U.S.

History is an important part of how we interpret legislation today, especially so in common law legal systems such as the one in the United States. While it is often imperative to keep in mind the origins of any given piece of legislation, it seems like unfair competition laws, and trade secrets as a part of that sphere, are especially clearly a product of their time. All legislation mirrors somewhat the values and the atmosphere of its time, and those in turn affect deeply the processes behind drafting laws. All that said, the road which led the United States trade secrets legislation to get where it is today is a remarkably interesting one and is crucial in order to understand why the law took on the form it has, and why so many legislative bodies around the world saw fit to use it as a base for their own trade secrets codes. The following is a broad strokes-version of the history of trade secret legislation in the United States.

From 1837, when the courts made their first acknowledgment of trade secrets in the United States, to 1939 the trade secrets litigation was largely based on case law, and wholly in the hands of state courts.[105] Of course, the trade secrets were not invented by the United States state courts in 1837; it was merely the first occasion when the courts could draw upon already existing English case law. After a while, what formed was somewhat clear guidelines for dealing with trade secrets in several states. However, there were several glaring issues: firstly, the inconsistency. While some states had comprehensive case law regarding trade secret protection, it was widely varied. Some states had next to nothing to draw upon, and even more had only a very patchwork environment in which to litigate. Secondly, there was a problem in limiting the scope of trade secret protection to only concern information that was actually a secret, and not all business information.

[105] Sandeen, 2010 pp. 498.

In 1938, the U.S. Supreme Court ruled in its historical case of *Erie Railroad Co. v. Tompkins* that there is no "federal common law".[106] This led to even more consistency issues with trade secrets protection, as it was largely based on regional case law. In 1939, the American Law Institute published the Restatement (first) of Torts, volume IV (Restatement First). This was a sort of codification of the existing state court common law, and it served as the primary guide to which American litigators would refer to in case of trade secrets law until roughly the year 1988.

The pressure to enact federal law concerning trade secrets became apparent in 1964, with cases *Sears, Roebuck & Co. v. Stiffel Co.*[107] , and *Compco Corp. v. Day-Brite Lighting, Inc.*[108] the U.S. Supreme Court ruled that state unfair competition law was preempted by the federal patent law.[109] This effectively prevented state courts from developing unfair competition law that was conflicting with federal patent law.

Before its adoption in 1979, the Uniform Trade Secrets Act (UTSA) went through a multitude of different iterations and drafts. It was worked on by a committee consisting of over 36 professional associations[110] that started its work in 1966. UTSA received its first reading in 1972 in the form of the Seventh Working Draft. In 1979 it finally was approved by the National Conference of Commissioners on Uniform State Laws. Therefore, the version approved in 1979 was a fruit of over 13 years of research and labor.

The UTSA aimed to solve the issues and fill the gaps in common law trade secrets protection. It was not meant to be a mere codification of the case law, but a comprehensive source for litigating trade secret cases. The issues it was seeking to solve or give answers to were, in short, the following: firstly, to comprehensively define a trade secret. Until the adoption of UTSA, the Restatement First had been the primary source, and it contained six qualifications of which a piece of information had to fulfill one of to be considered a trade secret. For UTSA, the committee came up with the now so familiar three requirements; information in question had to be an actual secret, that the owner of the secret had to have taken measures to keep as such, and that the information had to derive value from being a secret. The second issue was to exclude non-trade secret business information from the scope of the protection. This was partly done with the addition of the definition discussed previously. Third, the claimant would now have to

[106] *Erie R. Co. v. Tompkins*, 304 U. S. 64 (1938).
[107] *Compco Corp.* v. *Day-Brite Lighting, Inc.,* 376 U. S. 234 (1964).
[108] *Sears, Roebuck & Co. v. Stiffel Co*., 376 U. S. 225 (1964).
[109] Sandeen, 2010 pp. 507.
[110] ibid., pp. 509.

prove both the existence of a trade secret and the violation. Fourth, the new bill focused on the cohesion of the remedy system, both in scope and availability. Fifth, and perhaps most importantly after the definition itself, were the important protective orders that the court could give during the trial. And lastly, the preempting of other types of theories of liability, stemming for example from criminal law.[111]

While the UTSA was adopted originally in 1979, its implementation into force was slow, and during the transition, the Restatement First was still widely used. UTSA was amended as early as in 1985, and after the amendments, it started to slowly gain ground as the primary source of trade secret law. The act is a testament to the hard work of many determined judges, academics, and practicing lawyers, and perhaps this helps to explain why it was so widely borrowed in other legal systems. It is said to "…reflect the important balance that – in theory – all intellectual property laws should have: a balance between IP protection on one hand and free competition in the other."[112]

The road for trade secrets legislation in the U.S. has been a rocky one, and that is largely due to the differences of opinion among those that were drafting it. Designing legislation is always a political process, but this was perhaps amplified in the making of what ended up being UTSA. Next, we will take a look at the current federal trade secrets legislation in the U.S.

4.2. Current Trade Secrets Legislation in the U.S.

4.2.1. The Relevance of U.S. Law

The United States legal system differs fundamentally from any individual European system – the most similar, yet still different, is the United Kingdom's legal environment. Why, then, is it a relevant choice of comparison to the EU Trade Secrets system, as it is typically common to use something more akin to our own situation?

There are similarities in how the legislation is structured within the U.S. and the EU. Both are "coalitions" formed from multiple individual legal spheres, and the priority rules of U.S. federal law and the EU regulations and directives are strikingly similar. Both take precedence in certain areas of law while leaving the areas not specifically assigned to them to be a worry for the individual states and member states. Another common trait is that both the EU legislation as a whole and the U.S. are largely driven by the decisions of their respective courts, the Court of

[111] ibid. pp. 515.
[112] Sandeen, 2010 pp. 543.

Justice of the European Union in the EU, and the Supreme Court of the United States in the U.S. holding the highest authority and the other appellate courts working both in individual states and at the federal level. While ECJ has not been officially named as the "highest step" on the stages of the appeal process, it has become increasingly popular for national courts to use the opportunity to ask for a preliminary ruling[113] from the ECJ. The number of preliminary rulings has more than doubled between the years 2008 and 2018[114], though it can partially be explained by the fact that the EU legislation has become increasingly more prevalent and complex. On the other hand, more and more cases are tried in the national courts citing EU law directly, which obviously leads to more issues concerning specifically EU-law.

4.2.2. The Uniform Trade Secrets Act

The trade secret legislation is a particularly intriguing point of comparison between the EU and the U.S. systems, as the definitions for trade secret found in Uniform Trade Secrets Act and the Trade Secrets Directive are remarkably similar:

> *"(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:*
>
> *(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and*
>
> *(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy"*[115]

Compare this to the new Trade Secrets Directive definition of a trade secret:

> "*(1) 'trade secret' means information which meets all of the following requirements:*
>
> *(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
>
> *(b) it has commercial value because it is secret;*

[113] TEU, article 19.
[114] Court of Justice of the European Union, PRESS RELEASE NO 39/19 pp. 1.
[115] U.S.C. § 1839 1 (4) Uniform Trade Secrets Act of 1979 with 1985 amendments.

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;"[116]

While the phrasings and word choices are different, and the definition in Trade Secrets Directive has the (i) of UTSA is split into two points (a) and (b), the content boils down to the same three requirements (also found in TRIPS[117]); the information needs to be a secret, worth more because it is a secret and the holder has to have taken certain measures to keep the secret.

This, of course, means that the U.S. system of trade secret protection faces very similar issues as the EU system; how much commercial value is required to fill the criteria; to whom must the secret be valuable; what substitute as acceptable measures taken to try and keep the information a secret. This is, consequently, why we can compare the trade secrets legislation and its handling in the courts between the EU and the U.S., and have it yield fruitful information.

4.2.3. The Economic Espionage Act

Trade secret theft in the U.S. is criminalized under the Economic Espionage Act of 1996 (EEA). EEA defines trade secrets somewhat similarly to the Trade Secrets Directive and the UTSA:

"The term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

''(A) the owner thereof has taken reasonable measures to keep such information secret; and

''(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public"[118]

There are two notable distinctions between the EEA definition and the definitions of UTSA and Trade Secrets Directive[119]; first, the EEA requires storing of the in a form where it is tangible,

[116] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, article 2.
[117] Trade-Related Aspects of Intellectual Property Rights -agreement article, 39 2.
[118] U.S.C. § 1839 (3) Economic Espionage Act of 1996.
[119] Johnson 2010, pp. 555.

such as a computer drive or a stack of papers; second, the EEA only requires the public to be unaware of the information for it to constitute as a "secret".

Deviating definitions between UTSA and EEA are fascinating, seeing as, for example, in the Finnish Criminal Code, a trade secret is merely defined by referencing the relevant part of the Finnish Trade Secrets Act.[120] It would seem that EEA has a more lax definition on the one hand, as information is a secret so long as the public is not aware of it, but a more strict in the other, as it requires a more tangible form of data. This would increase the risk of differentiating and confusing decisions within the courts, furthering the air of uncertainty that often follows trade secrets no matter the jurisdiction, which has indeed been the case.[121]

4.2.4. Defend Trade Secrets Act

United States Defend Trade Secrets Act (DTSA) is the newest line of defense for trade secrets in the U.S. It was signed into force by President Obama in 2016 and is meant to allow civil action against misappropriation of trade secrets related to a product or service that is used or meant to be used in commerce that passes state lines or has foreign ties.[122] The act is meant to supplement the existing Economic Espionage Act, which had previously allowed for criminal action in such cases.[123] DTSA uses a very similar definition of a trade secret compared to UTSA, and the definition of misappropriation is identical.[124] It is curious, as noted above when discussing the Economic Espionage Act, that the definition of a trade secret found in UTSA differs from the one in EEA. DTSA differs from UTSA in multiple ways: it has the requirement of interstate or foreign commerce[125]; it allows *ex parte* civil seizure of infringing goods, in other words without requiring the presence of the misappropriating party, which means that the trade secret holder has a possibility to respond to an infringement rather quickly[126]; it protects whistleblowers[127] and lastly, it applies to misappropriation outside of the U.S.[128]

The Act is clearly meant to give American companies tools to combat the theft of trade secrets and the misappropriation that happens outside of the United States. However, it seems unlikely that this legislation will have a meaningful impact on cyber-theft and trade secrets leaking

[120] Rikoslaki 30:11 §.
[121] Johnson 2010 pp. 556.
[122] 18 U.S.C. § 1832 (a), Desai 2018 pp. 492.
[123] Goldman, 2016.
[124] Desai 2018 pp 492.
[125] U.S.C. § 1832 (a).
[126] Cohen et al. 2016 pp. 2.
[127] U.S.C. § 1833 (b), U.S.C § 1837.
[128] U.S.C. § 1837.

outside of the United States. Companies are unlikely to sue a cyber-theft for a multitude of reasons, especially if it originated outside of their domicile.[129] In most cases, it is simply not worth the effort.

Out of all the legislative sources of trade secrets legislation in the U.S., the DTSA is the most similar to the current Trade Secrets Directive in the EU. It would be shorter to list the differences between the two than the similarities, as both, for example, provide whistleblower protection (Directive slightly wider than DTSA)[130] and seek to protect employees[131]. A significant difference comes with the fact that while the DTSA does not include criminal provisions, it is possible to seek them through the Economic Espionage Act.[132] The directive does not require member states to enact criminal punishments for trade secrets misappropriation, though they may do so. The illicit use, acquisition, and disclosure of trade secrets have been criminalized in many member states within the EU, many of them long before the enactment of the directive. For example, in Finland it has been included in the criminal code since the 1970s.

4.3. Comparing U.S. and EU Trade Secret Definitions

In the United States, as it is everywhere in the world, the recent advancement of technological playfield has brought with it concerns regarding the protection of both private data and machine-generated, non-personal data. In 2018, the U.S. was dominating the world market in terms of data.[133] However, it has not yet seen fit to follow the EU in proposing any kind of allocation of ownership for non-personal data.[134] U.S. companies face difficulties similar to the ones present in the EU under the new Trade Secrets Directive, due to the fact that the wordings which define a trade secret are very close to each other.

The main questions when considering whether or not a piece of data can receive protection as a trade secret in civil law courts are the same, on the account of the UTSA provision defining a trade secret: was the information a secret, does it derive value from its secrecy and what steps have been taken to keep the secret?

The EEA definition would seem to better facilitate its use in the case of data by diversifying the information that could constitute a trade secret and by only requiring the information to have

[129] Argento, 2014 pp. 214.
[130] Desai, 2018, pp. 495.
[131] ibid., pp. 495-496.
[132] ibid., pp. 502.
[133] See e.g. Hilty, 2018 pp. 85.
[134] Yu, 2019 pp. 864.

been a secret from the public. It is interesting that the criminal law definition is much wider than its civil law counterpart. The UTSA only seems to allow remedies in cases where the object of the misappropriation included "…a formula, pattern, compilation, program, device, method, technique, or process…"[135], whereas the EEA allows for "…all forms and types of financial, business, scientific, technical, economic, or engineering information…"[136]. Needless to say, the EEA definition is preferable for someone seeking to prove that their data was, in fact, a trade secret. In this sense, it is much more similar to the definition in the Trade Secrets Directive, which only uses the word "information". It would seem that while the U.S. civil law is limited in its ability to facilitate data, the criminal code seems to be far more suited for it.

The question of value is left somewhat vague both in the EU and U.S. legislation. Both UTSA and EEA have the requirement of "independent" economic value, while the Trade Secrets Directive is worded to protect information with "commercial value". All of the codes require the value to derive from the secrecy of the information. In the EU, there has been speculation whether this would mean factual value, or if potential value[137] would be sufficient. It would seem, that UTSA allows potential value[138]. From the wording of the directive, this is not immediately clear. However, on the 14th recital the directive specifically mentions that "…such know-how or information should have commercial value, whether actual or potential."[139]. In the case of the U.S. civil law, value can be shown in more or less two ways: either by showing that the trade secret would bring an actual competitive edge, or by producing evidence that investments went into either creation or hiding of the secret, or that others were willing to pay license fees to use it.[140] As the EU legislation is relatively new, only required to have been implemented in 2018, and the court system is quite slow, there is little case law regarding the new legislation. However, there is, for example, a case from the Finnish system: a ruling from the Court of Appeals in Helsinki where the court states that in regards to trade secrets, all consideration should be done as "objective consideration from the perspective of the trade secret holder".[141] While this statement is meant to concern the trade secret consideration as a whole, it would suggest that, at least in the Finnish legal system, information needs to have objective value from the perspective of the secret holder to be considered a trade secret. When it comes to non-personal data, both the U.S. and the EU regimes have their uncertainties, perhaps more

[135] U.S.C. § 1839 1 (4).
[136] U.S.C. § 1839 (3).
[137] For example, de Werra, 2010 pp. 158.
[138] Sandeen, 2011 pp. 556.
[139] Trade Secrets Directive, recital 14.
[140] Green, 2015 pp. 188-189.
[141] Helsingin HO 16.2.2018, dnro R 16/1956.

so on the side of the EU, in the absence of relevant case law. It will be intriguing and exciting to see what the ECJ will consider when determining the value criterion of the Trade Secrets Directive. In the end, this may not be the deciding requirement for a lot of cases; if the data did not have significant value, businesses would hardly pursue litigation.

The final criterion of the trade secret definition is the requirement to take reasonable steps to keep the information, or data, a secret. None of the trade secret codes directly define what constitutes reasonable efforts. EEA, UTSA, and the Trade Secrets Directive all use the word "reasonable". It seems that it has been left up to the courts to specify what is and what is not reasonable, though it makes sense to tie the requirement into the context of the case.[142] These efforts should at least be objective[143] and actual[144]. Because this requirement is based on the facts of each individual case, it is extremely difficult to tell whether measures taken are sufficient to trigger protection.[145]

All in all, protection for data seems to have similar hurdles in the U.S. trade secret legislation as it does in its EU counterpart. The notable exception seems to be the narrower requirement of the nature of the information in UTSA. However, it should be noted that this study has no thorough exploration of the U.S. case law, as it feels that it would require a study of its own, which could provide more insight on how the requirements are handled in practice.

5. Possible Ways Forward in the Protection of Non-Personal Data

This chapter aims to provide some measure of possible paths forward through legislation, or through non-binding measures in protecting non-personal data. It seeks to give some examples of what has been discussed in the literature, on the legislative level of the EU. Also noteworthy is that while this study focuses on non-personal data, there has been similar discussion with regards to personal data. Three different avenues have been chosen for discussion in this chapter; defining data ownership, the Commission proposed data producer's right and possible non-legislative, "soft law" approaches.

[142] Sandeen, 2011 pp. 557, Green, 2015 pp. 192.
[143] de Werra, 2010 pp. 159.
[144] Slaby et al., 1989 pp. 327.
[145] Green, 2015 pp. 192.

5.1. Legislating Data Ownership

5.1.1. Possible Justifications for Data Ownership

Traditionally, intellectual property rights seek to incentivize innovation and creation. However, in the case of data, it is not as clear-cut. To create a definite classification of ownership, some justifications should be found for as to why is such a right even required. This chapter will consider six possible reasonings for data ownership:

1. incentives to collect or generate data;
2. stability for data transactions;
3. legal stability, or legal certainty;
4. incentives to commercialize data;
5. enhancing access through ownership, and;
6. the tragedy of the anticommons.

The first possible justification for data ownership would be if such a right would incentivize businesses or individuals to create or collect non-personal data.[146] However, most of this kind of data is a by-product of a machine, process, or a device that the potential rightsholder would be using either way, regardless of whether or not there is legal protection in place. It seems that this claim can be made quite safely, as there currently are no legal protection mechanisms, and clearly, this kind of data is already being generated and collected for both for economic purposes such as sale or licensing, and the manufacturer's own purposes such as research and development or maintenance. It seems clear that it would be difficult to justify a new property right; however, it is impossible to be certain that it would not change the data economy in any meaningful way.[147] As such it does not seem reasonable to cast this justification aside outright as moot.

Secondly, creating a clear doctrine of data ownership could bring stability to the transactions that involve non-personal data in some way, such as sale as-is or licensing of a database. The idea is that robust definitive ownership rights on data would increase the volume of data-related transactions. It should be noted that it cannot, however, provide any aid in the case of data being classified as a trade secret.[148] It is not inherently prohibited to use trade secrets, the new Trade Secrets Directive can be invoked only in the cases when the trade secret was acquired

[146] See Drexl, 2017 pp. 273.
[147] Wiebe, 2017 pp. 67.
[148] Drexl, 2017 pp. 275.

unlawfully.[149] As such, every transaction involving trade secrets inherently makes it more likely that the secret will be disclosed and consequently lawfully acquired.

Third, legal certainty is possibly the strongest argument for data rights, and its content mirrors that of the similar argument concerning data protection discussed earlier in chapter 2.2.2. From an economic standpoint, there has long been a discussion on the effects of uncertainty on investing resources.[150] The market for data definitely already exists, and a legal right would increase the efficiency of the data economy by unifying the rules for all stakeholders, no matter the size or market share. This would lead to more certainty and transparency towards the beneficiaries of non-personal data.[151] However, this argument is not necessarily very convincing. It would, most likely, lead to an influx of litigation relating to the new right, whether it be in national courts or on the EU level.[152] At the same time, since everything data-related is currently so unclear, creating a property right may only serve to increase the risk of unintentional breaches of rights, which might cause businesses to be even more careful with their investments in data analytics and datasets.

Fourth, it should be explored whether or not exclusive data rights would incentivize commercializing data. The economic theory that is known as "prospect theory"[153] states that by patenting an innovation before it is even properly developed, patents are "prospects".[154] While the theory is constructed around patents, it is quite accurate in many cases of data; investments are often needed after the subject of the potential protection (data) has been created or collected. Most often this is merely the beginning. Granting the ownership right to the original creator of the data might bring more profits to the original creator. However, it seems that this justification is quite weak in the case of the data economy. Often, the company that holds the data does not need to be afraid of competition in the commercialization of their data, as it is often licensed to be commercialized by someone else.[155]

Fifth, there is also a backward-sounding idea that allocating property rights for data will, in fact, enhance the access to data. This notion is interesting, and a related discussion has been had in

[149] On the definition of lawful acquisition, see Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, article 3.
[150] See for example Arrow, 1962 pp. 610-614.
[151] Wiebe, 2017 pp. 67.
[152] Drexl, 2017 pp. 275.
[153] More on prospect theory generally see Kitch, 1977 "The Nature and Function of the Patent System".
[154] Spulber, 2015 pp. 277.
[155] Drexl, 2017 pp. 274.

the case of *UsedSoft GmbH. v. Oracle International Corp*[156]. In it, the Court stipulated that by downloading, or buying a physical copy of, a licensed software (in this case provided by Oracle) the person who acquired the software becomes the owner of the copy.[157] The Court is effectively limiting copyright to promote the free flow of data in the form of a more free circulation of computer software.[158] Unfortunately (or fortunately, depending on the perspective), the Court has limited[159] this judgment to be applicable only on the case of "exhaustion rule"[160] in the Computer Programs Directive. However, it does offer a compelling precedent where the Court has proven that by broadening the concept of ownership in intellectual property rights, it can do it with beneficial effects on the free flow of data. It has also been discussed whether or not this means that any "digital content", including data, could have its ownership transferred.[161] Transferring ownership is, of course, a part of classic property rights. It should, however, be noted that the Court has limited the use of *UsedSoft* in their decision *C-166/15 Ranks and Vasiļevičs* in 2016, where it stipulated that while the exhaustion rule does concern the copies of a legally acquired computer software, the lawful acquirer has to make the copy in his possession unusable at the time of the sale of the reproduced copy in order to avoid copyright infringement.[162] This, while a sensible conclusion, means that the effect on the free flow of data is not incredibly wide.

Finally, the "tragedy of the anticommons"[163]. This means the situation where the number of property rights and property holders is simply too vast to effectively or even successfully use the property. It is somewhat related to the issue of defining data itself; if property rights were to be attached to all, or even a significant portion of the non-personal data, it could easily lead to a situation where it would become nigh impossible to separate all the property rights controlling any given piece of data. This is, however, more or less the situation under the current data leasing contracts, many of which contain differentiating clauses and guarantees, that overlap through the many analytic steps and the meshing of different databases. Somewhere, on the Nth step of the value chain[164], the piece of data could have so many overlapping property rights

[156] *C-128/11 UsedSoft GmbH. v. Oracle International Corp.*
[157] ibid., paras 45-52.
[158] Drexl, 2017 pp. 271.
[159] *C-128/11 UsedSoft GmbH. v. Oracle International Corp.*, para 63.
[160] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, article 4 (2).
[161] See for example De Franceschi and Lehmann, 2014.
[162] *C-166/15 - Ranks and Vasiļevičs*, para 55.
[163] Stepanov, 2020 pp. 79.
[164] For more on value chains, see for example Drexl, 2017 pp. 264.

attached to it that it cannot serve its intended purpose. It could be argued, that this could somewhat be untangled by clear, legislative approaches.

While the justification for the ownership of data is a topic that has been discussed widely in different legislative spheres, both in literature and at the governmental level, it does not seem that anyone has come to a definite conclusion whether it would be cause for more trouble and turmoil than it is worth. There are well-argued points in both corners, and it will be interesting to see which regime will be the first to enact laws that govern data ownership, if any. One would imagine that, as discussed above unless the ownership was done in a way that would harmonize it across the globe, the first implementor would have to take a massive risk in regard to their competitiveness in the market. As such, we might be stuck for years to come be in an international game of "chicken", where all governments wait for others to act first.

5.1.2. Possible Drawbacks from Granting Data Ownership

There have been numerous arguments against drafting legislation granting ownership of non-personal data. Many of them mirror the arguments against protective legislation, as it is indeed almost inevitable that the "owner" of data would be legally defined before any protection could be enacted. It seems fruitless to repeat the arguments already found in the second chapter of this study in their entirety. However, there are several perspectives that have not been discussed, as it did not seem quite appropriate in the context of protective legislation. Three such arguments will be discussed:

1. A lack of legal principles;
2. the problem of allocation, and;
3. practical problems.

First, it has been argued that there is no legal principle on which the need for ownership allocation of data could be based.[165] Essentially, this idea opposes both the broadening of the personal data protection of market data and the notion that the ownership of data generated by sensors should be allocated to the owners of the appliances which house those sensors. This argument may not be exactly correct, however. As was discussed above, in context with the *UsedSoft* -case, it could be seen as ECJ granting "digital content" some measure of property rights, namely the right to transfer ownership.[166] This, along with Commission's idea to bring

[165] Drexl et al., 2016 pp. 2.
[166] *Supra* 142; De Franceschi and Leeman, 2016 pp. 61.

the "data producer's right" [167] to EU law, it would seem that EU is planning to move towards a more clear legal framework, where data could be treated more like a traditional good in terms of classic property rights and contract law.[168] Time will tell whether or not this will be the right course of action to take, as it is nearly impossible to predict the effects of such changes on the market, and how the data economy itself will transform in the future.

The second argument against data rights is the problem of allocating data ownership.[169] This issue has been briefly discussed in chapter 2.2.3., but as it is a fascinating problem especially in the light of non-personal, sensor-generated data, it seems to warrant consideration in its own right. The core of the problem is this: if a legislator were to enact laws that would govern the ownership of such data, who would these laws allocate the ownership to? As mentioned earlier in the study, there are multiple answers to this question; for example, both the owner of the device that collects the data and the manufacturer of the said device have somewhat of a strong claim on the data. The owner of the device, i.e. smartphone or a smart car, is the one who conducts the activity that leads to the generation of the data. They are the one who drives the car or browses the internet with the phone. As the data is the result of their actions, would it not make sense to grant ownership to them? The manufacturer would also seem to have a rightful claim on the data; their patents, research and development, and production costs have already been invested into the product.

This question would be especially critical in joint investments where one party manufactures the machine, and the other uses it to create products. This is more or less the intention of the proposed data producer's right.[170] This proposed right will be explored more in chapter 5.2. Namely the allocation problem is to be solved by taking "…into the account the investments done, and the resources put into the creation of the data."[171]. Also, the possibility of "joint rights" by default is considered, with freedom of contract allowing differentiation from this rule.[172] It seems that joint ownership of the data would complicate things, and one would assume that the parties would seek to allocate the ownership to one of themselves in order to avoid messy legal proceedings at the end of the partnership.

Finally, the enactment of property right laws for non-personal (or personal) data would most likely cause a heap of practical issues. It would have to be balanced how large portion of the

[167] COM/2017/09 final, "Building a European Data Economy".
[168] De Franceschi and Leeman, 2016 pp. 71.
[169] See for example Wiebe, 2017 pp. 67.
[170] See COM/2017b, pp. 33-36.
[171] ibid., pp. 33.
[172] ibid., pp 34.

new protection would be subject to the freedom of contract. If too much of it is binding, it would potentially lead to massive renegotiations or terminations of existing contracts, as well as a surge of new claims, maybe from surprising parties, on already existing data that has been contractually allocated for years. On the other hand, if you make most of the legislation non-binding, it may change nothing at all.

While it is important to discuss both the potential justifications for any kind of property rights on non-personal data, it is equally vital to consider the drawbacks. Many of the justifications have been criticized in their respective paragraphs, but there were some considerations against the property rights in general that felt like they should be discussed more broadly. Neither of the lists is meant to be exhaustive, or to convey all the possible reasons to legislate or not to legislate on data ownership rights. Next, the study will explore a couple of different ways the data ownership rights could be constructed.

5.1.3. Bundle of Rights

As discussed briefly in chapter 2.3.3., defining data is very complicated, yet it is a crucial step if any rights are to be bestowed to the "owner" of data. It is very closely related to finding a feasible way to construct data "ownership", as it seems that data is too complicated to simply adhere to the conventional rules of property rights.

One often-discussed way of constructing a set of property rights which would be effectively applicable in the context of data, or information in general, is to build them as a "bundle of rights".[173] This method has been used by Professor Herbert Zech in his article "Information as Property" in JIPITEC in 2015.

First, according to Prof. Zech, to treat information as an object it should be divided into the layers discussed earlier in chapter 2.1.; semantic, syntactic, and structural layers. He notes that the traditional aspects of property right (use, enjoying the benefits of the use and changing the form or substance) can be distinguished in the context of information: possessing information, using information, and destroying information.

Possession of information can be seen to be synonymous with *access* when it comes to data.[174] Being able to view and handle the information means that you "possess" that information.

[173]For general "Bundle of Rights" theory of property rights, see for example Penner, 1996; for data application, see Zech, 2015 pp. 195 onwards.
[174] See e.g. Rifkin, 2000.

However, access to information is non-rival and non-exclusive. Multiple people can have access to the same information, and it does not get "used up" no matter how many people use it for their own purposes.

While access is necessary to *use* information or data, it is not one and the same. In his article, Prof. Zech uses an example of patent and copyright; while patent restricts the use of the information without limiting access (the information is made public when filing for a patent), copyright limits the use by limiting access (by limiting the ability to handle the information as wanted, namely copying and distributing it).

Finally, according to Prof. Zech, the destruction of information can be accomplished by either altering the syntactic layer of the information or by creating false data on the semantic level. Syntactic information can be completely deleted by destroying every "physical carrier" of that information, destroying the structural level of the information.

Ways to attribute the legal ownership of data would depend on the nature and level of the information, Prof. Zech writes. Personal data protection would give the right of ownership of both syntactic level of the information (for example photographs, recordings) and the semantic level of the information, so the meaning they confer of a certain natural person, to the individual concerned. Semantic mechanical information can be attributed in different ways. Fundamentally, the IP rights should belong to the person who creates the information, as is the case with, for example, patents. Trade secrets give another interesting view on the ownership of semantic information; as a consequence of the information being secret by nature, factual exclusivity pre-exists. The legal protection does not grant the exclusivity but intensifies it. The ownership is also not completely protected, as it allows for independent recreation and reverse-engineering.

According to Prof. Zech, on the syntactic level, the existing rules attribute the ownership rights to the creator. These rights allow the creator to both use the information themselves (i.e. copy) as well as grant access to others (distribute).

Finally, he notes that the structural level of the information is governed by classic property rights. By acquiring (legally) the physical carrier of certain information, assuming it is the only copy, one automatically receives the ability to use (by having access) and even destroy it as they see fit.

If a property right for non-personal data is to be legislated in the EU, the bundle of rights theory can offer a solid option in its construction. There has, however, been criticism[175] towards the idea of this property right theory, and it should not be seen as the only solution.[176] Next, the study will take a look at how the Commission of the European Union has proposed the allocation of property rights should take place in non-personal data.

5.1.4. Data Producer's Right

In 2017, the Commission of the European Union released a communication titled "Building a European Data Economy". In it, the Commission proposed the creation of a new property right for data that is titled "Data Producer's Right".[177] According to the communication, the aim was (or is) that "A right to use and authorise the use of non-personal data could be granted to the "data producer", i.e. the owner or long-term user (i.e. the lessee) of the device."[178] This would essentially mean that whatever non-personal data would belong to the owner or the long-term user of the device producing that data. It would apply specifically to non-personal data, as personal data would continue to be controlled by GDPR. The accompanying Staff Working Document[179] states that the intention is to "…enhance the tradability of non-personal or anonymized data as an economic good."[180]. EU seems to be the first regime that has lifted this notion on the stage of a proposal.[181]

What, exactly, is the Commission then proposing? The implementation of the property right, according to the Staff Working Document, could be formed either akin to the classical, *erga omnes* property rights, or as a collection of solely defensive rights. The first option would include "… a set of rights enforceable against any party independent of contractual relations thus preventing further use of data by third parties who have no right to use the data, including the right to claim damages for unauthorised access to and use of data."[182] This, of course, sounds very much like a traditional IP right, granting more or less the same rights as copyright. The second, "softer" option would give more protection when in "possession" of data, rather than aiming for full-fledged "ownership" rights.[183]

[175] See for example Smith, 2011.
[176] For an example of a different perspective to allocating property rights, see Merril, 2017.
[177] COM2017a, at 3.5.
[178] ibid.
[179] COM2017b.
[180] ibid. pp. 33.
[181] Yu, 2019 pp. 864.
[182] COM2017b, pp. 33, at (i).
[183] ibid. pp. 34, at (i).

The first option is surely the more radical one; it would essentially create a new intellectual property right within the EU that would allow the "owner" of non-personal data to have *erga omnes* property rights against anyone who would seek to use that data. Since it is so fundamental, this option has, understandably, gathered very heavy criticism[184] in the literature following the 2017 communication. Much of the criticism has already been covered in the previous parts of this study and it seems well justified. It is hard to imagine that a full new intellectual property right would be necessary; however, the Commission seems to see fit to at least consider it. It is not certain that it would achieve the desired effect. Prof. Hugenholtz, for example, argues that while it would surely raise the level of the current protection for non-personal data in the EU than the database right, but at the price of fundamentally compromising the current IP system.[185] There have also been endorsements for the legislation of the new property right, even though they seem somewhat cautious.[186]

The second proposed model of purely defensive rights would be akin to something that can be seen for instance in the Trade Secrets Directive. It would allow the *de facto* data holder to sue an infringing party for misappropriation of non-personal data. The Staff Working Document offers three possible remedies in case of infringement[187]:

1. The right to seek a court for injunctions against further infringement;
2. the right to have any possible products that are based on the misappropriated data removed from the market, and;
3. the possibility to claim damages.

Overall, the list does look very similar to the options provided in the Trade Secrets Directive. This more moderate approach seems to be more warranted, doubly so because as discussed earlier in the context of the Trade Secrets Directive, some of the data that requires protection could already fall under its umbrella and the legal owner would presently enjoy these rights. The Staff Working Document notes that this approach would assume that the current data economy functions without the need for a tougher legal intervention, but states that this may not be the case. However, there are scholars who would disagree.[188] As a curiosity, it is worth noting that the Staff Working Document also mentions re-evaluation of the criminal consequences for

[184] Perhaps most notably P.B. Hugenholtz, see for example 'Data property: An Unwelcome Guest in the House of IP".
[185] For a full list of consequences see Hugenholtz, 2017 pp. 2.
[186] Perhaps most notably Herbert Zech, see for example "Data as Tradeable Commodity – Implications for Contract Law", and above at "Bundle of Rights".
[187] COM2017b pp. 34.
[188] See for example: Drexl et al., 2016 pp.

these types of data breaches, i.e. that legislation would allow criminal law protection of more than just secret data.

The data producer's right suffers the same problem as all attempts to enact data ownership rules; who to allocate the ownership to? The solution proposed in the Staff Working Document for the *in rem* right has already been mentioned above, but bears repeating for the sake of clarity; it states that when allocating ownership, it would primarily go to the "data producer". However, the investments made, and the resources put towards the creating of the data could also be taken into account, as well as any liability considerations the parties are subject to. In the case of defensive rights, the protection would be granted to the *de facto* holder of the data. The Staff Working Document floats an idea of making technical protection steps a requirement to receive protection, similar to the Trade Secrets Directive.

Exceptions to the data producer's right would be governed by obligations to share data. Such cases would include, for example, public interest to make certain data available to private or public entities or the case of publicly funded scientific research.[189]

It is unlikely that the data producer's right would be enacted, at least in its more robust form; the change might simply be too profound. It seems that the Commission has taken a step back, seeing as, at the time of writing this study, in May of 2020, it has not released any concrete plans to bring the right to life. The Commission released a new communication on the 19th of February in 2020 titled "A European Strategy for Data"[190], which does not mention data ownership or data producer's right. It is uncertain whether or not this means that the Commission is reconsidering this radical idea, or that it is simply not ready yet to make a proper proposal.

5.2. Non-Legislative Measures

In addition to the legislative avenues to protect non-personal data, there is a multitude of possible softer, non-legislative ways to potentially control the data economy. For example, transactions between businesses can be guided with ready-modeled provisions to add into contracts that concern non-personal data transactions or data leasing.[191] Businesses can be encouraged to create their own codes of conduct that the stakeholders could enforce between themselves. On the member state level, things such as tax reductions, simpler start-up process, and school and university education could bring similar effects without the need for hard legislation.[192] This

[189] COM2017b, pp. 35-36.
[190] COM2020 66 final.
[191] COM2017a.
[192] Hilty, 2018 pp. 92.

study will take a closer look at two of these points, specifically; the default contract terms, and incentivizing businesses to share their data.

5.2.1. Model Contract Provisions

The Commission mentions default contract rules as one possible avenue in its October 2017 communication. These rules could be "…coupled with introducing an unfairness control in B2B contractual relationships…"[193]. The softer version of this would be the model contract terms.[194] The idea of default contract terms is usually meant to protect the lesser negotiating parties, giving them a chance at more fair contracts if their position is not solely based on negotiating power. In addition, it can give some measure of control over what kind of contracts are being used in data transactions. The Commission would let the stakeholders design this recommended set of default provisions.[195]

Contract law is the current standard in non-personal data protection. Often, however, the contracts used are akin to that of tangible property.[196] If Commission introduced certain basic, most commonly needed terms in data licensing contracts, it could greatly help the SMEs or even larger stakeholders that do not possess the know-how to draft these clauses. The integration of these terms would, naturally, have to be voluntary.[197] The freedom of contract would still be the default rule, as it can only be limited by hard legislation. The Staff Working Document notes that designed by industry stakeholders, these terms would be close to best business practices.

The model contract terms would most likely need some type of support. Tax reductions and other direct financial incentives have worked in the past (for example in environmental guidelines), and they may work again. Then again, streamlined data economy, lower transaction costs, and in general avoiding any binding legislation might be incentive enough. If the technology giants would still in practice dictate the terms of the contracts, then additional incentives should be considered. It does not benefit SMEs to know what their data licensing contracts should look like if they rarely get to have a say in the content. It should be noted, that the

[193] COM2017a.
[194] COM2017b pp. 31.
[195] COM2017a.
[196] Tantleff, 2015 pp. 14.
[197] COM2017b pp. 31.

contractual framework around data transactions would most likely benefit from legislation defining data ownership.[198]

Contract law alone would most likely not be enough to ensure a streamlined data economy.[199] However, it seems that the model contract terms would work well in tandem with some form of hard legislation. For example, if a purely defensive approach was taken in the legislation on data ownership, as described above, the contract terms could be modeled to as far as possible avoid any kind of accidental misappropriation of the non-personal data. The drawback then could be that the stakeholders might be less incentivized to follow the model terms if there were additional binding rules to limit the freedom of contract.

In terms of flexibility the model terms would have an advantage over any kind of hard legislation, as they could be amended to follow the rapid development of the market, thus adapting to the economic and technical environment much faster. Because of this, the situation in practice should be constantly monitored. Even a new organ of the EU could be appointed to keep an eye on the development of the non-personal data transactions specifically, in addition to any national authorities that would monitor the situation within the member states. But, given the right framework and an environment to thrive in, the model contract terms could have a positive impact on the data economy as a whole, improving market access and stability.

5.2.2. Guidance on Incentivizing Data Sharing

Another way to control the data economy without legislation is to make sure that consumers and stakeholders are well educated on the current state of the core legislation that would help them to deal with the contractual and legal obligations relating to data, and how they could use it in their data licensing contracts.[200] The Staff Working Document particularly mentions the Trade Secrets Directive, the Database Directive, and the general transparency and fairness rules present in the contract law within the EU. It seems that this would be close to something that this study has tried, hopefully successfully, to achieve; to make a review of the current legislation that could be used to deal with non-personal data. Getting this information to the stakeholders may significantly lower transaction costs, and, once again, may serve to bring SMEs to (more) equal footing among the industry titans.

[198] Kerber, 2016b pp. 12.
[199] Drexl, 2017 pp. 278.
[200] COM2017a, COM2017b, pp. 30.

This would, in turn, require efforts on both the EU level and on the level of the individual member states. Informing has to be penetrating enough to go through the market; from the state-provided entrepreneurship courses aimed towards start-ups, and to the top of the food chain where the big names such as Google, Apple, and Twitter exist. While this kind of informing would appear to usually benefit the SMEs the most, many of which do not have the capacity to employ a full-time legal or compliance team, it does not hurt to at least let the larger companies know that their smaller business partners have access to this knowledge.

5.2.3. Developing Technical Means

While not exactly the domain of law, it feels important to mention technical means of protection, albeit briefly. In fact, technological means are currently, alongside contract law, the main way that companies protect their data.[201] The Staff Working Document mentions multiple possible options, but two of them sound particularly fascinating; a standardized way of "watermarking" data, and the increased use of APIs (Application Programming Interfaces[202]).[203]

Watermarking has been around for a long time, most familiar, perhaps, in copyrighted images seen online. The Staff Working Document notes that it might be possible to create a standardized form of "watermark" to track the origins of non-personal data, secure any commercial interests, or even attach accompanying usage preferences. The benefit of this would be an increase in trust and security in the markets where massive amounts of data are moved through many stakeholders. It would be up to someone with a better grasp of the technical understanding to analyze whether or not this would be a cost-effective method to secure a business's non-personal data interests.

The use of APIs is already very prevalent in many day-to-day functions online. An Apple device allows a person to check up on their email inboxes through the built-in mail app, after which it checks the weather for you from (usually) the local weather service and finally asks you to log into Zoom using your Facebook account. APIs are very widely used to streamline our everyday experience, and according to the Staff Working Document, better documented and standardized

[201] See e.g. Stepanov, 2020 pp. 75, Drexl, 2017 pp. 272, Wiebe 2017, pp. 65.
[202] The Oxford Dictionary of Social Media (Chandler & Munday) describes API as: "A standardized set of protocols for accessing the functions of a particular program, enabling other programs to make use of them as modules. It is typically used to refer specifically to Web APIs; social media such as Twitter have APIs which software developers can use remotely in their own Twitter-based applications.". Some of the most well-known examples could be the many cloud services, Google Maps or Google Calendar.
[203] COM2017b pp. 30-31.

APIs can allow for smoother re-use, profit, and use of data in development. It could even include making the data available in a machine-readable format.[204]

This chapter was not meant as a technological deep dive to all the possible ways of protecting non-personal data but was a necessary mention in the context of the Commission's communication. It should also remind both the author and the reader, that sometimes the legal solution is not the most elegant one. It is easy to get sucked into designing legal constructs that would turn out to be inconvenient half-measures in practice. That said, nothing stops the legal and technical solutions working in harmony, and as they well should, considering that in an issue this complex, a multidisciplinary approach is definitely warranted.

6. Summarizing and Final Conclusions

Data is an extremely important part of today's data-driven economy. Information is power, and large groups of businesses are starting to rely more and more on data. Lately, the focus has been specifically on machine-generated, non-personal data. Entire business models depend solely on exclusive access and protection of their non-personal data. Big Data and Internet of Things are changing the internal market, and with the surge of data provided by IoT, Big Data Analytics are becoming an increasingly popular and significant tool for all market stakeholders, even if they are a part of more traditional branches of industry. This creates potential barriers to entry especially to Small and Medium Enterprises (SMEs) that do not necessarily possess the resources or the know-how to manage their data.

It is a fact that this kind of data often has commercial value, and the exact value depends on who it should be attributed to. It is valuable; thus, it would seem reasonable that those who hold it should have some measures to protect it *erga omnes*. Just because something has value, however, should not mean that it automatically requires protection. There are many arguments for and against the legal protection of machine-generated data. Based on the perspectives examined in this study, it seems difficult to choose action either way. On the one hand, the legislation would clarify many things; the legal environment in general, and the property rights attached to data. On the other, giving exclusive protection to industrial data through legislation can lead to many unintended side-effects, such as impediment of innovation or competition. It will be

[204] ibid., pp. 31.

nearly impossible to predict all the ripples such legislation would cause, and as such it seems like there is no "winning strategy" to regulate non-personal data.

It is important to note that currently the majority of non-personal data protection is handled by different kinds of contracts between the stakeholders. Often these contracts are modeled as if one could identify property rights for data, even though that is not currently the case. The main forms of contracts are non-disclosure agreements and data licensing agreements. Many businesses use the same base contract for both licensing tangible property and licensing data. However, since the data economy seems to currently flourish, it seems that contractual means can be effective in ensuring sufficient protection, together with technical means providing factual exclusivity. The contracts have their drawbacks, such as not being binding outside of the parties of the contract and the imbalance in negotiating terms for these contracts, mainly for SMEs and more traditional industry stakeholders.

There is no catch-all legislation in place for non-personal data within the EU. Three avenues of potential protection can be identified: The Database Directive, the Trade Secrets Directive, and, to very minor extent, the Copyright Directive. Traditional copyright very rarely offers any protection in the case of industrial data, as it usually completely lacks the degree of originality required to benefit from copyright legislation.

The Database Directive can offer some protection in a small minority of cases, though industrial data is often not arranged in a database in a way that would fulfill the requirement of being assembled in a methodical or systematic manner. However, the *sui generis* right found in the 7th article of the Database Directive provides a wider definition for industrial data to fit under. The "substantial part" -requirement is not as much of a hindrance, as it allows both quantity and quality of the data to be taken into account when considering the substantiality. However, the "substantial investment" -requirement may prove to be more troublesome, as the ECJ has ruled in its case law that the investments must be made toward the building of the database, and not gathering the information within the database. This makes it tricky to prove investment in the case of industrial data, as most of the investments are indeed made towards whatever appliances the data are collected by.

Trade Secrets Directive offers a somewhat more concrete definition for what kind of data could be considered a trade secret and as such gain benefit from the protection provided by the directive. It lays down three requirements, roughly put: Is the information a secret, does it have commercial value because it is a secret, and has reasonable measures been taken in order to

keep it a secret. While the first two are somewhat easy to prove, the "reasonable measures" -requirement seems to be a little more complicated. Secrecy and value are often assumed (though obviously evidence towards both is still required by the court) by the fact that the presumed trade secret holder is willing to litigate the misappropriation at all. However, what constitutes a reasonable measure is very much up to the court's discretion. It depends on the context of the situation, as the words "under the circumstances" can be expected to hint in the article 2 of the Trade Secrets Directive. In the end, a holistic consideration by the court is what decides whether certain information constitutes a trade secret, and that is also the case with industrial data.

The remedies set out in the articles 12-14 of the Trade Secrets Directive seem to lend themselves rather poorly to the case of industrial data. They can be divided into injunctions and damages, of which damages can be seen as a viable category to provide compensation in the case of a data breach. Injunctions are often too slow of a remedy to counteract something that may or may not be noticed by the infringed party at all, let alone early enough to allow meaningful intervention by the court. However, the Trade Secrets Directive stipulates a possibility for member states to legislate a temporary injunction, in which the plaintiff does not need to prove the existence of misappropriation, only to show that it is imminent.

Seeing as the U.S. Uniform Trade Secrets Act (UTSA) was used as a model for Trade-Related Aspects of Intellectual Property Rights agreement, which in turn was used to model the definition of a trade secret in the Trade Secrets Directive, it seems appropriate to take a brief look of the U.S. trade secrets legislation. It is composed of three separate acts: UTSA, which concerns the civil law procedures involving trade secrets, Economic Espionage Act (EEA) which lays down the criminal law side, and the Defend Trade Secrets Act (DTSA), which allows civil action against breaches that originate from outside of the U.S. The most interesting fact about the three acts is, that while UTSA and DTSA have nearly identical definitions for trade secrets, EEA has a much wider one, which is obviously much more favorable in cases of data, and also most akin to the one on the Trade Secrets Directive. This solution is doubly intriguing because the Finnish Criminal Code merely refers to the Trade Secrets Act in its provisions concerning crimes against trade secrets. In the end, it would seem that there is no clear-cut solution on the other side of the pond for the use of trade secrets legislation in the case of data breaches. However, it should be noted that the comparison in this study was narrow, focusing solely on the definition of the trade secret, and shallow, considering only the minimal amount of case law. A more comprehensive project would be required to gain a full understanding of the state of data protection under the trade secret legislation in the U.S.

Possible future developments in the protection of non-personal data within the EU include legislating a concrete legal construction for the ownership of data. There has been much discussion on whether or not this level of legal intervention is warranted. Most notable justifications are clarifying the legal environment for the data economy and enhancing stability in data transactions. As data transactions are part of the everyday functions of the current market, these could serve to significantly lower the transaction costs. Arguments against such *erga omnes* right are seemingly more numerous than the arguments for it. Perhaps the most notable ones are the issues of allocating the ownership and the problems in defining data itself.

The bundle of rights theory of property could be seen to lend itself to data rather well, at least in theory. The issues lie with defining the protected data; surely all of it cannot be protected, and where to then draw the line? The Commission of European Union has proposed the adoption of a "data producer's right", which would allocate the ownership of the machine-generated data to the entity that owns or is the long-term controller of the device that produces such data. In the Staff Working Document, the Commission proposes two alternative constructs of data rights: The *in rem* right, which would be akin to the traditional property rights, or a set of defensive rights, granted to the *de facto* holder of the data, such as those granted by the Trade Secrets Directive. It should be noted that given in October of 2017, the communication on the "Building a European Data Economy" is already quite dated in today's world, where technology and everything related to it is moving at an increasingly accelerating pace.

As for non-legislative measures, a few seem to be above the others in importance, namely providing model contract provisions and giving increased guidance in data-sharing and the use of existing legislation in cases that involve industrial data. Both could serve an important role in both bringing SMEs to a more equal footing with the tech giants in terms of contractual know-how and proficiency and knitting together the current legislative patchwork that serves as the framework for such data rights. Undoubtedly this would be a much simpler task if any non-persona data -related legislation would be enacted, but it is still important to consider it even without concrete laws in place, maybe even more so. In practice, the execution would be largely in the hands of the member states, as they would have to take up the responsibility of informing businesses and especially the SMEs in their jurisdictions.

Finally, it should be mentioned that legislative means may not be the best way to regulate the use of non-personal data, and certainly not alone. No matter what, the solutions will be closely linked to the currently available technology and should strive to adapt to meet the demands of the technologies that are yet to emerge. In general, this is an area where a multi-disciplinary

approach is mandatory; it would be completely pointless to enact laws that would be useless or unenforceable in practice. One can hope that there is enough heed being paid to both the stakeholders and the technical experts when considering whether or not these laws should be created in the first place, and if they are, it will not end up as a toothless political compromise.

In the end, data as a whole are a very complicated phenomenon to legislate on. It seems that no matter which way the legislators will choose, consequences will range from moderate to catastrophic on different areas of the market. It is certainly impossible to know or predict exactly how any kind of non-personal data legislation will affect the market where there currently are almost no legal rules in place aside from contract law. It seems that the best solution would be to avoid too strict ownership models and to create a form of protection which would be some combination of defensive rights, non-legislative means, and technical solutions. That is, however, very easy to write on a paper, but much more complicated in practice. The solutions will hardly ever be perfect, especially when considering how fast the development is in the data economy. To which degree is the current contract law solution adequate to control the data economy? Would widening the reach of injunctions and damages to non-personal data create chaos in the existing market? Is it technologically possible to enforce whatever solutions legal experts come up with? These, and many, many more questions should be aimed to be answered before the legislative process.

While a lot of discussions have been conducted, it feels there is much more to be discovered. Especially after the ECJ starts handing down judgments concerning the new Trade Secrets Directive, there will be many more interesting solutions to keep track of. The area of non-personal data should be explored further. All in all, additional research is surely required.