TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Ratul Sen

IP Protection of Personal Data for Data Subjects within the Personal Data Storage Ecosystem

Master's thesis
Programme HAJM, specialisation Law and Technology

Supervisor: Katrin Merike Nyman-Metcalf, Adjunct Professor, PhD,
Department of Law, SOC-327
Tel: 6202424
Tallinn University of Technology

Tallinn 2021

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same thesis
has not been previously presented for grading.
The document length is 21169 words from the introduction to the end of conclusion.

Ratul Sen 10th May 2021

(signature, date)

Student code: 195035HAJM

Student e-mail address: ratsen@ttu.ee

Supervisor: Katrin Merike Nyman-Metcalf, Adjunct Professor
PhD, International Law, Uppsala University

The thesis conforms to requirements in force

10th May 2021

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

In today's digital world personal data has become a prized asset of most corporations. Trade in personal data is now the norm and while modern technologies have allowed corporations to use data in order to provide personalised services, recent security breaches have shown that such pervasive use of personal data can have major repercussions.

This thesis looks into whether standard data protection laws of the EU are strong enough to control the various security and privacy issues which have crept up due to largescale use of data. To assist the data protection regime in maintaining a high level of privacy and security, the thesis explores the idea of individuals owning a distinct right in the form of an Intellectual Property over their data, in addition to their existing rights under the General Data Protection Regulation. The thesis analyses whether individuals are in fact capable of owning an intellectual property over their personal data so as to protect it better and if so how it could work practically. The thesis looks at relevant legal legislations, primarily EU data protection and IP law and reaches its conclusions through a qualitative analysis of the literature. Finally, practical proposals for solutions are examined and suggestions are made based on the analysis.

The results suggest that although in principle, there are various arguments to support individuals having an IP right over their data, no IP model currently exists under which this new regime can be implemented. The thesis finds that existing Ip rights all suffer from some disadvantage or another and therefore perhaps a novel type of IP right would have to be developed in order to provide data subjects with maximum security. The thesis also finds that multiple corporations have created ecosystems which can serve as an early inspiration for future models which provide data subjects with IP rights over their data. It is however made clear that giving individuals more control over their personal data is the only logical step forward and therefore this field requires further studies and analysis.

Keywords: IP right, Control of personal data, Ownership, Data Protection, Data subject owning a right over personal data.

INTRODUCTION

The idea that data is the oil of the 21st century has now become an established truth.[1] In today´s digital economy, the value of data has skyrocketed to quickly become one of the most prized possessions of individuals and corporates alike. Large scale corporations like Google and Facebook appear to value data more than their physical assets and shape their corporate policies based on data.

Data breaches are getting more and more common and are becoming legitimate security threats[2]. The development of modern data protection regimes all across the world seems to suggest that personal data warrants a higher degree of protection against exploitation. Many scholars believe that data protection laws are not enough, and data subjects should have enhanced rights and powers over their data[3]. Such power may be acquired through models of ownership and intellectual property[4]. As is the norm with intangible objects which contain significant economic value, protection through IP is often the most reliable option.

The hypothesis for the analysis in this thesis is that given the importance of data for the modern society, data protection legislation is not sufficient to provide adequate protection for personal data, as it suffers from weaknesses that make the protection less effective. Consequently, there is a need to examine whether other forms of protection can be of help, particularly IP protection. The main research question analyzed in this thesis is whether there is a need for enhanced legal protection of personal data in addition to modern data protection regimes and if so, whether ownership acquired through IP can serve this need. To answer this research question, the thesis analyses the following specific research questions:

[1] Kessler, J. (2019). Data protection in the wake of the gdpr: California's solution for protecting "the world's most valuable resource". Southern California Law Review, 93(1), 99-128.
[2] Cheng L., Liu F., Yao D. (September/October 2017). Enterprise data breaches: causes, challenges, prevention and future directions, Wires Data Mining and Knowledge Discovery, Vol 7, Issue 5, p 1211
[3] Trakman, L., Walters, R., Zeller, B. (2019). Is privacy and Personal Data set to become the new intellectual property, SpringerLink.
[4] *Ibid*

The thesis begins with an overview on how personal data is collected and used by large corporations and highlights whether they have a detrimental effect on data security and privacy. Through its analysis the thesis tries to answer whether data protection laws in their present form are strong enough to ensure a high level of data security and privacy. Thereafter the thesis looks at the whether an additional right such as an IP right can help fill in the gaps left by data protection regimes.

To understand whether an IP right could suffice, the thesis looks at how IP rights currently apply to personal data in the European Union. The thesis dwelves into the issue of whether data subjects can actually hold rights over their data and the rationale behind such a right. To understand what such a right could look like ideally, the thesis tries to distinguish between having traditional proprietary rights over data and owning an IP right over data. The thesis discusses various issues specific to personal data such as whether it is psychologically possible for individuals to perceive ownership over their data.

The thesis then attempts to present practical models which may be employed in order to support a possible IP regime for protection of personal data. The pros and cons of the proposed IP models are analyzed and thereafter the thesis concludes by presenting its findings.

In order to reach its conclusions, the thesis uses analytical and qualitative methods along with action research. The thesis evaluates case laws, interviews and academic literature in order to come up with its findings and suggested solutions.

The thesis limits its scope of application to the European Union and focuses only on the security and protection of personal data as defined in the General Data Protection Regulation. Therefore all forms of non personal data and foreign data protection regimes are out of the purview of the present thesis.

1. THE USE OF PERSONAL DATA IN TODAY´S DIGITAL WORLD

The world today has changed drastically in the last thirty years. The way the world works today is almost unrecognizable. Today the most valuable resource on this planet is no longer oil, but data.[5] It is almost strange to imagine that an intangible asset can actually hold so much value and drive the business models of the top technology companies of the planet. One of the reasons for this gargantuan valuation of data is the sheer amount of it being generated on a daily basis. In 2013 SINTEF, a research group from Norway claimed that the world had created more data in the previous two years than in the entire history of our existence.[6]

The billionaire Elon Musk predicts that AI and human would merge in the future simply because such a symbiotic way of life would be more efficient.[7] He claims that the process has already begun, the only issue is the rate of data transfer between the AI and the human brain is extremely slow and therefore it appears as if we are different entities.[8] Indeed, it is true that we cannot find a human brain which is totally disassociated with AI. Almost every single person in this world carries a mobile phone on his body. This device broadcast and tracks all kinds of data about the human and such data is later harvested by big technology companies in order to provide services. Today almost each and every human being leaves a digital footprint whenever they perform some activity. Amazon knows what we buy,[9] when we buy ad how often we buy. Air conditioners know what temperature we prefer to have inside our houses[10] and social media companies know sensitive aspects of our personality such as our political affiliations, hobbies,

[5]Senate Judiciary Committee Report. June 25, 2018).
2017-2018 Reg. Sess., Rep. On Internet Service Providers: Customer Privacy 1-2
[6] SINTEF. (2013, May 22). Big Data, for better or worse: 90% of world's data generated over last two years. ScienceDaily. Retrieved April 7, 2021
[7] Musk. E., CEO Neuralink, The Joe Rogan Experience # 1470, Joe Rogan, Video Podcast. published on www.youtube.com. (May 7, 2020).
[8] *Ibid*
[9] Weise, K. (2019). Amazon Knows What You Buy. And It´s Building a Big Ad Business From it. The New York Times, Retrieved 8th April, 2021
[10] Taştan, M & Gokozan, H. (2018). An Internet of Things Based Air Conditioning and Lighting Control System for Smart Home. American Scientific Research Journal for Engineering, Technology, and Sciences. 50. 181-189.

interests and even who our friends are.[11] This seems to be the current model of data collection as it stands today.

1.1. Large scale data collection of personal data

To understand how data collection works it is wise to study how the model works in detail. Let us take a social media website such as Facebook as an example. When a user creates a profile on Facebook, two things happen. Facebook offers all its services to the user and in exchange they proclaim ownership over all data which the user generates while using their services.[12] Facebook also collects all personal data which the user might enter on his own such as his name, date of birth etc. The user also forfeits all control over such data and their future use. This is done through user agreements. When a user signs up for the services of Facebook they provide them with consent to acquire and use some of the user's data. Facebook's policy defines how that data will be used in the future including which third parties they may sell that data to.[13] These third parties in turn may sell on that data or use that data to offer personalized services. In many situations third party apps may also sell their data to Facebook thereby creating a circle of data Exchange.[14]

Therefore, while car companies may use their own data to improve the performance of their vehicles they may also rely on data bought from Facebook to understand the trends in tastes and preferences in the market in order to shape their next model. Similarly, a supermarket chain might be interested in knowing what kind of products Facebook users most are interested in buying and shape their product catalogue based on it. These third parties may then sell on the data to other entities who might benefit from it in some other ways. The trail of data discussed herein originates from a user registering a profile on a social media platform. However, this same model of data sharing may take place whenever users use digital services. With the coming of the internet of things[15] everyday household objects are now able to track all sorts of information

[11] Paul. H., Lee. R., (January 16,2019). Facebook Algorithms and personal data. Pew Research Centre. accessed on 28th April 2021.
[12] Dwyer. C., "Privacy in the Age of Google and Facebook". IEEE Technology and Society Magazine, vol. 30, no. 3, 58-63, Fall 2011.
[13] Terms of Service, Facebook Inc, Retrieved on 10th April 2021
[14] Schechner.S., Secada.M., You Give Apps Sensitive Personal Information. Then They Tell Facebook. February 22, 2019. The Wall Street Journal.
[15] Aguzzi. S., and others, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (European Commission 2014). 10, 26, 61.

about its users. Therefore, data is being created and generated by every digital device being used by every digital user in the world every second. The scale of data collection is therefore enormous. There are certain potential problems with such large-scale data collection which are well known, and many scholars have already identified certain ethical[16] and legal concerns[17] within the model. Therefore, it appears that the data protection regime in place would have to be very efficient in order to manage such concerns. Some of these concerns will be explained further in the present chapter.

In the context of Europe, the data protection law concerned is the General Data Protection Regulation.[18] The GDPR in general tries to establish a model based on transparency and consent and as long as the rules are followed companies may use the data they collect for their own commercial gains.

1.1.1. Data breaches

A data breach involves an unauthorized access to data which might lead to sensitive information being compromised.[19] In the digital world corporations routinely deal with massive volumes of sensitive personal data. It would therefore appear that any leak of such data could have severe consequences for both individuals[20] and corporations[21] alike. The world has already seen some major breaches including big conglomerates such as British Airways[22] and Marriot Hotels[23] being subject to massive attacks. However, we may not have seen the full-scale effect of that

Globally, the number of connected devices is expected to grow from 9 billion in 2013 up to 50 billion by 2020: OECD, OECD Digital Economy Outlook 2017 (OECD Publishing 2017) 247; GAO, Technology assessment: Internet of Things: Status and implication of an increasingly connected world (GAO-17-75, May 2017) 1. McKinsey Global Institute. The Internet of Things: Mapping the Value Beyond the Hype (McKinsey 2015) 17.

[16] Van den Hoven, J. Internet of Things Factsheet Ethics (European Commission 2013).

[17] Drexl. J., and others. '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) Max Planck Institute for Innovation & Competition Research Paper No 16-10.

[18] 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).

[19] Sen, R. & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach, Journal of Management Information Systems, 32:2, 314-341.

[20] Pascual, A., Miller, S. Identity fraud report protecting vulnerable populations. Javelin Strategy and Research, (March 2015). (accessed June 30, 2015).

[21] The 2014 Cost of Data Breach Study: United States, Ponemon Institute, May 2014.

[22] Whitaker, T. (2018). The ba data breach. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 2(10), 15-16.

[23] Tidy, J. (2020). Marriot Hotels fined £18.4m for data breach that hit millions, BBC News. Retrieved 9th April, 2021.

data falling into the wrong hands yet. In principle however, a data breach has extremely serious consequences.[24] The Cambridge Analytica case showed us how enough data can even be used to sway public opinion without the public ever being made aware of it.[25]

The GDPR imposes strict fines and a high standard of security, and over the years has managed to see a reduction in the number of data breaches which are reported within the EU.[26] However the numbers still remain extremely high. The website haveibeenpwned[27] tracks all such cases where a certain email id was part of a data breach. As of 11th April 2021, more than eleven billion accounts have been compromised in data breaches.[28] However the overall trends in data breaches suggest that they are increasing. Moreover, since we are currently in the age of big data, it is foreseeable that cybercrimes including data breaches are here to stay.[29] Therefore it would appear that data protection laws would need to put in additional effort in other to counteract this trend.

1.1.2. Data subject's control over their data

One of the biggest concerns which large scale data processing has brought is that data subjects have lost total control over their data.[30] A thirty-year-old data subject who has used digital services all his life would probably not know how much data of his has been collected, what that data contains and who controls that data presently. This is because of several aspects. The first aspect is the problem of multiplicity of data. When we create a Gmail account we enter our personal details. We then enter the same personal details when creating an Aol account of a Facebook account. Therefore, the same personal data has been given to multiple entities and each time we have signed up to different terms and conditions allowing the recipients of our data to do different things with it. The second issue is that since the GDPR allows the commercial

[24] Citron, D., Solove, D. Risk and Anxiety: A Theory of Data Breach Harms. 96 Texas Law Review 737 (2018).
[25] Cadwalladr C., Graham-Harrison.E. (2018, March 17). "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". The Guardian.
See Also: Richterich, A. How data driven research fuelled the Cambridge analytica controversy. PArtecipazione e COnflitto * The Open Journal of Sociopolitical Studies, PACO, Issue 11(2) 2018: 528-543, Published in July 15, 2018
[26] Breitbarth, P. The impact of GDPR one year on. Network Security, Volume 2019, Issue 7, 2019, Pages 11-13.
[27] Have I Been Pwned. Website. Accessed 15 March 2021
[28] *Ibid*
[29] Wall, D.S. (2018). How Big Data Feeds Big Crime. Current History: A journal of contemporary world affairs, 1 January, 29- 34.
[30] Bottis, M., Bouchagiar, G. (2018). Personal Data v. Big Data in the EU: Control Lost, Discrimina- tion Found. Open Journal of Philosophy, 8, 192-205

exploitation of data it allows data to be bought and sold.[31] The only protection that the GDPR contains is that the data subject must be informed about what exactly will be done with his data. For example, Facebook would have to show in their terms all the companies to which they might sell the personal data which they have collected and take consent from the data subject before making the sale. However, that is essentially where the control of the data subject ends.[32] There is essentially no privity of contract between the data subject and the third party who Facebook sells the data to.[33] Therefore, what the third party decides to do with the personal data once the sale has been made is totally up to their agreement with Facebook and has nothing to do with the data subject's rights. Eventually as personal data keeps getting sold from entity A to B, the data subject loses complete track of who controls his data. Considering that personal data is in a way a digital image of our personality it there seems to be a need to present a way to users to regain control over such data.[34]

1.1.3. Data and human behaviour

Perhaps one of the biggest risks regarding mass scale collection of data is its ability to change public opinion. For many years it was assumed that data can be used only to predict public behavior and see the trends in their behavior after careful analysis. However, we now know that data analysis could lead to changing people's opinions therefore giving data analyst the power to dictate many aspects of our political and socio cultural lives.[35]

The Cambridge Analytica scandal proved to the world that even political parties can use such data on consumer behaviour and then use unethical tactics to shape public opinion.[36] The Trump campaign used data to identify which sets of the American population were undecided on their votes. They then followed this by analyzing what kind of topics the population was sensitive about in order to identify pressure points. Once pressure points were identified systematic

[31] Regulation (EU) 2016/679, (2016), *Supra Nota 18,* Recital 101 and Recital 18.
[32] Nyoni, P., Velempini, M. (2018). Privacy and user awareness on Facebook. South African Journal of Science, 114(5-6), 15.
[33] Trakman, (2019), *Supra Nota* 3
[34] Mitrou, L. (2009). The Commodification of the Individual in the Internet Era: Informa- tional Self-Determination or "Self-Alienation"?. In M. Bottis (Ed.), Proceedings of the 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE 2009) (466-484). Greece: Nomiki Vivliothiki.
[35] Lewandowsky, S., Smillie, L., Garcia, D., Hertwig, R., Weatherall, J., Egidy, S., Robertson, R.E., O'connor, C., Kozyreva, A., Lorenz-Spreen, P., Blaschke, Y. and Leiser, M. Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making. EUR 30422 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-24088-4 (online),978-92-76-24089-1 (print), JRC122023.
[36] Richterich. A. (2019). How data-driven research fuelled the Cambridge analytica controversy. The Open Journal of Sociopolitical Studies. PACO, Issue 11(2) 2018: 528-543.

targeted advertisements were used to hit those pressure points in order to sway their votes in favour of the Republication party.[37] The tactics used by the Trump campaign can very well be reproduced by other entities. In fact, data can also be used by criminal outfits to predict what kind of an ethnic population lives in which part of the world. Similarly, data analysis may also be used to authoritarian governments to curb free speech and sway public opinion in their favour. These facts make a compelling argument in favour of granting more rights to data subjects.

1.1.4. Data collection, consent and intrusiveness

With modern technologies corporations may know extremely intrusive data on a very large scale. The idea that a corporation can knows one's favorite restaurant is intrusive enough but if corporations can know at what pace an individual's heart beats from the data supplied by their health tracking device,[38] it could seriously raise privacy concerns.[39]

The other reason why data collection has become too intrusive is due to the sheer power of technology and data analysis. For example, sensitive information such as political views, ethnicity and sexual orientation can be gathered just by analyzing Facebook likes.[40] Cambridge Analytica claimed was able to identify more than five thousand data points for each individual they tracked on Facebook.[41] The other aspect which makes data quite dangerous is its power of predicting human behavior.[42] Data analysis techniques are so advanced today that they can analyze a human's behaviour a then realistically predict their next move so that the corporation may make money selling a product as per his expected behaviour.[43] Such analysis is done using big data technology where massive amounts of data are accumulated and then analyzed. Without such a massive sample of data it may be impossible to come up with such accurate predictive analysis. Therefore the individual in concern is not capable of ever reaching the same conclusions as the predictive algorithm.[44] The other power of big data is that it is capable of

[37] Berghel.H. (2018). Malice Domestic, The Cambridge Analytica Dystopia. IEEE Computer Society,
[38] Ho, J.-J., Novick, S., Yeung, C.: A snapshot of data sharing by select health and fitness apps. Federal Trade Commission, Washington (2014).
[39] Christovich, M. Why should we care what Fitbit shares: a proposed statutory solution to protect sensitive personal fitness information. Hastings Commun./Entertain. Law J. 38, 91–116 (2016)
[40]Kosinski, M., Stillwell, D., Graepe, T. Private traits and attributes are predictable from digital records of human behavior. (Retrieved from the Proceedings of the National Academy of Sciences of the USA (2013)
[41] Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting, Journal of Media Ethics,33:3, 133 148.
[42] Moat, H., Preis, T., Olivola, C., Liu, C., & Chater, N. (2014). Using big data to predict collective behavior in the real world. Behavioral and Brain Sciences, 37(1), 92-93.
[43] Kshetri, N., Big data′s impact on privacy, security and consumer welfare. Telecommunications Policy, Volume 38, Issue 11, 2014, Pages 1134-1145,

[44] Beales, H., Craswell, R., C. Salop,S. The efficient regulation of consumer information, Journal of Law and Economics. 24(1981), 491-539

aggregating a variety of different data sets from different sources and then cross reference them to find interesting conclusions.[45] For example coca cola might be studying twitter feeds mentioning the word coca cola across multiple jurisdictions of the world to find out which section of the population likes which flavour of coca cola. This knowledge of flavour preference might seem useful to another company who want to launch a new beverage in a certain market and therefore this data can easily be sold to such companies.

Data collection techniques have existed for many years. However, they never felt too intrusive because of two main reasons. The first reason is that it generally required extensive effort to collect important data which psychologically made it seem acceptable to data subjects. Consider the example of a local medicine shop who wants to launch an advanced blood pressure measuring device. To understand whether that product would sell in the neighborhood they send agents out to each and every household in the neighborhood with questionnaires collecting information about their health requirements. Presumably a few of the households would refuse to fill up the questionnaire and ultimately the market research conducted by the medicine shop would present a picture based on a small sample size. Therefore, the market research technique shown here involved a personal touch and significant effort in terms of time and human capital. In spite of the same the results would largely be imperfect and only cover the small area of one neighborhood. Additionally, clear consent was taken from the households while filing up the questionnaire. However, with big data, data collection can not only be extremely accurate, but they can also cover huge sample sizes while incurring minimum effort. The data from the Fitbit app can possibly tell a medical supplier much more about the medical requirements of the entire population of a country.[46] If we contrast this with the effort it took the medical shop to get an idea about the medical needs of just one neighborhood then we can see how much cheaper it is to collect an immense amount of data.

The second aspect which may make modern data collection techniques intrusive is that there seems to be almost no information which is outside the purview of data collection. We can assume that without big data technology, data collection would not only be time consuming and expensive, but it would also be extremely difficult to collect very sensitive data. For example, it would probably be almost impossible to know the political preferences of the entire population

[45] Drum, K. (2013, November/December). Privacy is dead. Long live transparency!. See also King, L. (2014). Alarm over the 'gold rush' for citizens' big data.
[46] Christovich, M, (2016), *Supra Nota* 39.

of a country without doing a large scale opinion poll. Today most social media websites could probably have this information. Social media websites can probably even tell why the population favors a certain political party and how they can improve one party's chances of winning the election over the other. This can be done by analyzing the social media feeds to check if conversations regarding them are positive or negative.[47] Similarly data could also give extremely accurate results about a population's views on homo sexuality or show the chances of them committing hate crimes. While such data may be used in a positive way, it seems like there is no information that can be kept secret anymore.[48]

The ethics of data collection are further challenged when we look at the issue of consent. The General Data Protection Regulation imposes various rules regarding consent and mandates that the consent should be free and informed. The rules imposed by the GDPR are quite bold, but the real issue is whether the end objective is being fulfilled. Are GDPR complaint consents truly free and informed? Allegedly it would seem that they are not.[49] This is because of a variety of factors including human indifference. Data protection is not a field which may come intuitively to people. It is a new complicated field, and it can be argued that most individuals still do not understand it properly.[50]

The consent gathered from data subjects cannot be termed as informed consent either because by definition it means that the data subject has read and understood what he is giving consent for. This is obviously not the case since no one ever reads the terms of agreement.[51] The other major issue is that data subjects are now addicted to technology and technology products. At this stage cutting off major services such as Google and Facebook from one's life may be challenging.

---

[47] Sharma,P., and Moh,.T. "Prediction of Indian election using sentiment analysis on Hindi Twitter". 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 2016, 1966-1971.
[48] Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society., Information & Communications Technology Law, 17:3, 185-197.
[49] Mitrou, L. (2017). The General Data Protection Regulation, New Law, New Obligations, New Rights. Greece: Sakkoulas. Page 466
[50] Andrews, V. 2019. Analyzing Awareness on Data Privacy. In Proceedings of the 2019 ACM Southeast Conference (ACM SE '19). Association for Computing Machinery, New York, NY, USA. 198–201.
[51] Manovich, L. (2011). Trending: The Promises and the Challenges of Big Social Data. In M. K. Gold (Ed.), Debates in the Digital Humanities. Minneapolis, MN: The University of Minnesota Press.
See also:
Turow. J., Hoofnagle. C. J., Mulligan. D. K., Good. N., & Grossklags, J. (2006). The FTC and Consumer Privacy in the Coming Decade. I/S: A Journal of Law and Policy for the Information Society, 3, 724 and
Pingo Z., & Narayan, B. (2016). When Personal Data Becomes Open Data: An Explora- tion of Lifelogging, User Privacy, and Implications for Privacy Literacy. In A. Mori- shima, A. Rauber, & C. L. Liew (Eds.), Digital Libraries: Knowledge, Information and Data in an Open Access Society—18th International Conference on Asia-Pacific Digital Libraries, Tsukuba, Japan (4). Japan: Springer International.

More importantly in the age of the "Internet of Things" everyday devices will collect and generate data about data subjects.[52] Therefore if one wants his personal data private then they would presumably have to stay away from most modern devices as well. In many situations in today's world various services are locked behind the creation of a digital profile. Therefore, choosing data privacy and security may mean not being able to use certain services.[53]

1.2. ARE DATA PROTECTION LAWS ENOUGH FOR DATA SECURITY AND PRIVACY?

Now that we have established the various risks associated with mass scale data collection let us look at the protections we have against such issues. Within the EU the only protection offered to data subjects regarding their data is the GDPR. The GDPR has now been active for almost three years which is a sufficiently high time for a new law to have major effects. However, from the discussion which follows we will see whether there are still issues on which the GDPR should work on.

1.2.1. The rules regarding legitimate interest

According to Article 6 of the GDPR there are only six conditions under which a company can process the personal data of individuals.[54] While this article is actually quite a strong article and lays down proper rules for processing one such condition for processing is legitimate interest. Legitimate interest is the most flexible ground for processing data under the GDPR. This is because almost anything can seemingly be legitimate interest. In general, an organisation just has to show three conditions in order to process any data due to legitimate interest. The conditions are

a. The processing isn't mandated by the law but there is a clear benefit to it
b. The risk of processing to the data subject's privacy is low

[52] Václav, J. Ownership of Personal Data in the Internet of Things (December 1, 2017). Computer Law & Security Review, 2018. 34(5). 1039-1052.
[53] Van Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E., Ascar, G. Security and Privacy in Online Social Networks. From social media service to advertising network: A critical analysis of Facebook's revised policies and terms [document on the Internet]. c2015 [cited 2016 Sep 14].
[54] Regulation (EU) 2016/679, (2016), *Supra Nota 18,* Article 6.

c. The data subject can reasonably expect their data to be processed for the purpose mentioned[55]

From a bare reading of this provision, it would appear that this provision is extremely vague.[56] Over the last few years the courts in the European Union have further defined the concept of legitimate interest however till date we still do not have a concrete definition.[57] If we take a look at each of the conditions mentioned above it becomes clear that these provisions may be misused by companies to process a multitude of different types of data. Condition 'a' specifies that the legitimate interest must have a clear benefit to it. However, should such benefit also include commercial benefits? Data subjects retain the right to challenge a processor's legitimate interest, however in the absence of clear cut rules it becomes difficult to understand whether such challenge would be successful or not.

1.2.2. Consent Forms and User Agreements

One of the major changes which the GDPR brought in was the importance of consent as one of the grounds for lawful processing. The consent required must also have to be clear and explicit.[58] Therefore, vague and confusing consent forms are barred by the GDPR. However, it appears as if organisations keep trying to work their way around the legislation. The GDPR does not say anything about the design of the consent forms. Therefore, organisations are free to design their own forms as long as they meet the basic requirements of being clear and explicit. One of the biggest problems here is that the companies who are designing the consent forms are the same people collecting the data of the data users. Since collecting data is generally in the interest of the companies, they often design consent forms in smart ways which while following the GDPR rules also may contribute to bending them.[59] The point of the rule on clear and explicit consent was to give the data subject a clear picture after which they could make an informed decision about giving their consent. However, in reality it is disputed whether this has happened.[60] If we

[55] When can you rely on Legitimate Interests?. Information Commissioner's Office UK. accessed on 25th April 2020.
[56] Kamara, I., De Hert, P. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. (August 8, 2018). Brussels Privacy Hub, Vol. 4, No. 12, August 2018.
[57] *Ibid*
[58] Regulation (EU) 2016/679, (2016), *Supra Nota 18,* Article 4(11) and Article 7.
[59] Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (Un)informed consent: Studying GDPR consent notices in the field. In: Conference on Computer and Communications Security (CCS) (ACM, 2019) 973–990
[60] Chesterman, S. (2017). Privacy and Our Digital Selves. The Straits Times.

casually browse through websites of most companies located within the EU, we find a few different types of cookie consent forms.[61]

Some websites simply have no option of refusing cookie tracking.[62] They also block further progression into the website unless one clicks on the accept button which authorises the company to install tracking cookies on the data subject's system. More often than not a data subject enters a website for a specific purpose. Perhaps he has entered the website of a newspaper to read an interesting article. At this stage when one is greeted with an obstacle which can be crossed by simply clicking an accept button, it is very likely that the data subject would choose to click it.[63] It would appear that most data subjects do not clearly understand the implications of data tracking. Therefore, when faced with the chance to access a page with a simple click most data subjects choose to just click it.[64]

The second type of consent forms which is fairly common in most websites is the form which gives every possible detail. Companies therefore may greet a data subject with options to reject or accept an endless list of data tracking permissions. To add to this many companies have designed their cookie consent forms in a very smart way intentionally making it very inconvenient for the user to reject all the cookies. An example of this would be to not include a reject all option but include an accept all option. The only way to reject would be to reject each and every permission one by one.[65]

It is even possible to find websites where in order to reject certain tracking options one would actually have to be redirected to third party webpages and then turn off tracking from there. The underlying problem with this set up is that the very entity who is being asked to design more transparent consent forms is also the entity who has an interest in collecting personal data. Unsurprisingly reports have found that users are not given any meaningful choice when faced with such consent forms.[66]

---

[61] Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P., and Santos, Igor. 2019. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19). Association for Computing Machinery, New York, NY, USA, 340–351.
[62] *Ibid*
[63] Vranaki, A. (2016). Social Networking Site Regulation: Facebook, Online Behavioral Ad- vertising, Power and Data Protection Laws. Queen Mary School of Law Legal Studies Research Paper No. 221, 29.
[64] *Ibid*
[65] Vranaki, (2016), *Supra Nota* 63.
[66] Vranaki, (2016), *Supra Nota* 63.

1.2.3. GDPR rules and Transparency

One of the purposes of the GDPR was to increase transparency in data collection and raise awareness. How it would appear that understanding the complexities of data collection and their use by companies would take a very long time.

Consider the example of opening a Google account simply because one wants to have an email address. At present the pdf version of Google's terms of service stands at sixteen pages consisting of various hyperlinks which may direct the user to further pages in order to give him more details.[67] While this method in a way does increase transparency, it is difficult to assume that most users are likely to read the entire terms of service. Despite the challenges, having such rules is essential and must not be removed even though they may not have the kind of impact they should be. This is because in the event that a data user actually challenges an organisation over their processing activities, the terms of agreement can be presented in court and carefully analysed. Conversely it may also be very difficult for bigger companies such as Google to present all their processing information in a concise and clear way. Therefore, a new model may have to be thought off if we want to increase the transparency involved in data collection.

1.2.4. The GDPR and anonymisation

One of the security methods the GDPR encourages is anonymization. That is a process by which data can be de-linked from any identifying element such that the data on its own becomes almost meaningless.[68] The idea is that if personal data can be anonymized then even in the event of a breach that data would not adversely affect anyone since there would be no way to tell who that data belongs to. However, while on the face of it, it seems like raw data cannot identify an individual it may actually not be true.[69]

It may actually be possible to identify individuals if raw data is accompanied by another set of raw data or ancillary data which can be equated to gather personal information. In the case of big data, many scholars have claimed that true anonymization is almost impossible simply because individuals can be identified by way of reidentification.[70] In fact, by analyzing mundane sets of

[67]Terms of Service, Google Inc, accessed on January 10th 2021
[68] Stalla-Bourdillon, S., Knight, A. (2017). Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization, and Personal Data. Wisconsin International Law Journal, 34, 284-322.
[69] Scholz, M. T. (2017). Big Data in Organizations and the Role of Human Resource Man- agement, a Complex Systems Theory-Based Conceptualization. New York: Peter Lang.
[70] Hern, A. (2019). Anonymized data can never be totally anonymous, says study, The Guardian.

anonymous data and cross referencing them to data sets, one can actually identify most individuals.[71] In the past movie preferences of users were deanonymized from an anonymous set of data provided by Netflix.[72] Similarly, the addresses of taxi drivers in New York were found by deanonymizing data sets related to individual taxi trips made in the city.[73] This being the case it seems like the concept of anonymization while still useful under certain conditions again fails to live up to its original purpose.

[71] Kulk, S., van Loevan, B. (2012). Brave New Open Data World?, International Journal of Spatial Data Infrastructure Research, 2012, Vol 7, 196-206
[72] Hern, A. (2014). New York taxi details can be extracted from anonymised data, researchers say. The Guardian.
[73] *Ibid*

2. CAN AN INTELLECTUAL PROPERTY BASED OWNERSHIP MODEL BE THE SOLUTION TO DATA PRIVACY AND SECURITY?

Now that we have seen that there may be legitimate concerns regarding the security and integrity of personal data, we will try to see whether a model which gives users more control over their data can help reduce these issues. Since data is a non-tangible asset, the most obvious choice to protect it better would be a model based on Intellectual Property. So now the real question is whether data subjects can actually claim to own IP over their personal data. Additionally, it would be wise to first explore whether there are sufficient arguments supporting the notion that data subjects should own IP over their data.

2.1. The rationale behind data subjects owning IP over their data

The primary argument for having IP rights for data subjects comes from the fears of security of such data[74] especially in an era where data is being manipulated at fearful rate.[75] Since privacy laws in its current form do not seem adequate to protect the abuse of personal information and data it would appear that an additional IP right would help.[76] It is also worth considering whether the individual deserves slightly more control over the data he or she has helped create. If not for purely economic reasons, then at least for reasons of security the idea of an IP protection over personal data for data subjects may be considered.[77] The idea of commoditization of data is emerging[78] although it is still not a very popular one currently since it has serious disadvantages. The most obvious one is that it might hinder research, development and progress by stifling

[74] Trakman, (2019), *Supra Nota* 3
[75] Dhanjani, N. (2015). Abusing the internet of things: blackouts, freakouts, and stakeouts. O'Reilly Media, Sebastopol, First Edition, ISBN: 063-6-920-03354-7
[76] Merges, P., Menell, P., Lemley, M., Jorde, T. (1997) Intellectual property in the new technological age. Aspen Law & Business, New Yor.k, 11–20
[77] Kamleitner B., Mitchell VW. (2018) Can Consumers Experience Ownership for Their Personal Data?From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints. In: Peck J., Shu S. (eds) Psychological Ownership and Consumer Behavior. Springer, Cham.
[78] Schwartz, P.M. (2004), Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055.

access to information.[79] The best solution would be to find a way to balance the human rights concerns of data subjects with the economic incentive which IP provides to data controllers.[80] The founder of the world wide web, Tim Bernes Lee is an advocate of granting full control over data to data subjects.[81] He however does not want it to become a property but rather a right.[82] One solution is offering an IP protection similar to the trade secret and sui generis protection which gives a similar kind of right in personal data without providing traditional property rights. Another option would be to perhaps grant data subjects absolute proprietary rights with the ability to trade their rights over the market.

Having established that there may be adequate reasons to perhaps explore the possibility of data subjects owning their data, it would be useful to look at the current EU laws regarding IP and personal data to see whether IP can exist over personal data in the first place. If that is indeed possible then it also has to be explored how such a right would work in the practical world. Additionally, the nature of the ownership right conformed on the data subject would also have to evaluated.

2.2. IP protection of personal data in the EU

As it stands today, companies and organizations are allowed to own IP over personal data. However, there is no such right available to data subjects.

The ethical concern over companies owning IP over personal data is that they would be able to know details such as where one lives, what kind of food ones prefers to eat, their political affiliations and other personal traits. On the flipside, it can be argued that companies have always relied on the commercial exploitation of user data through market research. Since companies invest in gathering such data and are heavily reliant on such data for their profits, it is natural that some form of protection of their investment must be in place. It is for this reason that perhaps unsurprisingly the law has allowed the commercial exploitation of data.[83] The GDPR allows the commercial exploitation of data by private parties by ways of direct marketing, customer

[79] Trakman, (2019), *Supra Nota* 3
[80] Trakman, (2019), *Supra Nota* 3
[81] Berners-Lee, T. (2019) Interview on the need to seek complete control of data.
[82] *Ibid*
[83] Regulation (EU) 2016/679, (2016), *Supra Nota 18,* Recital 101 and Recital 18.

profiling and also allows sales of customer data to third parties.[84] Since commercial exploitation is allowed it becomes extremely valuable for corporations to have control and ownership over their datasets.

2.3. Types of IP protection for personal data available in the EU

Since it is established that data sets offer enormous value to corporations, the next question is how they protect their investments to acquire and maintain such data. One of the ways in which this can be done is through IP Protection. The issue which comes to mind is that data does not satisfy the traditional conditions for IP protection. Traditionally IP has been divided in trademarks, patents and copyrights. Each of the three unique protections have some common elements, namely, they are all intangible products of human intellect and they have commercial value. While the specifics of Trademark, Patents and Copyright laws do not allow the protection of data in the traditional sense, new age IP's such as Trade Secrets and Data Base rights do.

2.3.1. Trade Secrets

Trade Secrets are protected as IP rights within the EU and can be found in the TRIPS agreement.[85] The minimum criterion for Trade Secret protection can be in Article 39 of the TRIPS agreement which states that in order to get the protection the information should be secret, have commercial value and can be shown to have been kept secret using reasonable steps.[86] Since the criterion is so broad, different member states within the EU have resorted to different protection mechanisms within their national law. To bring in more harmony across the different states in the EU, the Trade Secrets Directive[87] was passed. It is important to note that although it seems like the Trade Secret protection confers property rights on the holder of the secret, it is not the case. In fact, the purpose of the Directive is merely to prevent misappropriation of information which has been collected by the company.[88] The nature of the protection offered by the law on Trade Secrets however does seem quite vague and has been

[84] *Ibid*, Recital 24 and 47.
[85] Agreement On Trade-Related Aspects Of Intellectual Property Rights. The WIPO, 15th April, 1994
[86] *Ibid*, Article 39.
[87] 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
[88] DIRECTIVE (EU) 2016/943, (2016), *Ibid*, Recital 14 and 16,

widely debated.[89] This is accentuated by the fact there is no formal definition of what kind of information can be considered as a Trade Secret.[90] The TRIPS agreement specifies that any information can be protected as a trade secret as long as it has been kept secret using reasonable steps.[91] This information could be know-how of a particular product, list of clients, market information or any other business information of any other kind. Neither the TRIPS agreement nor the Directive attempts to clarify what constitutes business data. Therefore, from a plain reading of the sections and from European case laws it is evidence that sets of customer data can qualify as a trade secret as long as the other requirements of secrecy and reasonable steps are met.[92] The Directive is also extremely forgiving regarding its concept of commercial value and includes information which presents itself as both actual and potential commercial value. Finally, the directive is also quite lenient with respect to reasonable steps required to keep the information secret and portrays that the assessment of such criterion shall be proportional and made on a case by case basis. If we apply the conditions for Trade Secret protection to sets of personal data of customers then we can see that they do make a good case for such a protection. Sets of personal data must be kept secret as per the conditions of the GDPR. This is extremely important because the breach of data , especially sensitive data can be a massive violation of privacy. Therefore, the element of secrecy seems to be met by the GDPR itself. Moving on to the element of commercial value, it is no secret that customer data possesses an immense amount of value. For starters corporations invest money on human capital and technological capital in order to gather such data and therefore they have an interest in protecting their investment. Additionally, customer data is directly connected to a corporation's revenue since it directs their marketing strategy. It would seem that customer data is highly valued by corporations. Finally coming to the point of reasonable steps, we can observe that the GDPR imposes strict conditions under which personal data should be collected.[93] Hence, by virtue of being personal data, datasets seem to qualify for protection under the Trade Secrets law.

[89] Aplin, T. (2015), Right to Property and Trade Secrets, in: C. Geiger (Ed.), Research Handbook on Human Rights and Intellectual Property, Edward Elgar 421-437
[90] Baker & Mckenzie (2013), Study on Trade Secret and Confidential Business Information in the Internal Market, study prepared for the European Commission, Publication Office of the European Union.
[91] Sousa e Silva, N. (2014), What Exactly is a Trade Secret Under the Proposed Directive?, 9 (11) Journal of Intellectual Property Law & Practice 923.
[92] Torremans, P.L.C. (2015), The Road Towards the Harmonisation of Trade Secrets Law in the European Union, 20 Revista La Propiedad Inmaterial 27.
[93] Regulation (EU) 2016/679, (2016), *Supra Nota 18,* Article 6.

2.3.2. Sui Generis database right

The next IP right which datasets can be protected under is the sui generis database right. The database right was created through the Directive 96/9/EC.[94] Unlike the Trade Secrets right, this right confers proprietary benefits on the possessor[95] and is designed to protect the substantial investments made by the possessor to acquire the same. The database directive also confers a broad definition of what constitutes a database.[96] Essentially a database can be in any form whether written, digital or hybrid. What is important is that they must be information which is arranged systematically and must be accessible individually. Therefore, as long the information is organized and retrievable individually, the sui generis protection can apply regardless of what the data contained actually is. One of the defining criteria for database protection is substantial investment. The ECJ in its case laws has not laid down a proper test to identify what substantial means but has rather resorted to saying that it must not be very low.[97] However, the investment need not be only financial. The investment required for a database right may be made in human capital or may also be an investment in time and energy. The idea is to encourage corporations to take up new upcoming projects and different types of business ideas. Without any protection for their investments, there would be little incentive to pursue new innovative ideas. The type of protection offered is copyright in nature. The Database Directive however makes it clear that it does not protect investments made in creating new data. It only protects the investments made in obtaining, verifying and presenting data.

Considering the requirements for database rights, we can see that sets of personal customer data can easily be protected under the same. Indeed, many of the court in various member states have ruled the same. Just like the Trade Secrets directive, database rights can coexist with privacy laws.[98] This means that while sets of personal data can be collected and organized as a database, the same must be done keeping in mind the high standards of the GDPR. In order to satisfy the conditions of the sui generis right, companies will have to keep customer data in an organized manner so that they may be individually retrievable. Such is easily possible through modern data management tools. Companies invest in such tools and also hire human capital to use these tools. We can argue that there is a significant investment of money, time and energy in organizing data

[94] DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases
[95] *Ibid*, Article 7.
[96] Stamatoudi, I. (2002), To what extent are multimedia works films?, in: F. Dessemontet / R. Gani (Eds.), Creative ideas for intellectual property, The ATRIP Papers 2000 – 2001, CEDIDAC
[97] ECJ, Fixtures Marketing Ltd v Oy Veikkaus Ab., C-46/02, ECLI:EU:C:2004:694, para. 44
[98] *Supra nota* 94, Recital 18 and Article 7(4)

sets of personal data. Finally, these sets of personal data can be used in profiling and identifying target audiences for the products of the company. Therefore, these data sets are of immense commercial value for the companies. As such protecting sets of personal data should be possible under the sui generis rights of a database.

3. PERSONAL DATA, OWNERSHIP AND ITS PROTECTION

When we speak about data and its ownership, it is extremely important to understand its unique nature which makes applying traditional ownership models very tricky. Data is an intangible asset that holds extremely high commercial value. Individual pieces of personal data may have very low value[99] but when they are gathered in bulk, the value sees an unimaginable hike. Unlike traditional assets personal data can come in several forms each with its own challenges when it comes to its ownership.

3.1. Types of personal information and data

The first type is observable information which can be seen and perceived by individuals. This can be personal data contained in one's letters and even personal data which has been captured by a third party such as a photograph of an individual. The second category of personal data is observed information which is basically observable information which cannot be replicated by any party. In other words, this data is unique to an individual and reflects his personality. This could be anything from his name, work history, political preferences etc. Next, we have computed data which is essentially personal data which has been inferred by analyzing overserved and observable information. This data essentially describes unique qualities about an individual or a set of individuals. An example of this would be personality profiles created by Facebook after studying each individual's social media feed. Companies routinely make advertisement profiles of their customers so that they can come up with products better suited to

[99] Jennifer, R. (1998). "What Is Information?," Information Services & Use. 18 (4), 243-54
See Also:
Chaim, Z. (2007). "Conceptual Approaches for Defining Data, Information, and Knowledge,". Journal of the American Society for Information Science and Technology, 58 (4), 479-93.

them. This type of data is primary sold to companies who will benefit from such customer profiles and have an immense amount of value.

Lastly there is associated information which is data which on its own does not describe anything about an individual and on its own would not even qualify as personal data as per the GDPR. However, such information when combined with other observed or observable data may successfully identify an individual.[100] An example of this category of data could be IP addresses, bank account numbers etc. As we can see personal data can come in different forms and the primary challenge is to see whether the concepts of IP and ownership can apply uniformly throughout all such forms.

3.2. The unique nature of personal data

When speaking about granting an IP over a certain asset, the concept of ownership always comes into play. It is true when a musician says that they own an IP over their songs, it also means that they own that song, and any unauthorized misappropriation would be punishable as per IP laws. However, the concept of ownership through IP has always been slightly different from the traditional concept of the word. Traditionally ownership only applied to physical objects. And by its nature it conferred an exclusionary right over the object concerned. In other words, if a person owns the product, then that product automatically gets excluded from ownership by some other person. This is where IP differs.[101] While a musician may own a song, there could be millions of other people who also have access to that same song. Therefore, IP dose not confer exclusionary ownership of the product concerned.[102] Therefore, the idea of a data subject owning its personal data does not actually mean that that personal data cannot be used by another entity if it is legally licensed out to him.

Additionally, when it comes to personal data it might actually be very hard to confer any sort of ownership over them simply due to psychological reasons. While it may not occur to individuals instantly there are several psychological factors involved in how an individual feels ownership over a certain product. To start with human feel ownership over a product when the same

[100] Matuszewska, K. What is PII, non-PII and personal data? accessed on 10th January 2021.
[101] Chandra, R. (2009). Intellectual Property Rights: Excluding Other Rights of Other People. Economic and Political Weekly, 44(31), 86-93. Retrieved April 28, 2021.
[102] *Ibid*

product can be claimed by the human. Therefore, for a person to experience the feeling of ownership he must first be aware that the product exists.[103] When it comes to data it is very hard to actually know what the entire products is and how much of it actually exists. It is possible to make reasonable guesses to what kind of personal data a social media website may hold about him, but it is impossible to actually know the entire extent. One of biggest issues when appropriating any sort of rights over personal data is that individuals have no idea as to how much and exactly what data about them is held by organizations. Most people would probably say that Google Maps knows where they live and where they do to office. However, in reality Google Maps probably knows a lot more than that. A map app can possibly hold data on every single place visited by an individual in his lifetime. Moreover, they may use other complex algorithms combined with other services and derive several conclusions such where one's friends live and how likely one is to visit which friend's house. No individual would actually know the answers to these questions even though they have physically generated all this data. When personal data is used to come up with further conclusions thereby creating further personal data, it is impossible to know exactly what data a company has about an individual. Since no individual can ever be absolutely certain of what data about him exist, the question of ever claiming such data does not arise.[104] Therefore, claiming ownership over such data seems literally impossible.

3.3. Psychological aspects of ownership and their application on personal data

One aspect which makes data difficult to own is the concept of desirability and meaningfulness. Generally, humans claim ownership over what they consider valuable.[105] Consider the example of a person buying a tissue paper as opposed to buying a BMW car. It is highly unlikely that a person would refer to the tissue papers as 'my tissue papers'.[106] It's more likely that he would simply refer to them as 'the tissue papers. However, in the case of the BMW more often than not the person would refer to the car as his own. This notion comes from how desirable a product is to a person. If a product is not desirable at all to individuals then it is very unlikely that they

[103] Boulding. (1991), "Xxx," in To Have Possessions: A Handbook on Ownership and Property, Vol. 6, ed. Floyd Webster Rudmin: Select Press.
[104] Kamleitner, B., Stephan, D., Haddadi, H. (2016). "Can Users Price Real-Time Contextual Information?," WU Vienna Working Paper.
[105] Kamleitner, (2018), *Supra Nota* 77
[106] Kamleitner, (2018), *Supra Nota* 77

would claim ownership over it.[107] The same applies to the notion of meaningfulness. Individuals would often discard things which are meaningless in their lives even though they might have paid for it. No one would claim ownership over a single matchstick in spite of the fact that they may have bought the matchbox for real money. When it comes to personal data we can see that only small specific parts of it seem attractive and meaningful. While an individual's Facebook account might hold value and be meaningful to him,[108] the same cannot be said about all the other personal data which Facebook may have of him. Data which is available in code is hardly attractive or meaningful to the average data subject and therefore it becomes very hard for that data subject to actually feel any ownership over the same.

Next comes the concept of fungibility. psychologically individuals find it easy to claim ownership over objects which are not easily replaceable, and which can be personalized. The argument steps from the fact that once a user has used a certain product for an amount of time, that product starts reflecting the essence of that person.[109] Moreover, products which can be personalized to reflect the owner's own personality have a higher chance of being claimed by the owner. This is why tennis players feel a unique sense of ownership over their rackets although the exact same racket may be available in every store in the world. When it comes to personal data the concepts of replaceability and personalisability do not seem to apply. While theoretically it is true that one's location history is unique to that person and therefore in a way contains the essence of that person, the sheer fact that we cannot feel the product or personalize the product due to its intangible nature makes us unable to feel ownership over it. Except for the most basic personal data which might include your name and your date of birth, all other pieces of personal data seem too remote to be capable of personalization.[110]

Psychologically we also tend to claim ownership over things which we can control.[111] The issue with personal data is that not only is there too much of it, but we also have very little control over it. Personal data is also too vast in scope and therefore almost incomprehensible to the average person. The GDPR defines personal data as any data which can identify a natural person

[107] L. Pierce, J., Kostova, T and T. Dirks, K. (2003). "The State of Psychological Ownership: Integrating and Extending a Century of Research," Review of general Psychology, 7 (1), 84-107.
[108] Kamleitner, (2018), *Supra Nota* 77
[109] Argo, J.J, W. Dahl. D., and C. Morales, A. (2006). "Consumer Contamination: How Consumers React to Products Touched by Others," Journal of Marketing, 70 (2), 81-94
[110] Kamleitner, (2018), *Supra Nota* 77.
[111] L. Baxter, W., Aurisicchio, M. and R. N. Childs, P. (2015). "A Psychological Ownership Approach to Designing Object Attachment," Journal of Engineering Design, 26 (4-6), 140-56.

or lead to its identification. However, the law is extremely broad on that definition. Almost any data can be personal data if when combined with other pieces of data it leads to the identification of a person. Therefore, even an IP address which merely identifies a computer located in a place can also be classified as personal data under certain circumstances. Since there is virtually no limit on what can constitute personal data it is impossible for an individual to effectively control.[112]

Data subjects also seem to claim ownership over objects which they have themselves created.[113] A creation can be the result of investment of any sort. Essentially when a person has invested time, labour or money on an object they tend to feel a sense of ownership over it.[114] Therefore, the effort that goes into the creation of the product confers this feeling on the individual. While most personal data is in a way created by individuals, they hardly play any role in the creation. Personal data seem to be generated as a byproduct of an individual's life. The actual monetary investment which was put into the systems which track such personal data was put in by technology companies and not the individual themselves. This makes it extremely difficult for an average individual to feel a sense of ownership over his personal data.

Finally, individuals struggle to attribute the feeling of ownership over personal data because it is just too vast and complex[115] an idea to fathom for most people. An average person would not be able to fathom the vast number of data points which collectively form his digital personality on a social media site. For example, there might be thousands of personality points which a social media has identified about a person based on thousands of posts he made over the last twenty years of his life. The only way that personal data can somewhat be perceivable to the average user would be to group them together in meaningful clusters.[116] Therefore, if all data related to a person's movements using a taxi application is grouped as location data, then it's possible for a person to comprehend it. However, if the same data exists as individual trips, it becomes impossible to comprehend them and hence claim ownership over them.

---

[112] *Supra Nota* 108

[113] Kanngiesser, P., Itakura, S., and M. Hood, B. (2014). "The Effect of Labour on Ownership Decisions in Two Cultures: Developmental Evidence from Japan and the United Kingdom,". British Journal of Developmental Psychology, 32 (3), 320-29.

[114] Kamleitner, (2018), *Supra Nota* 77.

[115] Acquisti, A., Taylor, C., and Wagman, L. (2016), "The Economics of Privacy," Journal of Economic Literature, 54 (2), 442-92.

[116] Kamleitner, (2018), *Supra Nota* 77

3.4. The ownership model of protecting personal data and its challenges

As we can see the idea of feeling ownership over personal data maybe tougher to achieve that expected. It may sound like a noble idea on the face of it, but it seems that it won't make sense unless the law can get individuals to legitimately care about their data. This makes us question whether ownership over personal data would serve any purpose at all. We all know that ownership over data which companies can experience through trade secret and sui generis regimes are definitely extremely useful to them. But this is primarily because those data are valued extremely highly by companies since it directly relates to their profits. Therefore, companies often feel a strong sense of ownership over the personal data of individuals which they own. However, it seems like there are no such incentives provided to data subjects to make them feel the same way.

There are certain other issues when deploying a strict ownership model over personal data. The traditional model of ownership implies that there can only be one owner of the asset at any given point of time. Additionally, the ownership can change if the first owner decides to sell his ownership to a third party. This is however when it comes to data. The same data can be owned by multiple people since there can be more than one version of the same data. Our personal data such as our names and addresses have been entered multiple times on multiple online websites and now each of those websites own the same data. This makes it extremely difficult to regulate and protect data since there is a multiplicity of data across various platforms. The biggest concern seems to be that data can be sold for compensation. While this sounds good in principle since every data subject will now be entitled to some compensation in exchange of his personal data this thesis would argue that such a situation is not the best suited to achieve its ultimate goal. The ultimate goal of this thesis is to explore if personal data security can be improved from what it is currently through the protection of IP. If data subjects own personal data in the traditional sense such that they may be able to freely sell it to anyone[117] then after a period of time the situation would revert to what it is today. Corporations would eventually buy all the personal data available from consumer's willing to part with them. As explained previously most consumers are unable to feel ownership over their personal data. Most consumers do not even care about privacy of their personal data due to the fact that they do not truly understand the important of it.[118] This being the case, consumers might see this new arrangement as one which

[117] Litman, J. (2000). Information Privacy/Information Property. Stanford Law Review, 52, 1283.
[118] Kamleitner, (2018), *Supra Nota* 77

gives them free income and sell all their personal data to corporations. It is true that in some cases, consumers will refuse to sell their data to corporations or may demand an adequately high price for the same but in most other cases, corporations may easily be able to acquire the personal data from consumers for relatively cheap prices. This means that a proprietary model of personal data for data subjects may just result in the companies parting with some capital initially but in the long run they may acquire monopoly over the data as they do today. Therefore, this model would probably not serve any purpose.

The concept of data subjects having ownership over their data also seems unfair from the perspective of large corporations. This is because data subjects typically do not put in any investment to generate their data. Most of the investment is actually put in by corporations to collect and analyze the data. Typically, corporations put in the time, labour and monetary investment to make sure they have the infrastructure required to aggregate and analyze personal data fed by data subjects. In the case of computed and associated data, the investment required is even greater since the data in its original form has little value. Therefore, it would be extremely unfair to give traditional ownership rights to data subjects when they have put in the investment.

3.5. A rights-based approach to protect personal data?

Perhaps the best way to look at personal data would be through a right based system and not an ownership based system. Data rights should be akin to fundamental rights.[119] No individual has helped create their right to freedom of expression. Such rights are vested in individuals by the society simply by virtue of being an individual.[120] Similarly, such rights cannot be sold or waived off. Individuals should not be allowed to waive off their right to dignity for example. Perhaps data can be looked upon similarly. Data subjects should not be allowed to own their personal data in the traditional sense, but they should have extremely powerful rights over them. Additionally, they should also not have the option to sell or waive off this right because that would defeat the purpose. The only downside to such an argument would be such powerful

[119] Rodotà S. (2009) Data Protection as a Fundamental Right. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht.
See also: Oostveen, M., & Irion, K. (2018). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? In M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, & G. Surblyt-Namaviien (Eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? (7-26). (MPI Studies on Intellectual Property and Competition Law; Vol. 28). Berlin: Springer.
[120] Chatterjee, S. (2019), "Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective", International Journal of Law and Management, Vol. 61 No. 1, 170-190.

rights may disincentivize corporations for using personal data for analysis. It goes without saying that sometimes personal data analysis is extremely important for the society in general. While Facebook's personality predicting algorithms may not be useful for the society but analysis of medical records to identify public health levels and trends or use of personal data to help in the field of data is extremely useful. Moreover, even companies such as Facebook may rely on personal data to provide certain basic services. For example, to help you connect with your network better the Facebook algorithm needs to analyze personal photos, friends and the social feed and then give suggestions of potential new friends who one might know. Therefore, for some companies the entire business model is based on personal data. The problem which this thesis is trying to solve is not the basic use of data by large corporations for their day to day business but the pervasive abuse of data. Therefore, the challenge would be to balance the personal rights of data subjects to the economic needs of the society. It does however seem to me that such a balance is possible especially through the route of intellectual property.

3.6. An IP right over personal data for data subjects?

From the above discussions we can see that it is indeed possible for an IP to exist over personal data. Therefore, prima facie it is possible for data subjects to own an IP over their personal data as well. In fact, there is a trend in various Court decisions which follows that perhaps data subjects should also have some sort of IP over the data they create.[121] The same position has also been taken by various scholars over the years.[122]

In fact, the clauses of the GDPR pertaining to sensitive data and the value placed on consent, seems to suggest that regulators hold the interest of the data subjects very highly. Therefore, it would seem like the notion of data subjects owning an IP over their data should not be unacceptable in principle.

As seen above the concept of ownership as an additional protection against misuse of personal data may be contested. This does not however discourage the use of IP to fill in the gap. The IP

[121] Coogan v. News Group Newspapers Ltd [2012] EWCA Civ 48, [2012] 2 WLR 84, [2012] EMLR 14, [2012] 2 All ER 74.
See also: Price v. Hal Roach Studios, Inc., 400 F. Supp. 836 (S.D.N.Y. 1975).
[122] Trakman, (2019), *Supra Nota* 3

model appears to offer the perfect middle ground to balance the interest of both individuals and corporations alike and has several distinct advantages.

Firstly, the IP model would allow the licensing of personal data to corporations in order to provide personalised services. At the same time the IP would protect data subjects from misuse of their data since they would retain control over their data at all times. This would immediately solve the problem of consent and misuse with downstream users of personal data. Therefore this model would help increase the level of privacy and at the same time also provide a platform for corporations to keep providing services.

As discussed previously EU data protection laws are designed to work hand in hand with IP laws.[123] Therefore the IP protection would be an added level of protection for data subjects. Corporations would still be obligated to maintain data protection principles as specified in Article 6 of the GDPR, when processing personal data.

Additionally, IP rights are largely developed in most jurisdictions over the world.[124] Therefore adding such rights to personal data would make it possible for data subjects to get some protection over their data even if they are located in a jurisdiction which does not have a well developed data protection regime. It would therefore appear that having IP as an additional right for data subjects would lead to a much higher level of privacy and security over personal data. With that being said it is important to highlight the exact nature of this right, what it would look like practically and whether it is indeed feasible.

4. PRACTICAL APPLICATIONS AND MODELS

Having established that the IP model of protection has legitimate benefits when combined with the current data protection regime it would also be wise to look at certain practical models with which this idea could actually be implemented. Not surprisingly there are several companies who

[123] *Supra nota* 94, Recital 18 and Article 7(4)
[124] WIPO (2020). World Intellectual Property Indicators 2020. Geneva: World Intellectual Property Organization, accessed on 10th April 2021

have expressed the idea of granting data subjects control over their data when using their services. The caveat here is that most of these companies are still new and there is no guarantee that these companies will end up being sustainable in the long run. While these companies do not explicitly speak about the nature of the right which data subjects Will have over their data, it does seem like their models could work or at least provide inspiration for future models giving data subjects IP rights over their data.

4.1. SOLID by Inrupt

One of the best models present today is the Solid Privacy Platform developed by Tim Bernes Lee´s startup Inrupt. The idea behind Solid (Socially Linked Data) is to give users almost total control and true ownership over their own data.[125] Instead of companies owning the data sets of customers, Tim Bernes Lee proposes the idea of a PODS or personal online data stores which will store the personal data of data subjects.[126] This data will always be stored on these pods and cannot be copied by any other company.[127] These pods can be hosted on the servers of certain partner companies or they can be hosted on a data subjects own personal server.[128] When storing the personal data on third party servers, the third party would have access to the personal data. However, no party can actually copy or sell that data from the pods. At most they may get permission to read and write the data on the pod, a permission which can be withdrawn anytime by the user. Therefore, in practice the personal data of users will never go outside the pod.[129]

The company is also encouraging other companies to create apps which would work within the PODS infrastructure. All such applications will be decentralized[130] and not be able to store any

[125] Essam, M., Andrei Vlad S., Sandro H., Maged Z., Sarven C., Abdurrahman G., Ashraf A., and Berners-Lee, T., (2016). A Demonstration of the Solid Platform for Social Web Applications. In Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 223–226.
[126] About Inrupt and Solid. accessed on 10th April 2021
[127] *Ibid*
[128] Solanki, M.R. (2021) SOLID: A Web System to Restore the Control of Users' Personal Data. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore.
[129] *Ibid*
[130] Werbrouck, J., Pauwels, P., Beetz, J., & van Berlo, L. (2019). Towards a decentralised common data environment using linked building data and the solid ecosystem. In B. Kumar, F. Rahimian, D. Greenwood, & T. Hartmann (Eds.), Advances in ICT in Design, Construction and Management in Architecture, Engineering,

personal data from the PODS. PODS may also be split into several smaller PODS containing specific personal data.[131] For example, a data subject could have one POD containing his medical data and one containing financial information. This would give the data subject the option to only grant access to relevant PODS when using applications. For example, to make online payments the payment gateway would in principle only access the POD containing the financial data of the data subject and not have any access to the medical data. Let's take an example of a taxi company operating on the PODS infrastructure. For a taxi application to work efficiently, the company would access to your location and other personal data such as name and perhaps your photograph. Therefore, if a data subject would wish to use that application, they would first have to give permission to the taxi application to read and write only those personal data which are required from his pod. By giving this permission the user could use the taxi app. However, the taxi app would never have real control over this location data and therefore they would never be able to sell it on to other third parties. Secondly since the taxi app does not actually have the data on any servers under their control, there is no question of a data breach happening from their servers. Thirdly if the data user decides to stop using that application, he could simply revoke the permission[132] given to the taxi application and then the taxi application would not have access to the personal data of the data subject.

4.2. The Personal Data Storage System Model

The PODS system will also solve the issue of multiplicity and accuracy of data. Now personal data will only be stored in one location in the world and can only be modified by the data subject himself.[133] Therefore, the data subject can update their personal data themselves.[134] The PODS system may also solve the complex issue of data portability. Although the GDPR has brought in the concept of data portability such a concept may not be present in other data protection regimes. Moreover, it may be years before this new right can be used quickly and effectively. The entire process of data portability would be streamlined within the PODS infrastructure since the data subject has total control over his or her data. They know where the data exists and there

Construction and Operations (AECO) : Proceedings of the 36th CIB W78 2019 Conference (113–123). Newcastle, UK.

[131] About Inrupt and Solid, (2021), *Supra Nota* 126
[132] About Inrupt and Solid, (2021), *Supra Nota* 126
[133] About Inrupt and Solid, (2021), *Supra Nota* 126
[134] About Inrupt and Solid, (2021), *Supra Nota* 126

is only one copy of the data. Therefore, transferring data between two different services would be as simple as withdrawing consent from one service and giving consent to the other. This would streamline many services and make them faster. The medical service for example would greatly benefit since now your entire medical data will be stored in your pod and the user can approve certain doctors to read certain parts of that data and add notes to them. These notes can then be shown to other doctors subsequently if required. Therefore, there would be no need to give your medical data to multiple medical services or maintain a huge medical file containing your entire medical history to show to every medical doctor you visit.

The National Health service of the UK has already signed up to use the Solid Platform[135] which is already a step towards the right way. What Bernes Lee hopes to accomplish through this model is a brand new way for data subjects to interact with the internet. The next generation of data subjects will definitely be more privacy oriented, and this model would be a very easy way for them to maintain the privacy. The PODS infrastructure is also likely to create a new business model for large companies whose current economic model rely on harvesting and selling personal data. To maintain the balance between the privacy rights of data subjects and economic interests of technology companies, SOLID is encouraging companies to build their own decentralized applications on the SOLID network. In fact, some applications have already been created on the SOLID infrastructure including a social networking application.[136] However, the economic model for these applications cannot be based on collecting and selling data. There are many other routes to be followed such as advertisements or even charging a subscription fee. SOLID is currently at a nascent state and there are still several challenging questions which it has to answer before it becomes commercially viable, however in principle this could be a decent model which could support an IP right for data subjects.

Additionally, companies such as Digi.me, MyDex and Hub of all Things are using personal data storage systems[137] to provide similar services as SOLID. All these companies differ slightly in terms of business model, target audience and technology, however their primary purpose is similar, i.e., giving data subjects control over their data. The idea of giving data subjects full

[135] Cellan-Jones, R.. NHS data: Can web creator Tim Brenes-Lee fix it? BBC News, Accessed on 10th April 2021
[136] Solid Applications. accessed on 12th April 2021
[137] European Data Protection Supervisor, 'EDPS Opinion on Personal Information Management Systems' (Opinion No 9/2016. 20th October, 2016.

control over their data is currently also being tested out by Microsoft´s Bali project.[138] Similar trends can also be seen in the telecommunications industries with Telefonica´s Aura system.[139] All these new projects have their own set of challenges and concerns however they do not form a part of this thesis. The primary question is whether we can envisage an IP right for data subjects using such ecosystems as a model. From the look of how these platforms have been designed it seems to me that we can.

Looking closely at the platforms and their systems, it can be seen that none of these services have explicitly spoken about the nature of the right the data subjects would possess over their data stored in the personal storage devices. In fact, some of these services use the word ownership although it is unclear what exactly they mean by it. As explained previously in this thesis, control is more important that traditional ownership. Traditional ownership also has the issue of a data subject having the power to alienate his stored data.[140] This is a problematic issue and therefore a better model would be one where the data subject has a clear but non alienable IP over his entire data stored within such ecosystems. Looking at the IP systems which are already in place today, I do not see why that would be impossible to imagine.

4.3. Weaknesses of the present models

The model suggested above obviously has many concerns and weaknesses. The first consideration is that we still do not have a lot of information available about the real life models such as SOLID. Therefore, the final versions of these ecosystems could end up being drastically different. However, the purpose of this thesis is to explore whether the idea of giving IP rights to data subjects can actually work and if they do , see how they can be used within a practical model. From our discussion above it seems like this could be done. Having said that we can now look at the weaknesses which the final model would have to solve.

[138] Microsoft Research, accessed on 12th April 2021
[139] Telefónica, 'Telefónica presents AURA, a pioneering way in the industry to interact with customers based on cognitive intelligence' (press release, 26 February 2017)
[140] Litman, J. (2000). *Supra Nota,* 117.

4.3.1. Incentives for data subjects are not high enough

When we look at why big technology companies have so many data subjects using their services the answer becomes quite clear. Most technology companies are offering something very addictive. Facebook gives the option to create a large social network and get in touch with long lost friends, Google provides the best search engine in the world etc. Unfortunately, the incentive is not strong enough for data subjects to move to this new privacy centric ecosystem.[141] The only attractive feature within these ecosystems is that your data will remain private. However, considering the fact that the majority of the individuals are still not very invested in the security of their personal data, these ecosystems will need to come up with something more attractive than just the lure of privacy. Additionally, data subjects would have the added inconvenience of leaving established services to now be a part of the new ecosystem.[142] Therefore, they would have to give up all the privileges they enjoyed on these services for new and potentially untested solutions. Hence raising awareness about privacy rights and their importance would be key in driving the population to use these new services.

4.3.2. IP protection under the model ecosystem will not help prevent the breach of personal data already in the hands of corporations

The big issue with suggesting the new ecosystem is that it will take time to develop into a fully-fledged system which is trusted by a major part of the population. Additionally, many data subjects will choose to stay loyal to their preferred service providers.[143] However even if we assume that every single data subject in the world reverts to the new ecosystem, that still would not solve the risks with personal data which already exists with technology companies.[144] Therefore, the chances of breaches and misuse would still be there long after every data subject has switched to a more secure ecosystem. It will be many years before the personal data controlled by the technology companies become irrelevant and outdated. Until then the risks would stay the same even with the added protection offered through IP.

[141] Bolychevsk, I. How solid is Tim's plan to redecentralize the web?. Medium.com, accessed on 5th April 202.
[142] *Ibid*
[143] Bernoff, J. What would it take for Tim Berners-Lee's new Web replacement to succeed? Medium.com, accessed on 4th April 2021
[144] *Ibid*

CONCLUSION

From our analysis of the research questions above, it seems that IP protection of personal data will lead to a higher level of privacy for data subjects. Even though this concept is at a nascent stage, the early indications are that such a right may become a reality soon. Although current IP systems do not fit the profile of personal data, it may not be too much of a stretch to envisage a completely new type of IP specifically designed for personal data. Computer programs were not considered copyrightable in the past and even the sui generis database right is a fairly new creation. Therefore, as the society becomes more privacy centric the need for an additional data security may create a completely new IP. Another option which may arise would be to tweak current IP systems to become compatible with protecting personal data. IP protection of personal data in the form suggested in the thesis would come closest to Tim Bernes Lee's dream of data subjects getting control over their data through an inalienable right. Such an approach could also start a chain reaction of creating more privacy centric corporations. Personal data storage devices present us a unique way of creating and controlling our digital portfolio. In many ways it seems almost natural that every individual should have a right over his own portfolio similar to how celebrities have rights over their name and image. The suggested model would totally eliminate the problem of personal data flowing out of the hands of the data subject and therefore reduce the chances of breaches and misuses in the future. It would also help create a more responsible society built on trust and security. The suggested model would probably crush the current business model of technology companies which is based on harvesting of personal data. Instead, they would have to come up with a more privacy friendly economic model to run their businesses. Of course, there are still many challenges and concerns which must be overcome before such a model becomes a reality. However, from the discussions above it seems like this model deserves some serious though and attention in the future.

The IP protection of personal data for data subjects remains a hotly contested issue till date. While there is significant opposition for the same, there are enough reasons to at least think about it. This thesis has demonstrated that offering IP protection over data sets of personal data to data subjects in addition to standard data protection laws would lead to a higher standard of privacy and reduce the misuse of data. The thesis has given its view on how such a right should manifest itself and why it should be done in such a way. The thesis has also revealed that there are several practical models which can serve as inspiration to accommodate such a right and how such a right would

have a massive impact in changing the way corporations do business in the world. However there still exists various challenges which need to be solved before such models become a reality. Perhaps the biggest one being that there currently exists no IP regime which would seamlessly fit into the models which were suggested. Therefore it may be so that a entirely new IP right would need to be created in order to give data subjects the right in its ideal form. Without any existing IP regime, the future of having IP rights over personal data would depend on the action of concerned citizens and governments alike. However this thesis has demonstrated that it may be in the interest of both these parties to lobby for reforms as may be required in order to acquire such a right. The thesis has shown that there are several reasons why such a right should be thought about in the form mentioned in the thesis and has demonstrated that it is definitely possible to envisage such a right in the future. Whether or not such a right materializes in the future or not, it is clear from this thesis, that this idea atleast deserves additional research and consideration by scholars and the legal fraternity at large.

5. FINAL ANALYSIS AND FINDINGS

5.1. Using existing IP models to protect personal data may not work

In all the services mentioned, the central theme is that personal data would be stored on some sort of a private server and that the data subject would have complete control over this data for eternity. The personal data stored on these personal data storage devices would essentially take the form of a database. From our analysis of the research questions above, we now know that sets of personal data can easily qualify for a database protection. The only other criterion to get such a protection would be to put in investment. The personal data which these data storage devices would contain would represent the personality of an individual and can be further subcategorized into smaller sets when using the SOLID ecosystem. Therefore, one could argue that there is enough options of customization available to the data set. Additionally, most of these data sets would be created by the data subject themselves. All contact and personality details such as name, address and even financial details would have to be fed into these storage devices by the data subject. Even in the case of computed and associated personal data which could be generated by applications on the personal data storage ecosystem involve some level of investment from the data subject. As mentioned before the Database Directive is extremely lenient when it comes to the type of investment required. The investment could therefore come in the form of time and effort. In certain cases, data subjects could actually need to pay a subscription fees to avail of this service. Therefore, there is an element of monetary investment as well. Such being the case the data subject could definitely possess sui generis right over all the personal data contained in these data storage devices. The issue of implementing the database system of rights for data subjects is that database rights confer traditional property rights over the owner. This means that the data subject could have the option of selling his database to a third party. Our analysis of the research questions previously has shown why this is potentially dangerous. It is possible that the platforms mentioned earlier could outright bar this from happening. For example, the platforms could implement general security rules which meant that once a data subject owns a personal database, they own it forever and cannot sell it. However, if

we are to implement the database IP right in its current form, the rules would contradict each other. In our opinion, the best option would be having an inalienable IP right akin to human rights. Since privacy has already been defined as a human right this should not be impossible. However, IP rights must be the same for everyone. We cannot have a database rights system which allows corporations to have proprietary rights over their databases but deny data subjects from having the same benefit. There it seems that the Database Directive in its current form would fall short in this regard.

The Trade Secrets Directive however could be a step in the right direction. As pointed out during the analysis of the research questions, the Trade Secret Directive does not grant exclusive rights to the IP owner but serves merely as a right against misappropriation. To qualify for such a protection, the Trade Secrets Directive mandates secrecy, commercial value and reasonable steps to keep the information secret. On the face of it, it seems like personal datasets stored in persona data storage systems on the cloud would qualify for such a protection. Personal data obviously has huge commercial value and by its very nature has to be kept secret. The business models of Mydex for example is based on keeping the personal data of data subjects secret by using highly advanced security.[145] Moreover, the GDPR mandates the secrecy of personal data. The Trade Secret Directive also mandates that reasonable steps must have been taken to keep the data secret. This can also be satisfied under the current model. The very fact that data subjects are engaging in personal data storage capabilities mean that they are taking steps to keep their data a secret. The issue however arises when one considers whether the secrecy of personal data stored within the personal data storage system would be challenged when the customer allows the use of this personal data for certain services. A data subject using this ecosystem would at point give consent to an application to read and write his personal data. It is still not clear whether at this stage the personal data would still be considered as a trade secret. Trade Secrets typically loses its protection once the information becomes public knowledge.[146] Now it can be argued that allowing a few apps to use the personal information is not the same as the data becoming public knowledge. However, there is some confusion in this regard. Another challenge is that although the Trade Secret Directive does not give exclusive rights to its holder unlike the other IP rights,

[145] About MyDex, accessed on 10th February 2021
[146] Legal protection of trade secret and know-how. (2007). Ius Mentis, Law and technology explained. Accessed on 10th January 2021.

Trade Secrets can still be bought and sold. Therefore, they suffer from the same issue which we face with the sui generis protection.

It therefore seems that the current IP models which the world has all suffer from some issue or another and perhaps none of them can be directly implemented to work on data subject's rights in their present form.

5.2. Essential elements of the ideal model

The ideal protection which data subjects should receive should be an inalienable right in the form of an IP. If such an IP can be developed, then the model presented by companies such as SOLID and MyDex can serve as an effective inspiration. This is because most of the rights and benefits which an IP holder has can be satisfied through these models. For example, the models listed above allow data subjects to give consent to third parties for using their data. The consent given is contractual in nature and could definitely be seen a license agreement. Therefore, if an IP system can be implemented within these models, a licensing contract can be drawn up between the data subject and every third party application who uses the data similar to how an IP would be licensed out. The only difference in such a license agreement would be that it should not have fixed time commitment which is quite common to have in standard IP licenses. Instead, these license agreements would have to have a feature which allows the data subject to opt out at any given point and thereby terminate the license.

5.3. Advantages of an additional IP right within the ideal model

A big advantage of this new model would be that Intellectual Property rights are capable of working hand in hand with data protection regimes.[147] This would lead to enhanced levels of protection for data subjects since now their data could be protected by two complementary regimes. The idea which is being proposed is that the data subject would have an IP over his entire personal data set. This could essentially be an IP portfolio of one´s personality. These portfolios would be specific to each and every individual since they would all be unique and therefore distinctive. This idea would be similar to the protection received by a trademark except

[147] *Supra nota* 94, Recital 18 and Article 7(4)

that here the distinctiveness cannot be visually seen. The IP right could protect a data subject in case there is any misrepresentation made using his personal data similar to the law of passing off for trademarks. For example, if in a data breach an individual's social security number is compromised and is used eventually by the perpetrator to buy a house, then the data subject would have the power to raise a claim against him not only under traditional civil/criminal laws and data protection laws but also through IP laws. Therefore, IP laws would operate in case there is any misuse of the personal data stored in personal data storage ecosystems along with data protection and traditional civil and criminal laws. Data protection rules would also operate within such an ecosystem and go hand in hand with the IP protection enjoyed by the data subject. For example, the principles of data minimization, data protection by design and consent would apply to all entities involved in the ecosystem, i.e., service providers such as SOLID as well as all third parties who interact with the data subject such as application developers. Since both data protection and IP laws would also apply to service providers, it would ensure that all such providers would have to consistently keep their privacy standards at a very high level. IP laws would also ensure that data subjects would have an additional claim over the ecosystem providers in case any personal data is compromised due to an error on their part. The biggest advantage of the IP system would be that it would give data subjects absolute rights over their personal data even if an ecosystem allows sublicensing of the personal data in any way. Therefore, data subjects can now have a claim over downstream users as well.

The ideal model which data subjects deserve could end up being a combination of the ideas seen from some of the models which exist today. The most important rules which should be followed is that the data should always stay with the data subject in a place which is always accessible by them. This data can only be licensed and never be allowed to be sold. The IP right therefore which a data subject would have would be inalienable and can be used at any given point of time. Since Licensing is allowed, data subjects should be incentivized to license their data to essential services such as for medical research. This would ensure that the rare benefits of large scale data processing in the fields of research are not adversely affected. The concept of renewal of the IP should also not apply in this case since it would not make sense if a data subject suddenly lost her IP right in her personal data if she forgets to renew them. Similarly charging subscription fees from the data subjects to build these databases would disincentivize data subjects to sign up on these ecosystems and is therefore not recommended. It may be so that these ecosystems have to rely on a different business model to make their project successful.

LIST OF REFERENCES

Scientific Books

1. Chandra, R. (2009). Intellectual Property Rights: Excluding Other Rights of Other People. Economic and Political Weekly, 44(31), 86-93. Retrieved April 28, 2021, from http://www.jstor.org/stable/25663395

2. Cheng L., Liu F., Yao D. (September/October 2017), Enterprise data breaches: causes, challenges, prevention and future directions, Wires Data Mining and Knowledge Discovery, Vol 7, Issue 5, https://doi.org/10.1002/widm.1211

3. Dhanjani, N. (2015). Abusing the internet of things: blackouts, freakouts, and stakeouts. O'Reilly Media, Sebastopol, First Edition, ISBN: 063-6-920-03354-7

4. Lewandowsky, S., Smillie, L., Garcia, D., Hertwig, R., Weatherall, J., Egidy, S., Robertson, R.E., O'connor, C., Kozyreva, A., Lorenz-Spreen, P., Blaschke, Y. and Leiser, M. (2020). Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making, EUR 30422 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-24088-4 (online),978-92-76-24089-1 (print), doi:10.2760/709177 (online),10.2760/593478 (print), JRC122023.

5. Mitrou, L. (2017). The General Data Protection Regulation, New Law, New Obligations, New Rights. Greece: Sakkoulas. 466

Scientific Articles

1. Acquisti, A., Taylor, C., and Wagman, L. (2016), "The Economics of Privacy," Journal of Economic Literature, 54 (2), 442-92.

2. Andrews, V. (2019). Analyzing Awareness on Data Privacy. In Proceedings of the 2019 ACM Southeast Conference (ACM SE '19). Association for Computing Machinery, New York, NY, USA, 198–201. DOI:https://doi.org/10.1145/3299815.3314458

3. Aplin, T. (2015), Right to Property and Trade Secrets, in: C. Geiger (Ed.), Research Handbook on Human Rights and Intellectual Property, Edward Elgar 421-437 (also available at: http://ssrn.com/abstract=2620999)

4. Argo, J.J, W. Dahl. D., and C. Morales, A. (2006). "Consumer Contamination: How Consumers React to Products Touched by Others," Journal of Marketing, 70 (2), 81-94

5. Baxter, W., Aurisicchio, M. and R. N. Childs, P. (2015). "A Psychological Ownership Approach to Designing Object Attachment," Journal of Engineering Design, 26 (4-6), 140-56.

6. Beales, H., Craswell, R., C. Salop,S. The efficient regulation of consumer information, Journal of Law and Economics. 24. (1981), 491-539

7. Bottis, M., Bouchagiar, G. (2018). Personal Data v. Big Data in the EU: Control Lost, Discrimina- tion Found. Open Journal of Philosophy, 8, 192-205 https://doi.org/10.4236/ojpp.2018.83014

8. Boulding. (1991). "Xxx," in To Have Possessions: A Handbook on Ownership and Property, Vol. 6, ed. Floyd Webster Rudmin: Select Press.

9. Breitbarth, P. (2019) The impact of GDPR one year on. Network Security, Volume 2019, Issue 7, 2019, 11-13, ISSN1353-4858,https://doi.org/10.1016/S1353-4858(19)30084-4. (https://www.sciencedirect.com/science/article/pii/S1353485819300844)

10. Chaim, Z. (2007). "Conceptual Approaches for Defining Data, Information, and Knowledge,". Journal of the American Society for Information Science and Technology, 58 (4), 479-93.

11. Chatterjee, S. (2019), "Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective", International Journal of Law and Management, Vol. 61 No. 1, 170-190. https://doi.org/10.1108/IJLMA-01-2018-0013

12. Christovich, M. (2016). Why should we care what Fitbit shares: a proposed statutory solution to protect sensitive personal fitness information. Hastings Commun./Entertain. Law J. 38, 91–116

13. Citron, D., Solove, D., (2018). D. Risk and Anxiety: A Theory of Data Breach Harms. 96 Texas Law Review 737. Available at: https://scholarship.law.bu.edu/faculty_scholarship/616

14. Drexl, J. and others, (2016) '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'. Max Planck Institute for Innovation & Competition Research Paper No 16-10 https://ssrn.com/abstract=2833165 accessed 16 November 2017.

15. Dwyer, C. (2011) "Privacy in the Age of Google and Facebook,". in IEEE Technology and Society Magazine. vol. 30, no. 3, 58-63, Fall 2011, doi: 10.1109/MTS.2011.942309.

16. Essam, M., Andrei Vlad S., Sandro H., Maged Z., Sarven C., Abdurrahman G., Ashraf A., and Berners-Lee, T., (2016). A Demonstration of the Solid Platform for Social Web Applications. In Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion). International World Wide Web

Conferences Steering Committee, Republic and Canton of Geneva, CHE, 223–226. DOI:https://doi.org/10.1145/2872518.2890529

17. Janeček, Václav, Ownership of Personal Data in the Internet of Things (December 1, 2017). Computer Law & Security Review, 2018, 34(5), 1039-1052, Available at SSRN: https://ssrn.com/abstract=3111047 or http://dx.doi.org/10.2139/ssrn.3111047

18. Jennifer, R. (1998). "What Is Information?," Information Services & Use. 18 (4), 243-54.

19. Kamara, I., De Hert, P. (August 8, 2018). Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. Brussels Privacy Hub, Vol. 4, No. 12, August 2018, Available at SSRN: https://ssrn.com/abstract=3228369 or http://dx.doi.org/10.2139/ssrn.3228369

20. Kamleitner B., Mitchell VW. (2018) Can Consumers Experience Ownership for Their Personal Data?From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints. In: Peck J., Shu S. (eds) Psychological Ownership and Consumer Behavior. Springer, Cham. https://doi.org/10.1007/978-3-319-77158-8_6

21. Kanngiesser, P., Itakura, S., and M. Hood, B. (2014). "The Effect of Labour on Ownership Decisions in Two Cultures: Developmental Evidence from Japan and the United Kingdom,". British Journal of Developmental Psychology, 32 (3), 320-29.

22. Kessler, J. (2019). Data protection in the wake of the gdpr: California's solution for protecting "the world's most valuable resource". Southern California Law Review, 93(1), 99-128.

23. Kosinski, M., Stillwell, D., Graepe, T. (2013). Private traits and attributes are predictable from digital records of human behavior. (Retrieved from the Proceedings of the National Academy of Sciences of the USA 〈 http://www.pnas.org/content/early/2013/03/06/1218772110〉

24. Kshetri, (2014). N. Big data′s impact on privacy, security and consumer welfare. Telecommunications Policy, Volume 38, Issue 11, 2014, 1134-1145, ISSN 0308-5961,https://doi.org/10.1016/j.telpol.2014.10.002. (https://www.sciencedirect.com/science/article/pii/S0308596114001542)

25. Kulk, S., van Loevan, B. (2012). Brave New Open Data World?, International Journal of Spatial Data Infrastructure Research, 2012, Vol 7, 196-206

26. Litman, J. (2000). Information Privacy/Information Property. Stanford Law Review, 52, 1283.

27. Manovich, L. (2011). Trending: The Promises and the Challenges of Big Social Data. In

M. K. Gold (Ed.), Debates in the Digital Humanities. Minneapolis, MN: The University of Minnesota Press. http://manovich.net/index.php/projects/trending-the-promises-and-the-challenges-of- big-social-data

28. Merges, P., Menell, P., Lemley, M., Jorde, T. (1997) Intellectual property in the new technological age. Aspen Law & Business, New Yor.k, 11–20

29. Moat, H., Preis, T., Olivola, C., Liu, C., & Chater, N. (2014). Using big data to predict collective behavior in the real world. Behavioral and Brain Sciences, 37(1), 92-93. doi:10.1017/S0140525X13001817

30. Nyoni, P., Velempini, M. (2018). Privacy and user awareness on Facebook. South African Journal of Science, 114(5-6), 15. https://dx.doi.org/10.17159/sajs.2018/20170103

31. Oostveen, M., & Irion, K. (2018). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? In M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, & G. Surblyt-Namaviien (Eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? (7-26). (MPI Studies on Intellectual Property and Competition Law; Vol. 28). Berlin: Springer. https://doi.org/10.1007/978-3- 662-57646-5_2

32. Pierce, J., Kostova, T and T. Dirks, K. (2003). "The State of Psychological Ownership: Integrating and Extending a Century of Research," Review of general Psychology, 7 (1), 84-107.

33. Pingo Z., & Narayan, B. (2016). When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy. In A. Morishima, A. Rauber, & C. L. Liew (Eds.), Digital Libraries: Knowledge, Information and Data in an Open Access Society—18th International Conference on Asia-Pacific Digital Libraries, Tsukuba, Japan (4). Japan: Springer International.

34. Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society., Information & Communications Technology Law, 17:3, 185-197, DOI: 10.1080/13600830802472990

35. Richterich, A. (2018). How data driven research fuelled the Cambridge analytica controversy. PArtecipazione e COnflitto * The Open Journal of Sociopolitical Studies http://siba-ese.unisalento.it/index.php/paco ISSN: 1972-7623 (print version) ISSN: 2035-6609 (electronic version) PACO, Issue 11(2) 2018: 528-543 DOI: 10.1285/i20356609v11i2p528, Published in July 15, 2018

36. Rodotà, S. (2009). Data Protection as a Fundamental Right. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_3

37. Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P., and Santos, Igor. (2019). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In Proceedings of the 2019 ACM Asia Conference on Computer and

Communications Security (Asia CCS '19). Association for Computing Machinery, New York, NY, USA, 340–351. DOI:https://doi.org/10.1145/3321705.3329806

38. Scholz, M. T. (2017). Big Data in Organizations and the Role of Human Resource Management, a Complex Systems Theory-Based Conceptualization. New York: Peter Lang.

39. Schwartz, P.M. (2004), Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055 (also available at: http://ssrn.com/abstract=721642)

40. Sen, R. & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach, Journal of Management Information Systems, 32:2, 314-341, DOI: 10.1080/07421222.2015.1063315

41. Solanki, M.R. (2021). SOLID: A Web System to Restore the Control of Users' Personal Data. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore. https://doi.org/10.1007/978-981-15-8289-9_24

42. Sousa e Silva, N. (2014), What Exactly is a Trade Secret Under the Proposed Directive?, 9 (11) Journal of Intellectual Property Law & Practice 923 (also available at: http://ssrn.com/abstract=2427002)

43. Stalla-Bourdillon, S., Knight, A. (2017). Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization, and Personal Data. Wisconsin International Law Journal, 34, 284-322. https://eprints.soton.ac.uk/400388/

44. Stamatoudi, I. (2002), To what extent are multimedia works films?, in: F. Dessemontet / R. Gani (Eds.), Creative ideas for intellectual property, The ATRIP Papers 2000 – 2001, CEDIDAC

45. Taştan, M & Gokozan, H. (2018). An Internet of Things Based Air Conditioning and Lighting Control System for Smart Home. American Scientific Research Journal for Engineering, Technology, and Sciences. 50. 181-189.

46. Torremans, P.L.C. (2015), The Road Towards the Harmonisation of Trade Secrets Law in the European Union, 20 Revista La Propiedad Inmaterial 27 (also available at: http://ssrn.com/abstract=2719015)

47. Trakman, L., Walters, R., Zeller, B. (2019). Is privacy and Personal Data set to become the new intellectual property, SpringerLink, https://link.springer.com/article/10.1007/s40319-019-00859-0

48. Turow, J., Hoofnagle, C. J., Mulligan, D. K., Good, N., & Grossklags, J. (2006). The FTC and Consumer Privacy in the Coming Decade. I/S: A Journal of Law and Policy for the Information Society, 3, 724, https://repository.upenn.edu/cgi/viewcontent.cgi?referer=https://www.Google.nl/&http sredir=1&article=1066&context=asc_papers

49. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In: Conference on Computer and Communications Security (CCS) (ACM, 2019) 973–990

50. Vranaki, A. (2016). Social Networking Site Regulation: Facebook, Online Behavioral Ad- vertising, Power and Data Protection Laws. Queen Mary School of Law Legal Studies Research Paper No. 221, 29. https://ssrn.com/abstract=2731159

51. Wall, D.S. (2018) How Big Data Feeds Big Crime, Current History: A journal of contemporary world affairs, 1 January, 29- 34.

52. Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting, Journal of Media Ethics,33:3, 133
148, DOI: 10.1080/23736992.2018.1477047

53. Werbrouck, J., Pauwels, P., Beetz, J., & van Berlo, L. (2019). Towards a decentralised common data environment using linked building data and the solid ecosystem. In B. Kumar, F. Rahimian, D. Greenwood, & T. Hartmann (Eds.), Advances in ICT in Design, Construction and Management in Architecture, Engineering, Construction and Operations (AECO) : Proceedings of the 36th CIB W78 2019 Conference (113–123). Newcastle, UK.

54. Whitaker, T. (2018). The ba data breach. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 2(10), 15-16.

EU and international legislation

1. Agreement On Trade-Related Aspects Of Intellectual Property Rights, The WIPO, (15th April, 1994).

2. Directive 96/9/EC Of The European Parliament And Of The Council

   of 11 March 1996 on the legal protection of databases

3. 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

4. European Data Protection Supervisor, 'EDPS Opinion on Personal Information Management Systems' (Opinion No 9/2016) , 20th October, 2016.https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf [https://perma.cc/X236-GR48].

5. 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)

6. Senate Judiciary Committee Report. (June 25, 2018). 2017-2018 Reg. Sess., Rep. On Internet Service Providers: Customer Privacy 1-2. available at https://digitalcommons.law.scu.edu/historical/ 1748 [https://perma.cc/8L4E-6GD3]

Other court decisions

1. ECJ, Fixtures Marketing Ltd v Oy Veikkaus Ab., C-46/02, ECLI:EU:C:2004:694, para. 44

2. Coogan v. News Group Newspapers Ltd [2012] EWCA Civ 48, [2012] 2 WLR 84, [2012] EMLR 14, [2012] 2 All ER 74.

3. Price v. Hal Roach Studios, Inc., 400 F. Supp. 836 (S.D.N.Y. 1975).

Other sources

1. About MyDex. (2021). Accessible at : https://mydex.org/about-us/about-mydex/, accessed on 10th February 2021

2. Aguzzi, S., and others, (2014). Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (European Commission 2014) 10, 26, 61. Globally, the number of connected devices is expected to grow from 9 billion in 2013 up to 50 billion by 2020: OECD, OECD Digital Economy Outlook 2017 (OECD Publishing 2017) 247; GAO, Technology assessment: Internet of Things: Status and implication of an increasingly connected world (GAO-17-75, May 2017) 1; McKinsey Global Institute, The Internet of Things: Mapping the Value Beyond the Hype (McKinsey 2015) 17.

3. Baker & Mckenzie (2013), Study on Trade Secret and Confidential Business Information in the Internal Market, study prepared for the European Commission, Publication Office of the European Union, available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final- study_en.pdf

4. Berghel, H. (2018). Malice Domestic, The Cambridge Analytica Dystopia, IEEE Computer Society.

5. Berners-Lee, T. (2019). Interview on the need to seek complete control of data. https://www.channelnewsasia.com/news/world/web-inventor-urges-users-to-seek--complete-control--of-data-11334546. Accessed 12 March 2019

6. Bernoff, J. (2018). What would it take for Tim Berners-Lee's new Web replacement to succeed?. Medium.com, can be accessed at https://medium.com/@jbernoff/what-would-it-take-for-tim-berners-lees-new-web-replacement-to-succeed-7b20544ec25, accessed on 4th April 2021

7. Bolychevsky, I. (2018). How solid is Tim's plan to redecentralize the web?.

Medium.com, can be accessed on https://medium.com/zero-equals-false/how-solid-is-tims-plan-to-redecentralize-the-web-b163ba78e835, accessed on 5th April 2021

8. Cadwalladr C., E. Graham-Harrison (2018, March 17), "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian. Re-trieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-Facebook-influence-us-election

9. Cellan-Jones, R. (2020). NHS data: Can web creator Tim Brenes-Lee fix it?. BBC News, can be accessed at https://www.bbc.com/news/technology-54871705, Accessed on 10th April 2021

10. Chesterman, S. (2017). Privacy and Our Digital Selves. The Straits Times. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3033449

11. Drum, K. (2013, November/December). Privacy is dead. Long live transparency! Retrieved from 〈http://www.motherjones.com/politics/2013/10/future-of-privacy-nsa-snowden〉

12. Have I Been Pwned. Website. https://haveibeenpwned.com. Accessed 15 March 2021

13. Hern, A. (2014). New York taxi details can be extracted from anonymised data, researchers say, The Guardian, https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn

14. Hern, A. (2019). Anonymized data can never be totally anonymous, says study, The Guardian, https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds?CMP=share_btn_fb

15. Ho, J.-J., Novick, S., Yeung, C. (2014). A snapshot of data sharing by select health and fitness apps. Federal Trade Commission, Washington (2014)

16. When can you rely on Legitimate Interests?. Information Commissioner's Office UK, retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/.

17. Kamleitner, B., Stephan, D., Haddadi, H. (2016). "Can Users Price Real-Time Contextual Information?," WU Vienna Working Paper.

18. King, L. (2014). Alarm over the 'gold rush' for citizens′ big data. Retrieved from 〈http://www.forbes.com/sites/leoking/2014/03/29/alarm-over-the-gold-rush-for-citizens-big-data/〉.Matuszewska K, What is PII, non-PII and personal data? Accessed at : https://piwik.pro/blog/what-is-pii-personal-

data/#what-is-personally-identifiable-information-(pii)?, accessed on 10th January 2021.

19. Legal protection of trade secret and know-how. (2007). Ius Mentis, Law and technology explained.
Accessed on 10th January 2021. Accessible at https://www.iusmentis.com/innovation/tradesecrets/

20. Microsoft Research, can be accessed at
https://www.microsoft.com/en-us/research/project/bali/, accessed on 12th April 2021

21. Mitrou, L. (2009). The Commodification of the Individual in the Internet Era: Informational Self-Determination or "Self-Alienation"? In M. Bottis (Ed.), Proceedings of the 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE 2009) (466-484). Greece: Nomiki Vivliothiki.

22. Musk, E. (2020). CEO Neuralink, The Joe Rogan Experience # 1470, Joe Rogan, Video Podcast, published on www.youtube.com, on May 7, 2020, https://www.youtube.com/watch?v=RcYjXbSJBN8&t=6378s

23. Pascual, A., Miller, S. (March 2015). Identity fraud report protecting vulnerable populations. Javelin Strategy and Research, http://securityaffairs.co/wordpress/34449/cyber- crime/javelin-study-2015-identity-fraud.html (accessed June 30, 2015).

24. Paul, H., Lee, R. (January 16,2019). Facebook Algorithms and personal data, Pew Research Centre, available at https://www.pewresearch.org/internet/2019/01/16/Facebook-algorithms-and-personal-data/, accessed on 28th April 2021.

25. Schechner, S., Secada, M. (2019). You Give Apps Sensitive Personal Information. Then They Tell Facebook, February 22, 2019, The Wall Street Journal https://www.wsj.com/articles/yougiveappssensitivepersonalinformationthentheytell-Facebook11550851636

26. Sharma, P., Moh, T. (2016). "Prediction of Indian election using sentiment analysis on Hindi Twitter,". 2016 IEEE International Conference on Big Data (Big Data). Washington, DC, USA, 2016, 1966-1971, doi: 10.1109/BigData.2016.7840818.

27. Telefónica, (2017). 'Telefónica presents AURA, a pioneering way in the industry to interact with customers based on cognitive intelligence' (press release, 26 February 2017) <https://www.telefonica.com/en/web/pressoffice/-/telefonica-presents-aura-a-pioneering-way-in-the-industry-to-interact-with-customers-based-oncognitive-intelligence> [https://perma.cc/F59Q-LV74]. In 2018, the platform will be launched also in Electronic copy available at: https://ssrn.com/abstract=3111047

28. Terms of Service, Facebook Inc,
Retrieved from https://www.Facebook.com/terms.php on 10th April 2021

29. The 2014 Cost of Data Breach Study: United States, Ponemon Institute, May 2014.

30. Tidy, J. (2020), Marriot Hotels fined £18.4m for data breach that hit millions, BBC News, Retrieved from https://www.bbc.com/news/technology-54748843, 9th April, 2021

31. Van Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E., Ascar, G. (2015). Security and Privacy in Online Social Networks. From social media service to advertising network: A critical analysis of Facebook's revised policies and terms [document on the Internet]. c2015 [cited 2016 Sep 14]. Available from: https://www.law.kuleuven.be/citip/en/news/facebook-1/facebooks-revised-policies-and-terms-v1-2.pdfSINTEF. (2013, May 22). Big Data, for better or worse: 90% of world's data generated over last two years. ScienceDaily. Retrieved April 7, 2021 from www.sciencedaily.com/releases/2013/05/130522085217.htm

32. Van den Hoven, J. Internet of Things Factsheet Ethics. (European Commission 2013).

33. Weise, K. (2019). Amazon Knows What You Buy. And It´s Building a Big Ad Business From it. The New York Times, Retrieved from https://www.nytimes.com/2019/01/20/technology/amazon-ads-advertising.html, 8th April, 2021

34. WIPO (2020). World Intellectual Property Indicators 2020. Geneva: World Intellectual Property Organization, ISSN: 2709-5207 (online). Retrieved from https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2020.pdf

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[148]

I Ratul Sen (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

IP Protection of Personal Data for Data Subjects within the Personal Data Storage Ecosystem,

(*title of the graduation thesis*)

supervised by : Kathrin Merike Nyman-Metcalf,

(*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

11.05.2021 (date)

[148] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*