Privacy Protection Amid Surveillance Capitalism: A Cross-Atlantic Comparative Legal Enquiry

Candidate: Bence Juhász

Comparative Constitutional Law,
Central European University.

In partial fulfilment of the requirements for the degree of Masters of Laws

Supervisor: dr. Marie-Pierre Granger

Budapest, Hungary and Vienna, Austria
2020-2021

Abstract

This thesis researches privacy laws related to the analysis of big data performed by global online service (GOS) corporations like Google and Facebook. First, I expose the business model of GOS corporations, 'surveillance capitalism' and discuss its potential to undermine the dignity of individuals and the integrity of the democratic process[1]. Next, I perform a comparative legal investigation between the USA and the EU to evaluate their regulatory frameworks amid surveillance capitalism. Additionally, I propose an initiative to enhance individuals' data protection. I conclude that the current US framework is unable to provide an effective protection of data and privacy, due to the lacking horizontal effect of the Fourth Amendment and its restricted protective scope due to the third party doctrine. The EU regime however, could effectively protect citizen's data amid surveillance capitalism by considering the requirements for free user consent in conjunction with tests following from consumer protection and competition law. Thus, I suggest that in the US a federal legislative bill should be institutionalized mimicking the GDPR, while the GDPR should be adjusted to accept the exploitation of User-Generated Content (UGC) data, as opposed to User-Generated Traces (UGT) data, according to the logic of the reasonable expectation of privacy test.

[1] Shoshana Zuboff (2019) *The Age of Surveillance Capitalism*, Public Affairs Books, New York.

TABLE OF CONTENTS

INTRODUCTION

While the technological revolution unfolding throughout the last decades granted people the capability of continuous access to information and communication, it also provided novel challenges for citizens and policy-makers to overcome. Citizens might face challenges in the form of addictive urges for online platforms[2], feelings of depression due to their excessive, agonistic use[3] and feelings of stress due to the relative scarcity of their attention compared to the constant overload of information online[4]. Simultaneously, a major regulatory challenge concerns the legal status attached to vast networks of data sets produced by the users of online services and collected or rather 'aggressively hunted' by surveillance capitalists[5]. Global Online Service (GOS) provider corporations such as Google, 'the pioneer of surveillance capitalism', are in the business of commodifying private human experiences[6]. Their surveillance tools, cookies or mobile cell towers gather and translate human experiences into standardized data sets. These are consequently fed into powerful artificial intelligence neural networks where machine learning capabilities generate predictions on the potential future needs, desires and activities of agents, driven by the aim of maximizing user attention paid to the online platform[7]. The knowledge derived from these predictions are then sold to firms seeking to advertise on these influential platforms, generating the vast majority of the GOS corporations' revenue[8]. Provided the extensive analysis of rich behavioural data,

[2] D'Arienzo, M.C., Boursier, V., Griffiths, M.D., (2019) 'Addiction to Social Media and Attachment Styles: A Systematic Literature Review'. *Int J Ment Health Addiction* 17, 1094–1118.
[3] Christina Sagioglou and Tobias Greitemeyer, (2014) 'Facebook's emotional consequences: Why Facebook causes a decrease in mood and why people still use it'. *Computers in Human Behavior*. 35. 359–363.
[4] Claudio Celis Bueno, (2016) 'The Attention Economy: Labour, Time and Power in Cognitive Capitalism', Rowman & Littlefield International.
[5] Shoshana Zuboff (2019) The Age of Surveillance Capitalism, Hachette Book Group. page 94.
[6] Ibid. Page 9.
[7] Claudio Celis Bueno Ibid., and Facebook on Predicting by Machine learning: https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads
[8] "In 2019, about 98.5 percent of Facebook's global revenue was generated from advertising, whereas only around two percent was generated by payments and other fees revenue." Facebook: advertising revenue worldwide 2009-2019 Published by J. Clement, Feb 28, 2020 https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

the content eventually shown to users has the potential of exploiting human psychological vulnerabilities, of nudging and manipulating citizens into feelings and actions the advertising customer and the surveillance capitalists see fit[9]. Given such potent capabilities to manipulate and exploit the users of online services and the crucial instrumental value that behavioural data possesses in this novel business model, the legal status attached to these big data sets and the regulatory framework that ought to control their collection, use and transfer lie in the focus of this thesis.

The underlying hypothesis of my thesis – the empirical testing of which falls outside the scope of the study - is that by limiting the data we feed into the neural networks of artificial intelligence, we can effectively mitigate and temper the manipulative capabilities of the social networks that we are so reliant upon. Consequentially, my assumption is that by taming the manipulative power of online services, we can meaningfully contribute to a greater protection of individual dignity and social cohesion amid surveillance capitalism. Therefore, the primary aim of this study is to contribute to a legal framework of data protection that secures cheap and wide access to information for people combined with respect for personal and collective autonomy, while also providing a reasonable revenue stream for innovative GOS corporations. Contributing to the development of such an 'ideal' regulatory framework is thus the primary aim of this thesis, motivated by the indirect, ultimate objective of protecting individual dignity and social cohesion in liberal democratic regimes.

"In the most recent fiscal period, advertising revenue through Google Sites made up 70.9 percent of the company's revenues." Google: annual advertising revenue 2001-2019 Published by J. Clement, Feb 5, 2020 https://www.statista.com/statistics/266249/advertising-revenue-of-google/

[9] This study revealed that a person's online context influences her emotions and actions. Thus, the authority or algorithm that determines the posts in one's feed, can influence the person's emotions and actions. Adam D. I. Kramer, Jamie E. Guillory, Jeffrey T. Hancock (2014) 'Emotional contagion through social networks' Proceedings of the National Academy of Sciences 111 (24) 8788-8790., and Bond, R., Fariss, C., Jones, J. *et al.* (2012) 'A 61-million-person experiment in social influence and political mobilization', Nature 489**,** 295–298. https://doi.org/10.1038/nature11421

Pursuant to these aims, firstly I establish the relevance, the methodology and the theoretical frame of the thesis. In section two I proceed by engaging with normative arguments from liberalism and Marxism converging upon a criticism calling for reforms amid surveillance capitalism. Then, I assess the (il)legitimacy of state intervention into the private contractual relationship between GOS corporations and their users. In section three, a comparison of the regulatory frameworks of two liberal democratic jurisdictions with significant market and normative powers follows. The framework of data protection in the USA and the EU will be scrutinized by means of a primarily doctrinal, internal[10] research focusing on authoritative texts such as the US Constitution, the European Convention on Human Rights (ECHR), the Charter of Fundamental Rights of the European Union (CFR), the EU's General Data Protection Regulation (2016/679) and the relevant case law from the apex courts of the jurisdictions.

I conclude, informed by the external moral arguments and the internal legal comparison, that the current US framework is unable to provide an effective protection of data and privacy, due to the lacking horizontal effect of the Fourth Amendment and its restricted protective scope due to the third party doctrine. The EU regime however, could effectively protect citizen's data amid surveillance capitalism by considering the requirements for free user consent in conjunction with tests following from consumer protection and competition law. Finally, I remark that a federal privacy bill shall be institutionalized in the US mimicking the GDPR. Moreover, a slight reform to the GDPR framework should be pursued, by accepting the exploitation of User-Generated Content (UGC) data, as opposed to User-Generated Traces (UGT) data, based on consent that is required for the use of the GOS. This way citizens would continue with unprecedented communication capabilities without monetary

[10] McCrudden, (2006) 'Legal Research and the Social Sciences', 122 Law Quarterly Review pp. 632-650.

fees and they could effectively decide what information they give up for exploitation, while the manipulative capabilities of GOS providers would be tempered and GOS providers would still secure stable revenues.

I. GROUNDWORK

The aim of the first section is to establish and legitimize the methodological and theoretical approach of the thesis. Additionally, it aims to create a common understanding of key concepts that repeatedly appear throughout the following sections. Therefore, after elaborating upon the relevance of the overall project, I discuss and define the methods and theories underpinning the thesis.

I.I RELEVANCE OF THE PROJECT

There are several factors that justify, or indeed necessitate that legal scholars, social and behavioural scientists, analysts of the global political economy, statisticians and ethicists engage in a multidisciplinary project to examine the nature of surveillance capitalism. On the one hand, behavioural data as the raw material of surveillance capitalism produced some of the most valuable corporations of the 21st century[11]. It is a major component of the globalized corporate competition, while some even refer to data as the oil of the 21st century[12]. In turn, corporations who refuse to collect the 'surveillance dividend'[13], face significant comparative disadvantage vis-á-vis their peers. Therefore, data protection is highly relevant from the perspective of corporate competition, wealth generation and innovation. On the other hand, the collection and exploitation of behavioural data is relevant for those whose experiences are analysed, for those whose work and leisure activities are exploited by surveillance capitalists to maximise profits. Some might be concerned by a violation of their private experiences, as

[11] Out of the 10 largest corporations in the world by market capitalization a minimum of four are GOS corporations using the methods of surveillance capitalism. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

[12] The metaphor was allegedly coined by mathematician Clive Humby - https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

[13] 'Surveillance dividend' refers to the marginal advertising profits a corporation can reap as a result of exploiting behavioural data. Shoshana Zuboff (2020) 'You are now remotely controlled', NY Times, https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

they are apparently accessible raw material for profit-seeking activities. Meanwhile, others might be concerned by the loss of their autonomy, as the knowledge GOS corporations derive from analysing massive behavioural data enables them to manipulate the future feelings and actions of their users[14].

Additional to this personal perspective is the aggregate, social aspect of individual privacy and autonomy. Liberal democratic regimes are based on the assumption that individual citizens comprising the sovereign power and supplying authority to its constitution[15] are self-reflective, autonomous and morally responsible agents of society who are in themselves capable of judging the ends they wish to pursue and capable of collectively and indirectly leading society[16]. Under surveillance capitalism the validity of this assumption is severely threatened. As humans increasingly inform themselves from online sources, instead of their general situatedness in the matrix of timespace[17], nowadays increasingly the algorithms of GOS corporations determine their informational input. This is relevant from the perspective of liberal democracy for citizens formulate their conceptions of the good, their moral judgements and their political opinion on the basis of that information input[18]. Additionally, the insight of surveillance capitalism revealed that the very reactions of citizens to the received information is constantly fed into the neural networks of GOS algorithms to further improve their ability to maximize user engagement with their platform[19]. This exposes the operation of a massive attempt to exploit human psychological vulnerabilities and to addict citizens to GOS. Therefore, these corporations exercise an ever-increasing influence over

[14] Kramer et al., (2014)
[15] András Sajó, Renáta Uitz, (2017) 'The Constitution of Freedom, An introduction to legal constitutionalism', New York, OUP, 87.
[16] Jeremy Waldron, (1989) 'Autonomy and Perfectionism in Raz's Morality of Freedom', 62 S. CAL. L. REV. and Bence Juhász, (2019) 'Manipulation, Exploitation and Information', Texas A&M University, unpublished.
[17] Linda Martin Alcoff, (2007) 'Epistemologies of Ignorance, Three Types' In: Shannon Sullivan and Nancy Tuana (Eds.) *Epistemologies of Ignorance*, State University of New York Press.
[18] Bence Juhász (2019)
[19] Shoshana Zuboff (2019)

citizens' moral judgements, conception of the good and eventually, political opinion[20]. If the fundamental assumption of liberal democracy concerning the autonomy of citizens ceases to be valid, the logical hierarchy of these regimes are severely undermined. Afterall, as Jürgen Habermas put it: 'the institutions of constitutional freedom are only worth as much as a population makes of them'[21]. Are not then liberal democracies running the risk of handing over sovereign power to private corporations and undermining their own logical and moral basis? For these reasons, the protection of individual privacy, has immense implications for the proper functioning of liberal democratic regimes. Therefore, individual privacy should also be thought of as a public good under liberal constitutionalism[22].

As pointed out in the introduction, this study approaches this complex challenge from the perspective of regulating the raw material of behavioural modification (big data) that fuels surveillance capitalism[23]. The legitimacy of this approach rests on two assumptions: 1) by better regulating the extraction and exploitation of behavioural data, the manipulative capabilities of GOS would be tempered, 2) by tempering the manipulative capabilities of GOS corporations, individual dignity and social cohesion could be better protected than under the status quo. Thus, the importance of protecting values such as autonomy, self-ownership or freedom from exploitation and the logical stability of the liberal democratic state provide relevance to the project.

I.II. Methodological Approach

[20] Bence Juhász (2019)
[21] Jürgen Habermas (1992) 'Citizenship and National Identity: some reflections on the future of Europe' Praxis International, 12/1: 1-19. 1992:7 in Will Kymlicka's (2002) *'Contemporary Political Philosophy an Introduction'*, Oxford University Press, page 285.
[22] Shoshana Zuboff (2019)
[23] Ibid.

The methodology this enquiry applies is first and foremost multidisciplinary in its nature, since insights from economics, psychology, machine learning and moral philosophy inform the comparative legal enquiry. Afterall, 'law is not autonomous, standing outside of the social world, but is deeply embedded within society', [24] legal rules should thus be studied and formulated with an eye on a wide range of social phenomena studied by disciplines other than law itself. The core subject of the thesis involves a comparison of authoritative legal texts from the perspectives of constitutional and human rights law, specifically focusing on the doctrinal issue of data protection and searching for its potential legal reform. Unsurprisingly, this legal endeavour is motivated, supported and legitimized by an underlying normative aim, the preservation of individual dignity, autonomy, collective self-ownership and the integrity of the democratic process. These considerations necessitate the inclusion of a particular theory of justice, exposing the philosophical basis of the thesis rooted in ethics and natural law. With other words, one might refer to this primarily comparative legal enquiry, as a 'universalist' pursuit of moral principles that should formally compel societies, as being posited upon the citizenry by means of the law[25]. This thesis however, does not attempt to argue for a novel theory of justice, as a truly universal attempt would do. Rather, it limits itself to operating within the boundaries of liberal democratic constitutionalism - the adequacy of which I hereby assume explicitly - and employs the strategy of 'aversive precedents'[26]. Thus, the thesis aims to establish, by performing a comparative legal exercise, principles and practices that societies properly committed to liberal democracy should institutionalize amid the challenge of surveillance capitalism. While the universalist theoretical standpoint is applied, the enquiry is limited to liberal democratic regimes. This

[24] Lynn Mather, (2008) 'Law and Society', In: Gregory A. Cladeira, R. Daniel Kelemen, Keith E. Whittington (Eds.), *The Oxford Handbook of Law and Politics,* Oxford University Press., page 1.
[25] Vicki C. Jackson (2012)
[26] Ibid. Page 6.

limitation is legitimate and necessary, since the scope of this thesis does not allow for a meaningful discussion of theories of justice and simultaneously, without an explicit normative framework, the objectives of the 'ideal' theory would be arbitrary. By means of this limitation, the objectives that I aim to protect are supplied by the constitutional identities of the studied liberal democratic regimes. Only under this paradigm, the legal enquiry attempts to find principles and regulative practices that could secure individual dignity and the integrity of the democratic process as fundamental building blocks of the liberal democratic enterprise.

Narrowing the focus to the comparative legal exercise there are additional methodological issues to justify. As such, the decisive factors determining the selection of comparators include the substantive market power that the USA and the EU with their roughly 800 million citizens signify. Similarly, the significant normative power of these entities also motivated their inclusion. The US Constitution, as the oldest of its kind, is widely regarded as a prime example of liberal constitutionalism, while the regional human rights institutions effective in the EU and European historical traditions dating from the Athenian democracy also serve as international exemplars and trend setters. Moreover, since the EU has engaged in creating a substantive data protection framework including, notably the GDPR, and that many GOS corporations reside in the USA these jurisdictions in theory could practice substantive control over surveillance capitalists. Furthermore, the choice of these jurisdictions, both being of a federal type, is motivated by the global nature of the phenomena under scrutiny and the appearance of 'new spheres of normativity distinct from the nation state'[27]. Additionally, the focus on these two comparators was motivated by their shared historical traditions and liberal

[27] Robert Leckey (2017) 'Review of Comparative Law', *Social & Legal Studies*, pp. 3-24, (p. 16)

democratic constitutional identities which might facilitate a convergence between their regulatory practices amid the global challenge of surveillance capitalism.

Additional to the primary role that the legal perspective occupies in the thesis, insights from psychology, economics and machine learning are essential in maintaining that the core values of liberal democracy are under siege. Identifying and grasping the essence of the challenge posed by surveillance capitalism would not be possible without involving these disciplines. Novel explanatory theories of modern-day capitalism such as surveillance capitalism[28] and the attention economy[29] help to understand the new method of wealth generation and means of production. Key behavioural insights revealed by social psychologists[30] identified vulnerabilities of the human mind that are rather easily exploited by modern day capitalists operating GOS. Thus, exposing the unprecedented risk of manipulation humans have to live with today and helping policy-makers to understand how exploitation in the 21st century might be wide-spread. In addition, computer scientists engaged in AI and machine learning capabilities informed policy-makers on how neural networks function, identified their raw material and highlighted the crucial role that their objective has in the logic of GOS corporations[31]. Finally, building on the immense work of these scientists, engaging in a multidisciplinary discourse and connecting the relevant insights, legal and political theorists might propose reform initiatives to preserve the foundational values of liberal democratic societies. The aim of performing this thesis is precisely to contribute to the embryonic social discourse around overcoming the challenge posed by surveillance capitalism and to feed into policy and legal reform processes that could preserve liberal democratic values.

[28] Shoshana Zuboff (2019)
[29] Claudio Celis Bueno (2016)
[30] D'Arienzo et al., (2019) and Sagioglou, and Greitemeyer, (2014)
[31] Jürgen Schmidhuber, (2015) 'Deep learning in neural networks: An overview', *Neural Networks*, Volume 61, Pages 85-11 ISSN 0893-6080,

I.III. Theoretical Framework

To proceed meaningfully, establishing a common denominator of key concepts appearing in this thesis is necessary. First, the ultimate subject of this enquiry is information in the form of data and meta-data. Data refers to behavioural information generated by users and collected by corporations, while meta-data refers to information derived as a result of analysing data, data about data. Moreover, I attempt to introduce a distinction in terms of the data that lies in the core of this dissertation. The line of demarcation in this case should follow the intention of users and demarcate data which is intentionally shared by the user of a GOS, from data that is not intentionally shared, rather left behind as an online fingerprint or trace that any user's online behaviour generates automatically, 'by dint of the online service's operation'[32]. The intentionally shared data might be referred to as user-generated content (UGC) and the unintentionally shared data as user-generated traces (UGT)[33]. This distinction is relevant in questions of determining the validity of claims of privacy, since the intentional sharing of information with several people could undermine one's 'legitimate expectation of privacy', a test in legal reasoning established by the US Supreme Court and subsequently applied by the European Court of Human Rights too[34]. However, this might imply that the data generated unintentionally, that is compiled as a seemingly unavoidable consequence of the functioning of the services – UGT - should fall under privacy protection. The aim of performing this distinction is to work towards the 'ideal' theory that would be able to protect individual dignity, while providing reasonable revenues for GOS corporations.

[32] 'by dint of its operation' this phrase referring to cell site location information was a significant determinant of the US Supreme Court decision *Carpenter v. USA 585 US* (2018). I introduced this distinction in my previous paper: Bence Juhász (2019)
[33] Bence Juhász (2019)
[34] Katz v United States 389 US (1967) and Barbulescu v Romania 61496/08

Data protection amid surveillance capitalism is fundamentally a challenge that centres upon humanity's relationship to newly accessible qualities and quantities of information. The revolutionary changes of communication technologies unfolding during the previous decades, altered the way how individuals and societies relate to information. This transformation, which I referred to in another essay as the 'information revolution', shifted the human struggle from receiving information, to the struggle of distinguishing between 'harmful, manipulative and overwhelming versus valuable, trustworthy and necessary' qualities of information[35]. Induced by technological advancements, the 'information revolution' alleviated the human struggle of receiving information, as this resource is nowadays constantly and abundantly available to most of us, members of the online community. The difficulty is no longer to gain access to the continuous flow of global information, rather exercising one's capability to process overwhelming quantities of information and to judge their quality against one's particular objectives became the key challenge[36]. The constant overload of information that humans face under the condition of global online interconnectedness, highlights the limited human capability to processing information and assessing its reliability, value and utility.

The 'information revolution' is a relevant concept for this thesis, since it supplies a crucial premise to explanatory theories such as the 'Attention Economy' and 'Surveillance capitalism'. From the perspective of such theories, corporations compete to maximize the amount of human attention they might absorb[37]. The scarcity of human processing power or attention is thus a major limit upon GOS corporations' capability to sell advertisements. According to the law of supply and demand scarcity of a raw material drives up its price and creates value for those who are in possession of the precious resource. This explains why the

[35] Bence Juhász (2019) p3.
[36] Ibid.
[37] Claudio Celis Bueno, (2016)

competition for human attention is so fierce as to even involve constant surveillance and exploitation of private human behaviour.

According to Shoshana Zuboff, Google was the first corporation to realize how to effectively commodify the immense amount of behavioural data compiling in their servers as a side effect of their popular search engine and simultaneously, how to maximize the absorbed human attention by their platform[38]. This revolutionary method consists in gathering and 'aggressively hunting' UGC and UGT as behavioural data, standardizing and feeding it into powerful neural networks, tasked with figuring out how to best engage the user so as to maximize the attention absorbed[39]. The better the behavioural data analysis, the more user engagement. The more engagement, the more place for ads and the more revenue for surveillance capitalists. The objective of these neural networks is to maximize user engagement and by means of positive and negative feedback loops they develop personalized strategies for absorbing the attention of a given user. As shown by psychology studies, often what maximizes engagement is content that provokes either complete surprise, fear and outrage[40] or content that resonates well with the already existing opinion of the user[41]. Thus, the spreading of fake news and the proliferation of echo chambers online might also be linked to the logic of surveillance capitalism exploiting human psychological vulnerabilities to maximize profits. As the services provided by surveillance capitalists became essential to a

[38] Shoshana Zuboff (2019)
[39] Ibid. Page 94.
[40] S. Vosoughi, D. Roy, S. Aral. (2018). 'The spread of true and false news online', Science. Vol 359, Iss 6380.
[41] "Again, we find support for the hypothesis that platforms implementing news feed algorithms like Facebook may elicit the emergence of echo-chambers." Cinelli et al., (2020) 'Echo Chambers on Social Media: A comparative analysis' Cornell University https://arxiv.org/abs/2004.09603v1
While certain studies do establish this link between GOS algorithms and echo chambers, it is worth mentioning that humans in themselves are more prone to interact with opinions that align with their identity. See: Dan M. Kahan, (2017) 'Misconceptions, Misinformation, and the Logic of Identity-Protective Cognition', Cultural Cognition Project Working Paper Series No. 164, Yale Law School, Public Law Research Paper No. 605, Yale Law & Economics Research Paper No. 575.

meaningful and flourishing participation in society, it seems that people's novel capability to communicate and access information online on unprecedented scales, reciprocally translates into a capability on the side of GOS corporations to control and steer the information a particular person or a community receives. As experiments showcase, by means of their immense agenda setting power, GOS corporations can manipulate the emotions and actions of users which is not only concerning from the perspective of individual mental health, but also from the perspective of voter behaviour and the integrity of the democratic process [42].

On the other hand, approaching the challenge of surveillance capitalism from a legal perspective, a significant and relevant theoretical debate concerning the distinction between public and private law must be clarified. Afterall, there are constitutional provisions securing individual privacy, the Fourth Amendment to the US Constitution, Article 8 of the ECHR or Article 7 of the CFREU, which cover online communication. Nevertheless, these fundamental constitutional rights are a matter of public law, concerning the relationship between the state and a citizen. Meanwhile, the relationship under scrutiny in this thesis concerns private parties, corporations and citizens, which falls under the realm of private law. The private-public law debate essentially concerns whether fundamental and constitutional rights should have a horizontal direct effect in private disputes. That is to say, whether fundamental rights, originally conceived as limitations upon the exercise of state powers vis-á-vis individuals, should also influence the relationship between private parties and if so, to what an extent? There are generally two sides of this debate: some legal theorists would argue that fundamental rights are exogenous, while others would contend that fundamental

[42] Kramer et al., (2014) and Bond et al., (2012)

rights are endogenous to private law[43]. Those arguing that fundamental rights are exogenous recall the historical development of such rights, which have been conceived so as to temper the exercise of governmental powers over individuals and to limit intrusions by the state into a citizen's private life. Additionally, they claim that individuals do not have to pursue public interests, their autonomy in their decisions should prevail[44]. Thus, the application of fundamental rights should be limited to the domain of public law, while private parties should be free to engage in voluntary contractual relationships with each other without having to worry about fundamental rights. This position is allegedly represented by the USA, but a more detailed discussion will follow later.

In contrast, legal theorists arguing that fundamental rights are endogenous to private law emphasize the hierarchical normative structure of legal systems having the constitutional texts as the basis of jurisdictions, creating the state itself that posits other laws effecting the domain of private law for example. They claim that it is in the nature of fundamental rights that their normative value trumps that of other laws, they logically uphold the entire legal system, thus their provisions should also constrain parties of voluntary private contracts[45]. This has been the status awarded to fundamental rights under the German Basic Law, where the Federal Constitutional Court (FCC) in the classical *Lüth* decision provided that fundamental rights are objective principles of the legal order and thus have a radiating effect into horizontal disputes.[46] The EU has also undertaken to provide horizontal applicability to some of its fundamental rights provided in the CFR, such as the right to non-discrimination

[43] Mirjam de Mol (2011) 'The novel approach of the CJEU on the horizontal direct effect of the EU principle of non-discrimination: (unbridled) expansionism of EU law?', *Maastricht Journal of European and Comparative Law.* 18(1-2):109-135.
[44] Ibid.
[45] Ibid.
[46] Dieter Grimm, (2010) 'The Basic Law at 60 – Identity and Change', *German Law Journal*, vol. 11, no. 1, 33–46., p 43.

(Article 21) in the *Kücükdeveci* decision.[47] Moreover, through directly applicable regulations such as the GDPR, the EU has provided for their direct application in private disputes. The answer to this theoretical debate has immense consequences for the protection of data amid surveillance capitalism. Therefore, it will be one of the crucial perspectives during the comparative exercise of Section III.

[47] Eleni Frantziou, (2020) 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle', Cambridge Yearbook of European Legal Studies, vol. 22, 2020, pp. 208–232.,

II. THE NORMATIVE BASIS FOR PRIVACY REGULATION

This section exposes arguments why jurisdictions properly committed to the values of dignity and the integrity of the democratic process should develop regulatory frameworks that effectively protect citizen's privacy in the online sphere. Moreover, as most of the online services regularly used by citizens are provided by innovative private corporations, section II.I. attempts to establish the legitimacy of governmental intervention into the horizontal relationship between GOS corporations and their users.

II.I. TWO ARGUMENTS FOR DATA PROTECTION

Shortly, I discuss two normative arguments following from sharply different philosophical traditions, but converging on their conclusion as to the present case. These are two critiques of the status quo one based on liberal premises and the other one originating in the Marxist tradition, both requiring a regulatory intervention.

Under the school of liberal egalitarianism, it is generally assumed that a person is free, equal to other persons and is capable to be the author of her own life, to behave autonomously.[48] As Rawls put it, 'citizens recognize one another as having the moral power to have a conception of the good (…) capable of revising and changing this conception on reasonable and rational grounds'.[49] Based on those assumptions about the nature of a person, in liberal democratic regimes a huge responsibility is awarded to citizens, namely the collective leadership of the constituency through their constitutive power and through elected representatives in

[48] See Jeremy Waldron, (1989), furthermore, the classical works of Immanuel Kant, (1785) [1983]. 'Grounding for the Metaphysics of Morals', in I. Kant, *Ethical Philosophy*, James W. Ellington (trans.), Indianapolis, IA: Hackett Publishing Co. and of John Stuart Mill, (1859) [1975] 'On Liberty', David Spitz (ed.), New York: Norton.
Moreover: Bence Juhász, (2019)

[49] John Rawls, (1980) 'Kantian Constructivism in Moral Theory: The Dewey Lectures 1980', Journal of Philosophy 77. 515-572. In Will kymlicka (2002) *'Contemporary Political Philosophy, an Introduction'* Oxford, OUP. p215.

parliaments. Therefore, the political opinion of citizens matters hugely in such regimes. Now the question should be asked: what serves as a basis for that opinion? How is the opinion of the individual formed? In that regard, the crucial role of the media becomes apparent, as it is the institution that is supposed to supply the citizen with information about the state of the world, complementing her own sensory experience. Based upon such information about a particular state of the world X, a citizen intuitively and rationally develops a moral judgement concerning the adequacy of X. This judgement subsequently becomes a constituent part of her own conception of the good. Therefore, if one accepts that politics might be defined as the arena where competing conceptions of the good supply alternative solutions to collective action problems and social dilemmas, one sees that there is a straightforward relationship between the informational input of citizens – largely supplied by the media - and their political alignment, action or inaction. Thus, it is clear that the institution of the media – often referred to as the 4th branch of power – exerts a significant influence on citizens' political stance. Now, is the third liberal assumption regarding the nature of a person still valid in the era of surveillance capitalism?

While citizens' vulnerability towards the media has remained largely unchanged during the modern history of mankind, when technological changes increased the manipulative capabilities of mediums, the development of novel regulatory frameworks was necessary to secure the continued integrity of liberal democratic regimes. With the development of the community of continuous flow of information online and the employment of the logic of surveillance capitalism, the service providers of such a community – GOS corporations – possess of an unprecedented capability to manipulate and nudge citizens' conception of the good.[50] Today it is overwhelmingly human-made online service algorithms that determine

[50] Adam Kramer et al., (2014) and Bond, R., *et al.* (2012)

who receives what information and when. More accurately, the content a user is served with online is determined by artificial neural networks working toward the human created objective of maximizing user engagement. With the constant surveillance of people on private GOS platforms, citizen's very reactions are fed back into algorithms tasked with exploiting psychological vulnerabilities to maximise user engagement by every means possible, including by exposing the citizen to false, misleading or superfluous information. Therefore, those who create and control these algorithms substantiate an enormous amount of control and consequent responsibility over the users of GOS. Therefore, I maintain that the third liberal assumption is at best under a serious threat by the largely unregulated business model of GOS corporations. From a liberal perspective the unrestricted operation of GOS corporations, under their right to property, freedom of business and contractual freedom, threatens the personal and collective decision-making process. Thus, it should be regulated to preserve the state's core liberal characteristics in the form of personal self-ownership and the integrity of the democratic process.

On the other side of the same coin, one finds argumentative grounds for the regulation of GOS corporations in Marxist moral philosophy. The centrepiece of that school is the exploitation of the less powerful, by the more powerful, concretely in its historical context, the exploitation of the proletariat by the bourgeoisie. Exploitation is often defined as taking unfair advantage of someone, or 'using another person's vulnerability for one's own benefit'.[51] Here the emphasis is on unfair, since few would condemn a person for taking advantage of the inattention of the opponent in an otherwise structurally fair setting such as a football game.[52] What makes taking advantage unfair is the element of coercion or necessity

[51] Matt Zwolinski and Alan Wertheimer, 'Exploitation', *The Stanford Encyclopedia of Philosophy* (Summer 2017 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/sum2017/entries/exploitation/
[52] Ibid.

to submit oneself to a particular treatment. In the famous account of Marx, without ownership of the means of production, the workers' need to sustain themselves effectively forces them to sell their labour. If the wage they receive for labour is insufficient to secure a meaningful life, then their vulnerability is being exploited by the more powerful.[53]

The application of the Marxist account of exploitation to the subject of the present thesis is elegantly performed by Celis Bueno in his book 'The Attention Economy'. His point of departure is that as societies get richer in terms of the production and consumption of information, comparatively they get poorer in terms of human attention.[54] With the overabundance of information online, human attention becomes an 'intrinsically scarce and therefore valuable resource'.[55] Provided that advertising companies derive profit off capturing human attention and of performing surveillance on its allocation, there is a fierce competition to maximise user engagement including by means of employing constant surveillance. Similarly, Zuboff (2019) claims that GOS corporations regard human experience – data derived about the allocation of attention – as 'free raw material for hidden commercial practices of extraction, prediction and sales'.[56] 'At first such data was found', but as the pioneers of surveillance capitalism became conscious of the possibilities behind the resource, it was 'hunted aggressively' by means of mass surveillance.[57] Effectively, the act of paying attention became a new form of labour creating surplus value.[58] This simultaneously 'blurs the line between labour time and leisure time', while alienating the spectator from her own vision.[59] Therefore, GOS corporations generate profit from maximising the absorbed attention by their platforms. This they attempt to achieve by performing a constant and

[53] Ibid.
[54] Claudio Celis Bueno (2017) p1.
[55] Ibid. p3.
[56] Zuboff (2019) p1.
[57] Ibid. p94.
[58] Ibid.
[59] Ibid. p6.

indiscriminate surveillance of their users to gather exploitable behavioural data on the basis of which their content is enhanced to further improve the absorption of user attention.

The only premise missing from legitimately claiming that the structure of the attention economy amounts to exploitation of the user of a GOS corporation is the element of necessity or coercion. Fortunately, it has already been established before, that humans of the 21st century are effectively obliged to be a member of the online community of continuous flow of information. Not only is the membership essential in the job-market, considering the effects of covid-19, it also became a prerequisite of attending classes and receiving an education. Thus, it is not far-fetched to claim that under the status quo, GOS corporations are exploiting their users by performing a constant surveillance of their actions to effectively exploit their psychological vulnerabilities, create addiction to their sites and reap profits by the maximised user engagement.

All in all, it is rather alarming that the application of such diverse moral traditions as liberalism and Marxism jointly imply that the status quo necessitates reforms to protect and respect people's autonomy. Uniting the forces of these arguments, I intend to claim that undermining personal and collective autonomy by manipulation and exploitation amounts to using people as a mere means as opposed to ends in themselves. Of course, this conduct goes against the second formulation of the Kantian Categorical Imperative prescribing that one must treat humanity 'always at the same time as an end, never merely as a means'.[60] Now the violation of this deontological principle is important to highlight in this primarily legal enquiry, for this formulation of the Categorical Imperative has been highly influential in constructing a meaning for the term 'dignity', often referred to as a supreme, legitimating

[60] Immanuel Kant (1785) p429.

value of human rights protection.[61] This is the case under the German Basic Law for example, where Article 1 §1 provides that 'human dignity shall be inviolable' and §2 that 'The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.' Moreover, dignity is also an essential underlying value of the jurisprudence of the ECtHR.[62] Thus, it seems that if the argument for the violation of dignity remains intact, it might have severe consequences for the legality of the behaviour of GOS corporations.

II.II. THE (IL)LEGITIMACY OF STATE INTERVENTION

While some arguments have been presented exposing the troublesome nature of GOS corporations, it is yet to be determined whether a public intervention into the investigated private relationship would be legitimate. Given that the present thesis operates within the boundaries of liberal democracy, the legitimacy of state intervention must also be established within that paradigm. This might result to be a challenging task, since state neutrality is often praised as a foundational liberal principle.[63] This principle shall be understood as requiring the state to refrain from prioritizing any particular conception of the good over others, to respect and secure the autonomy of citizens. Afterall, from the perspective of liberal neutrality, 'no life goes better by being led from the outside according to values the person does not endorse'.[64] Therefore, the argument is made that the state should refrain from

[61] Matthias Mahlmann, (2012) 'Human Dignity and Autonomy in Modern Constitutional Orders', In *The Oxford Handbook of Comparative Constitutional Law* (Eds): Michel Rosenfeld, András Sajó, Oxford, OUP. 371-393. Mahlmann recalls that dignity appears in the Preamble and Art 1. to the Universal Declaration of Human Rights and the Preamble to the ECHR among many other examples.
[62] Christine Goodwin v. The United Kingdom, no. 28957/95, in § 90 the Court provides that: 'the very essence of the Convention is respect for human dignity and human freedom.'
[63] Will Kymlicka (2002) p217. referring to endorsements of liberal neutrality by Rawls, Ackerman and Dworkin.
[64] Ibid. p216.

paternalism and provide the individual with the capability to deliberate upon the ends she wishes to pursue and to experience the choices she makes.

Nevertheless, there is another strand of liberal thought that positions itself closer to communitarianism and objects first and foremost to the atomistic perspective employed by scholars endorsing state neutrality and their negligence regarding the social preconditions of the enjoyment of personal autonomy.[65] This latter position is defended and elaborated for example by Charles Taylor in his 'social thesis' arguing that individual autonomy might only be exercised in a particular community with an enabling environment, provided and sustained by a non-neutral government of the common good.[66] 'Some limits on individual self-determination are required to preserve the social conditions which enable self-determination'.[67] The degree of autonomy available for a particular individual is largely determined by the surrounding social environment. In order for the community as a whole to be free and for its members to enjoy the beauty of self-ownership, the state shall be under a positive obligation to actively protect the community's dominant way of life, in the present case the way of life led by the values of personal autonomy and dignity. The state's duty is to maximize the aggregate level of autonomy enjoyed by the members of the community and often this requires the limiting of some agents' autonomy. Indeed, even Rawls concedes in the formulation of his 'First Priority Rule' that liberty might be limited, however, only for the sake of liberty.[68]

This position is not alien to legal thinking, more so, the often and rightly praised proportionality analysis between competing fundamental rights is a prime example of the social thesis in practice. The state attempting to maximize overall enjoyment of liberty, often

[65] Ibid. p244.
[66] Ibid. 245.
[67] Ibid.
[68] Ibid. 56.

limits some citizens' ability to do so on the basis of a rule of law. Having mentioned the proportionality analysis, another method employed by Germany after the Second World War also underpins the legitimacy of a politics of the common good. This is the notion of the militant democracy, which is embodied in constitutional provisions such as the possible ban of associations and even political parties that are considered to be unconstitutional.[69]

Turning from the level of abstract principles to the concrete controversy at hand, there is certainly a natural reaction to the attempt of intervening into the private relationship between GOS corporations and users. Namely, that if the use of GOS poses such a threat to individual dignity and autonomy, people should just stop using them. Afterall, it is their decision to be online or not and governmental regulation should not restrict the private contractual relationship between GOS corporations and their users. While there is certainly some legitimacy to this remark, there is a tripartite counterargument that I defend below.

Firstly, I maintain that leaving citizens with a choice between giving up their capability for self-ownership or abandoning the tremendous benefits that GOS provide them would impose an undue burden on individuals. Composing this thesis in 2020/2021 perfectly showcases citizens' high level of dependency upon the various online services and thus, the undue burden that avoiding them would impose upon citizens. From library access to a 10 year old's math class, from communication with the state to participation in remote work opportunities, humans of the '20s are to rely upon online services to meaningfully participate in society. Specifically, as education migrated to online services due to covid-19, students who face difficulties in accessing online communication experience a decrease in their capabilities to participate in education, which increases the already existing achievement gaps due to social

[69] Gelijn Molier and Bastiaan Rijpkema, (2017) 'Germany's New Militant Democracy Regime: National Democratic Party II and the German Federal Constitutional Court's 'Potentiality' Criterion for Party Bans, Bundesverfassungsgericht, Judgment of 17 January 2017, 2 BvB 1/13, National Democratic Party II.', European Constitutional Law Review, vol. 14, no. 2, 394–409.

backgrounds[70]. If one accepts the premise that access to education is constitutive of human flourishing, then one should also accept the conclusion that - at least with C-19[71] - membership in the online community became a prerequisite of achieving social flourishing[72]. Provided that both self-ownership and access to GOS are integral to human flourishing, the supposedly free decision between these values imposes an undue burden on individuals. This choice should not be forced upon citizens. Therefore, governmental regulation of data protection remains legitimate.

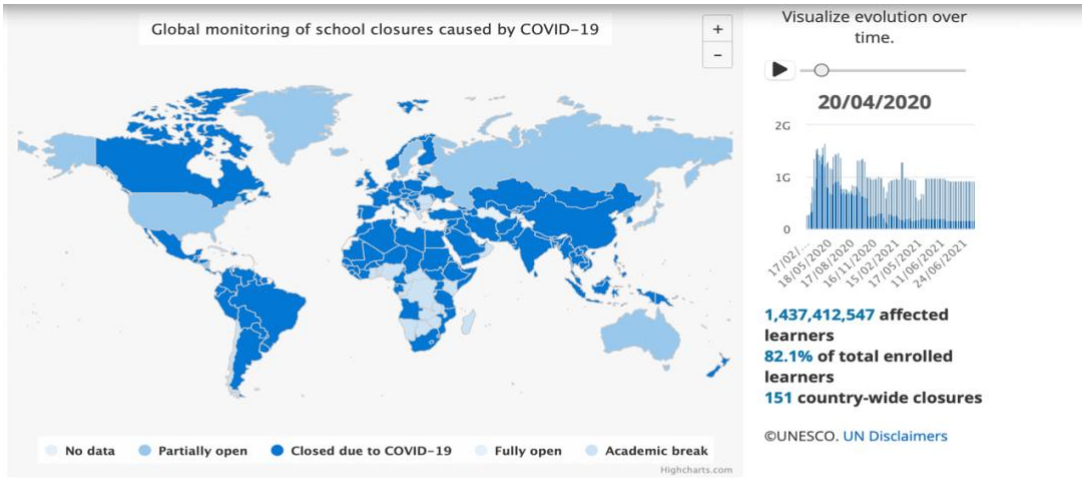

Figure 1.[73]

Another argument for the legitimacy of governmental intrusion into the private contractual relationship between GOS corporations and their users rests on the social relevance of

[70] Emma Dorn et al., (2020) 'New evidence shows that the shutdowns caused by COVID-19 could exacerbate existing achievement gaps', McKinsey, accessed from: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/covid-19-and-student-learning-in-the-united-states-the-hurt-could-last-a-lifetime#

[71] While the influence of C-19 on education, work and leisure is most probably temporary, it is not evident how long this would last. Thus, it is legitimate to argue on the basis of current circumstances.

[72] Bence Juhász (2019) and US Supreme Court case Carpenter v. USA 585 US (2018) The Court asserted that "carrying one (a mobile device) is indispensable to participation in modern society." Although strictly speaking mobile devices and GOS differ, if carrying a mobile device "is indispensable to participation in modern society", one should ask: whether this logic – especially with the disruption of C-19 - should or could be extended to cover GOS?

[73] Number of children forced to participate in online education. Source: Unesco, Global Monitoring of School Closures, accessed from: https://en.unesco.org/covid19/educationresponse

individual privacy in liberal democratic regimes. This has been duly considered above in Section II.I as part of the liberal critique of the status quo. Since the business model of GOS threatens the foundational values of liberal democratic regimes – autonomy, dignity and the integrity of the democratic process – recalling Taylor's social thesis it is not only legitimate, but should be a duty of a state properly committed to the above values to develop a regulatory framework that effectively protects its citizens and itself from the threat of surveillance capitalism. The preservation of the liberal democratic constitutional identity legitimizes intervention.

The third line of defence of state intervention targets the validity of the contractual relationship between the corporations and individuals. In developing this account the normative foundations of consumer and competition law become relevant, particularly the notion of exploiting a dominant position and operating under an information and power asymmetry[74]. The freedom of economic competition is at the heart of a liberal market economy. Economic actors should be free to practice their autonomy within the provided limits of the law, however the aim those limits ought to promote remains contested. Some argue that the overall welfare created by a regulatory framework - the sum of consumer and producer surplus - should be maximized by regulation.[75] Nevertheless, others maintain, notably Adam Smith, that a market regulation should make 'consumer preferences the ultimate controlling force in the process of production' a principle also known as consumer sovereignty.[76] The reason for claiming this is that ultimately in a constitutional democracy the citizens constitute the sovereign power whose interests should be promoted by the law. While

[74] Renato Nazzini (2011) 'The Objective of Article 102', In: Renato Nazzini, *The Foundations of European Union Competition Law: The Objective and Principles of Article 102*, Oxford Studies in European Law, OUP Oxford, 2011, ISBN 0191630128, 9780191630125 pp 109-110-
[75] Viktor Vanberg, (2011) 'Consumer welfare, total welfare and economic freedom: on the normative foundations of competition policy'. Competition Policy and the Economic Approach: Foundations and Limitations, Freiburg Discussion Papers on Constitutional Economics, 09/3, p15.
[76] Ibid. p15.

the producers that might benefit by 'escaping the burden of competition' will inevitably only represent a segment of producers and will conflict with others, a market regulation that favours consumer sovereignty will benefit all consumers indiscriminately, thus assuring a general compensation for any particular cost they have as a producer.[77] A similar conclusion is implied by assessing the specific objectives behind EU competition law. In that regard, referring to Articles 101 and 102 TFEU, Botta and Wiedemann asserts that by sanctioning the anticompetitive behaviour of undertakings, indirectly EU competition law 'safeguards the aggregate welfare of consumers.'[78] Furthermore, crucially for the present thesis, they also assert that the application of these provisions is horizontal, they apply directly to private undertakings.[79] All in all, this limited account of the normative basis of consumer and competition law implies that consumer interest should be prioritized by maintaining a healthy competition in the market.

Finally, one additional line of argument could be developed concerning the public importance of the functions that certain GOS corporations perform.[80] For example, operating the most wide-reaching contemporary political agora and the consequent regulation of sensitive issues such as freedom of speech or the reliability of news. While there is no space to duly expand this counterargument here, I believe the case is made that for the protection of the liberal democratic constitutional identity and its constitutive foundational values, governmental intervention into the investigated relationships is legitimate. This position implies that concerning the specific doctrinal issue at hand, the protection of privacy, I intend to maintain

[77] Ibid. p16-17.
[78] Marco Botta and Klaus Wiedemann (2019) 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey', *The Antitrust Bulletin*, vol. 64, no. 3, pp. 428–446, doi:10.1177/0003603X19863590. P434.
[79] Ibid.
[80] See for example: Oreste Pollicino (2021) ' Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions', ECHR, accessed from: https://echr.coe.int/Documents/Intervention_20210415_Pollicino_Rule_of_Law_ENG.pdf

that its constitutional protection should have a horizontal effect on the private contractual agreements between GOS providers and their users.

III. CROSS-ATLANTIC COMPARISON: DOES REGULATION KEEP THE PACE OF TECHNOLOGY?

In this section I intend to investigate in a comparative fashion the legal protection of privacy and data in the jurisdictions of the USA and the EU. After comparing the structural architecture of the jurisdictions, I perform a textual and contextual analysis of the main authoritative texts: the Fourth Amendment to the US Constitution including notable case law developments and in the EU context Article 8 ECHR, Article 7 and 8 CFR. Since the EU has engaged in further elaborating the relevant fundamental rights in secondary legislation, I also assess the adequacy of the E-Privacy Directive[81] (ePD) and the General Data Protection Regulation[82] (GDPR). Finally, I conclude the comparative exercise by assessing how effectively could the different jurisdictions protect individual's privacy amid surveillance capitalism and expose a reform initiative.

III.I. STRUCTURAL DIFFERENCES BETWEEN THE JURISDICTIONS

First, a few preliminary remarks regarding the structure of the jurisdictions shall be discussed. Provided their liberal democratic constitutional identity, both praise individual privacy, autonomy and dignity as important values of their constitutional order.[83] It must be taken into account that while the USA is a fully established federal state with a comparatively stable balance of powers regarding the federal and the state levels based upon the oldest valid Constitution of our time, the EU is a more dynamic union with a less stable power balance

[81] E-privacy Directive 2002/58/EC
[82] General Data Protection Regulation 2016/679
[83] As for the US, the separation of powers model in the Constitution aims to secure individual autonomy and liberty, but for more specific references see: The Fourth Amendment – right to privacy, and The First Amendment – protection of religious freedom, freedom of speech, and freedom of assembly all constitutive parts of human autonomy and thus dignity. For the definition of dignity referred to here see note 65. As for the EU see for example: TEU Article 2, The preamble and Articles 1, 3, 7, 10, of the EU Charter of Fundamental Rights and similarly Articles 5, 8, 9, 10, of the ECHR.

between the state and the federal levels. Indeed, the mere use of the term 'federal' when referring to the EU is a politically contested one. There is a lot of tension surrounding the debate upon the nature of the EU as an international or a supranational entity. Still, the US and the EU 'share similar federal political institutions' and in fact both could be categorized from a comparative federalism perspective as 'compound polities' portraying both horizontal and vertical separation of powers. [84] Furthermore, as the supremacy of EU law is an established jurisprudential doctrine[85] and the CJEU is the apex court of the EU whose decisions have binding force upon member states, the treatment of the EU as a quasi-federal state for the sake of the comparative analysis is legitimate. The CJEU's jurisdiction is invoked when an EU institution or a member state is directly involved in a legal controversy, when a domestic court requests a preliminary ruling from the CJEU in accordance with Article 267 TFEU or when an EU citizen petitions the Court directly.

Similarly, the apex court of the USA, the Supreme Court has original jurisdiction to conduct a trial when the federal government or a state is a party to a controversy and has appellate jurisdiction when a controversy involves an aspect of federal or constitutional law.[86] Moreover, it exercises the power of judicial review, ensuring that each branch of the government adheres to the limits of its power according to the Constitution.[87] Importantly, the Supreme Court might exercise its powers 'both as to Law and Fact' thus, it might reinvestigate the facts of a controversy and reinterpret the applicable laws too.[88] This point brings us to the third apex court that this investigation included into its scope, the European

[84] Fernando Mendez and Mario Mendez (2009) 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States', *The Journal of Federalism*, vol. 40 (4), pp. 617-645. page 620-621.
[85] Costa v. Enel Case 6/64
[86] Constitution of the United States of America Article III. Section II.
[87] This power is not granted in the Constitution itself, but was established by the Supreme Court in Marbury v. Madison 5 US 137 (1803)
[88] Ibid.

Court of Human Rights (ECtHR) which contrary to the Supreme Court has less powers when it comes to the facts of a case. The ECtHR is an institution of the Council of Europe (CoE), thus it is not an EU institution, but it is responsible to hear cases arising under the ECHR with its currently 47 contracting parties, including all member states of the EU, but not the EU itself. The CoE is an intergovernmental institution, hence the principle of conferral and subsidiarity play a significant role in the Court's jurisdiction. While its decisions are binding upon the contracting parties, their late execution often raises concerns.[89] The Court might hear cases brought by contracting parties against one another, but also brought by a citizen of a contracting party against a state, provided that all domestic remedies have been exhausted.[90] The inclusion of the ECtHR into the present investigation is legitimate since as of 2021, all 27 EU member states are signatories to the ECHR and the EU itself is legally obliged to become a contracting party according to Article 6(2) TEU. Moreover, there is also a considerable amount of interaction between the ECHR and EU law. The provisions of the ECHR and its case law development inspire the general principles of EU law as recognized by the CJEU[91] and the ECHR has also been a source of inspiration when drafting the EU CFR.

III.II. The Basis of Privacy Protection – A Textual and Contextual Analysis

Below, I perform a textual and contextual analysis of constitutional provisions relevant from the doctrinal perspective of privacy and data protection. I also account for the historical contexts concerning the framing of these documents and relevant case law developments.

[89] Elisabeth Lambert Abdelgawad (2008) 'The execution of judgments of the European Court of Human Rights', CoE Publishing, P.64
[90] ECHR Article 35 (1).
[91] Gráinne De Búrca (2011) 'The road not taken: the European Union as a global human rights actors', The Americal Journal of International Law, Vol. 105, No. 4, pp. 649-693 p668.

Moreover, I assess the adequacy of the GDPR and the ePD which are crucial EU secondary legislations concerning online privacy.

First, I turn towards the US Constitution out of respect for its 232 years of existence. The particular structure of the Constitution with its seven main Articles and the following Amendments is a result of the tense political debates between the federalist and the anti-federalists.[92] Known as the Massachusetts Compromise, a sufficient number of states of the Confederation agreed to ratify the new Constitution provided that certain amendments will be proposed rather soon in order to prevent the freshly established executive power from usurping too much power and threatening individual rights.[93] Thus, in the context of protecting the rights of individuals against encroachments of the federal government, 10 Amendments were codified into the Constitution. One of such is the Fourth Amendment:

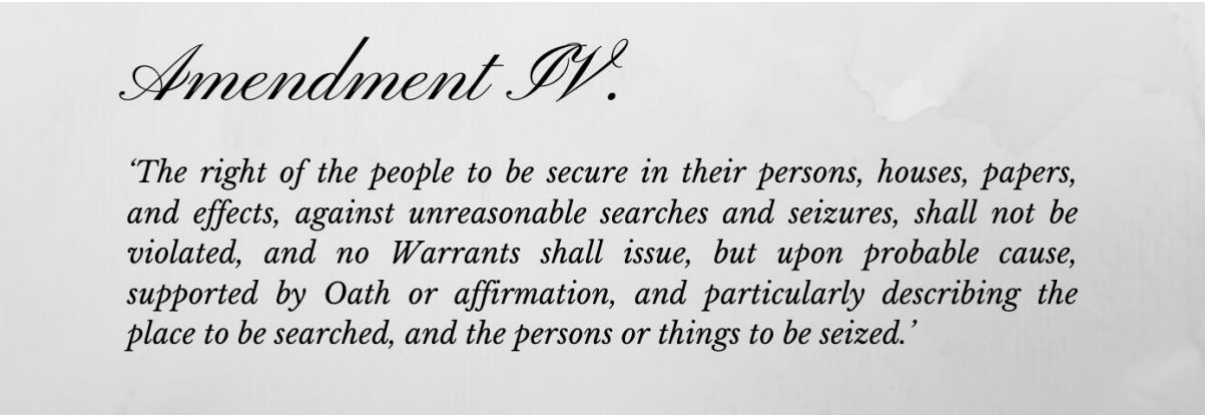

Figure 2.[94]

Without any doubt this Amendment primarily aims to protect US citizens' privacy and security from arbitrary interferences by the government.[95] One crucial characteristic of the

[92] Mark Tushnet (2015) *The Constitution of the United States of America A Contextual Analysis,* 1. An Overview of the History of the US Constitution, Hart Publishing, pp 10-14.
[93] Ibid.
[94] The Fourth Amendment to the US Constitution, own illustration.
[95] Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967)

Fourth Amendment is that it does not confer an absolute right upon citizens, but similarly to its European counterparts[96], only a limited one. The phrase *'The right of the people to be secure (...) against unreasonable searches and seizures*' implies a balancing exercise between the competing interest of the government and the individual as an inherent part of determining which interferences meet the reasonability criteria. The reasonable expectation of privacy test was fleshed out in *Katz v. United States*.[97] The test has two levels, first it must be evaluated whether the individual concerned had a subjective expectation of privacy and second, whether society would be prepared to recognize that subjective expectation as a reasonable one.[98] Interestingly, this test has migrated to the other side of the Atlantic as well, where the ECtHR has integrated it into its own jurisprudence, but there are references to the reasonable expectation of privacy even in the GDPR.[99]

In comparison, Article 8 of the ECHR protects citizens' 'private and family life, home and correspondence' against interferences primarily from public authorities, but indirectly also from private ones. The ECHR came into existence as a fruit of a specific historical development following the Second World War as a reaction to the horrors of the Nazi regime. Hence, similarly to the US Constitution, it primarily aims to temper state power. Thus, the fundamental rights provided therein primarily entail negative obligations on states not to engage in certain activities that would violate such rights. Nevertheless, contrary to the US, to undertake positive obligations by contracting parties was a clear intention among the framers of the Convention. This effort is most notably present in article 1 of the ECHR, where it is provided that High Contracting Parties must not only respect, but shall also secure the rights

[96] See: Article 8 §2 ECHR and the case Privacy International v. Secretary of state C-623/17. In this case the CJEU ruled that despite national security might be a compelling reason for surveillance, the general and indisciminate retention of data is disproportional.
[97] Katz v. United States 389 U.S. 347
[98] Smith v. Maryland, 442 U.S. 735
[99] See note 38 for ECHR and Recital §47 referring to GDPR Article 6 (1)

enlisted in the Convention.[100] Thus, providing the textual basis for positive state duties regarding citizens' enjoyment of convention rights.

Similarly to the US, the rights entailed in Article 8 ECHR are not absolute, they are limited in various ways. As § 2 provides, legitimacy to an interference with one's right to privacy might be supplied if the interference is authorized by law and is necessary in a democratic society to provide for the various legitimate aims enlisted therein such as national security or the protection of the rights of others. Thus, like in the USA, the interest of the individual in the form of the enjoyment of her right must be balanced against the state interest of providing the enlisted public goods. Contrary to the US however, positive state obligations arise under the Convention originating from the state's duty to protect citizens under its jurisdiction.[101] For the state to violate its positive duties, the conduct of private parties allegedly contrary to the Convention must arise from the contracting party's failure to act or toleration.[102] In line with the principles of conferral and subsidiarity, in controversies involving positive duties, the Court grants a certain margin of appreciation to the states.[103] Nevertheless, under certain circumstances, especially where vulnerable parties are concerned, contracting states are under the positive obligation to develop regulatory frameworks that provide practical and effective[104] protection to citizens from foreseeable infringements of their rights resulting from the actions of private parties.[105]

[100] For positive state obligations concerning Article 8 ECHR see for example *Barbulescu* (discussed later). Barbulescu v Romania App no. 61496/08 (ECtHR, 5 September 2017)
[101] Jean-François Akandji-Kombe (2007) 'Positive obligations under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights', CoE, Human rights handbooks, No. 7. p14.
[102] Ibid.
[103] Jean-François Akandji-Kombe (2007) 'Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights', Human rights handbooks, No. 7., Council of Europe.
[104] The practical and effective doctrine is present e. g. in X and Y v. Netherlands, no. 8978/80, 26 March 1985 and Airey v. Ireland, No. 6289/73, 11 September 1979.
[105] Barbulescu v Romania App no. 61496/08 (ECtHR, 5 September 2017) §115 and *X and Y v. the Netherlands*, (Application no. 8978/80) §§ 23, 24 and 27

For example, in *Barbulescu*, a case involving corporate surveillance at the workplace, the Court provides a checklist of several items to assess the developed legislative frame's adherence to the Convention.[106] The Court aims to secure that state discretion is not unlimited and the legislative frame ensures that restrictions of privacy are 'accompanied by adequate and sufficient safeguards against abuse'.[107] The Court requires that notification of the possible surveillance must be clear and given in advance, while the scope of the surveillance and the degree of intrusion should be minimized. It is relevant whether the actual content is accessed, the length of the surveillance and the people that gained access to the information. It must be considered whether the aims could have been reached by a less intrusive method, whether the information was actually used for the declared purpose and the consequences of the surveillance upon the citizen must be accounted for.[108] Importantly from the perspective of privacy protection amid surveillance capitalism, article 8 protects individuals' right to conduct a private social life or to develop a private social identity.[109] Moreover, the Court has also recognized that information derived from monitoring a person's internet use also falls under the protective scope of article 8.[110] While the legitimate expectation of privacy tests is also applied by the ECtHR, the Court recalls that - at least in the workplace – an employer's instructions cannot reduce private social life to zero', even if the employee consents to such terms.[111] The logic of these standards could perhaps be extended to the relationship between GOS providers and their consumers thus setting limits to what a data subject can consent for.

Turning to the US, the European focus on the universality of fundamental rights[112] constitutes a major textual difference compared to the US Constitution. Nevertheless, in the USA human

[106] Barbulescu §§ 121-123
[107] Barbulescu § 120 – referring to Zakharov §§ 232-234
[108] Barbulescu § 121 (iv-v)
[109] Barbulescu §70
[110] Berbulescu §72
[111] Berbulescu §80
[112] See CFR Article 1, and Article 1 ECHR all implying an objective value order.

rights also have their foundations in natural law, implying a universalistic conception of rights and an objective value order.[113] This is exemplified by the famous lines of the Declaration of Independence: *'We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights.'* Therefore, while from a textual perspective[114] and from one perspective of the contextual analysis the Constitution implies a clear intention to only create negative obligations for the state, another contextual perspective undoubtedly implies that the theoretical foundation of human rights in the US lies in natural law, implying and objective value order. From this theoretical perspective, it would not be overambitious to maintain that constitutional rights such as the one provided in the Fourth Amendment should have a radiating effect into private disputes.

Crucial for the present enquiry is whether and when the Fourth Amendment could cover online communications and if so, what kinds of data? Concerning online data flows the case law is divided as it is not straightforward whether a person has a legitimate expectation of privacy when using an online service and thus sharing information with a third-party service provider. Cases concerning access to one's location information through GPS tracking were deemed to raise justified privacy expectations.[115] However, the Supreme Court found no justified expectation of privacy with regards to financial records being accessed through the network of a bank[116] or dialled phone numbers beings accessed by means of installing a pen register device to a telephone line.[117]

[113] Charles S. Desmond (1953) 'Natural Law and the American Constitution', Fordham Law Review, Volume 22 Issue 3 Article 1.
[114] See the Fourtheenth Amendment's 'state action doctrine'
[115] United States v. Jones, 565 U.S. 400
[116] United States v. Miller, 425 U.S. 435
[117] Smith v. Maryland, 442 U.S. 735

Interestingly, if one consents to a warrantless search or does not object to one, it becomes legitimate in the eyes of the law,[118] a logic that lies at the heart of EU privacy protection.[119] What are the safeguards surrounding consent in the US? The Supreme Court decided that the burden of proof rests with the prosecution as for the voluntariness of the consent and the awareness of the right of choice.[120] While these are important safeguards, from the perspective of surveillance capitalism, would sharing data with a service provider with the intention of using a service qualify as consenting to a warrantless search? It would be perhaps counterintuitive to think so, but the matter is certainly a complicated one under the Fourth Amendment. In order to understand why, one must get acquainted with the 'third party doctrine'. This principle was developed in *Smith v. Maryland* where it has been asserted that information that is voluntarily turned over to a third party can no longer fall under one's legitimate expectation of privacy.[121] This logic could have substantive implications for the present investigation as it implies that data stored by private telecommunication companies could not fall under an individual's sphere of privacy.

In this regard, the case *Carpenter v. United States* will offer some more appealing conclusions. Here the surveillance of cell site location information (CSLI) by government agents was at the centrepiece of the controversy. CSLI is a 'detailed, encyclopedic, and effortlessly compiled' data set, that is generated when a phone routinely connects to a nearby radio antenna.[122] The FBI accessed almost 13.000 data points illustrating the movement of a robbery suspect without a warrant and tried to use the information as evidence at the trials. Carpenter petitioned the Supreme Court to supress the data and eventually won. In its

[118] Amos v. United States, 255 U.S. 313 (1921)
[119] In the EU under the GDPR, not objecting to surveillance, such as cookies does not constitute legal grounds for the search. The consent has to be an affirmative act from the user.
[120] Bumper v. North Carolina, 391 U.S. 543 (1968) and Johnson v. United States, 333 U.S. 10, 13 (1948).
[121] Smith v. Maryland 442 U.S. 735
[122] Carpenter v. U.S., 138 S.Ct. 2206 (2018)

reasoning the Court recalled that sharing such information with a service provider implies the application of the third party doctrine following *Smith*. Nevertheless, the Court asserted that individuals have a *'reasonable expectation of privacy in the whole of their physical movements'*, and access to CSLI would enable the government to 'near perfectly retrace a person's whereabouts'.[123] Moreover, an individual does not truly voluntarily expose her CSLI, rather the *'cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up'*.[124] Finally, having regard to the fact that *'cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society'*,[125] the Court refuses to apply the doctrine here. Rather, the Court recognized Carpenter's legitimate expectation of privacy and in similar cases requires a warrant upon probable cause to access the information.[126] With *Carpenter,* I attempt to illustrate that the Supreme Court in its Fourth Amendment jurisprudence has the ability and the tools to recognize citizens' extensive vulnerability and to protect their privacy in the 21st century's digital reality. However, applying *Carpenter's* logic in a contractual, horizontal dispute would be at best contentious due to the lacking horizontal applicability of the Fourth Amendment and the third party doctrine's negative implications on one's legitimate expectation of privacy related to data held by private corporations.

As for the EU community law, the fundamental rights relevant to the present analysis are provided for in Article 7 and 8 of the CFR and Article 16 of TFEU. Concerning the context of these provisions, it should be noted that according to Article 1 CFR: '*Human dignity is*

[123] Carpenter (1).
[124] Carpenter (2).
[125] Carpenter (2).
[126] The Court referred to its conclusion as a 'narrow' one: 'does not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security.'

inviolable. It must be respected and protected.' This formulation, similarly to the ECHR and the German Basic law[127], seems to endorse an objective value order and a universal theory of fundamental rights, a key textual difference compared to the US Constitution. Regarding the material scope of constitutional privacy protection, the EU provisions are largely similar compared to the ECHR and US texts. Article 7 and 8 CFR provide that *'Everyone has the right to respect for his or her private and family life, home and communications.*' and that *'Everyone has the right to the protection of personal data concerning him or her.'* The only explicit difference between the three textual bases is that the protection of personal data is explicitly covered under EU law. This is most probably due to the fact that the EU instruments are substantively younger than its comparators. However, this textual difference need not result in a substantively wider protection since both Article 8 ECHR and the Fourth Amendment apply to online communication data.[128] Another difference between the frameworks from the textual perspective is found in Article 8 §2 CFR: *'data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.'* The element of consent is central in the protection of privacy under EU law. To investigate how this principle is further specified, I turn to the analysis of EU secondary legislation, towards the GDPR and the ePD.

Before focusing on the crucial element of consent, I provide a limited overview of the landmark GDPR. It aims to protect the rights of natural people regarding the processing of their personal data and by establishing a uniform framework it aims to facilitate the flow of data within the EU.[129] Similarly to the limitations found in ECHR Article 8 §2, the GDPR

[127] The preamble to the ECHR provides: 'this Declaration aims at securing the universal and effective recognition and observance of the Rights therein declared', while the German BL Article 1 §1: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.' For an application of the objective value order See: FCC Lüth Decision, 1958, BVerfGE 7, 198.
[128] See: Barbulescu v. Romania 61496/08) and Carpenter v. US 138 S.Ct. 2206 (2018)
[129] GDPR Article 1 (1-3)

does not apply to processing of competent authorities connected to security and foreign policy and the prevention or detection of crime.[130] Crucial from the comparative perspective, the GDPR has an extraterritorial effect. It applies to the activities of establishments of controllers and processors in the EU, regardless of whether the actual processing takes place within the EU.[131] Furthermore, it also applies where the controller or processor is not established in the EU, but it offers goods for or monitors the behaviour of data subjects in the EU.[132] Thus, whenever American GOS providers interact with data subjects in the EU, they must comply with the GDPR, or face administrative fines up to 4% of their total global turnover.[133] When defining its protective scope, Article 4(1) provides that the term 'personal data' which the GDPR protects, refers to data about an 'identifiable natural person', who is identifiable by reference to her name, ID number, 'location data, online identifier, the physical, physiological, genetic, mental, economic, cultural or social identity'.[134] In this regard it is important to highlight that according to recital §26, pseudonymised data - data turned into codes – should still fall under 'personal data', since with the keycode the data subject is identifiable. Furthermore, recital §30 asserts that natural persons are in theory identifiable by IP addresses, cookie identifiers and other device-generated identifiers which should thus also be covered by the GDPR. While alternative interpretations of the GDPR's protective scope raise concerns from our normative perspective, I continue the overview with articles 5 and 6 and revisit this issue later. The general principles assert that processing should be lawful, fair and transparent.[135] Data should be 'collected for specified, explicit and legitimate purposes', it shall be limited to what is necessary for the provided purpose and

[130] GDPR Article 2 (2) b-d
[131] GDPR Article 3 (1)
[132] GDPR Article 3 (2)
[133] GDPR Article 83(5)
[134] GDPR Article 4 (1)
[135] GDPR Article 5.

confidentiality should be ensured.[136] In order for the processing to be lawful, it shall either be necessary for the performance of a contract with the data subject or necessary for a legitimate interest pursued by a controller.[137] In determining what a legitimate interest could be, according to recital §47, the reasonable expectation of privacy of data subjects shall be taken into account. Lastly, consent provided by data subjects also serves as a legal basis for processing.[138]

Now, I shift the investigation's focus to the legitimacy of consent, since in relation to many GOS providers the use of services is conditional upon consenting to contracts or privacy policies, while consenting legalizes the exploitation of data.[139] As discussed above, there are good reasons to maintain that GOS function as effective preconditions for realizing one's potential for social flourishing.[140] Thus, the requirements for the qualification of consents as free and unconstrained are perhaps the most important factors in EU data protection. Consent should be a freely given, specific, informed and unambiguous indication from the data subject.[141] Controllers shall request consent in a 'clearly distinguishable', 'intelligible and easily accessible form', 'using clear and plain language'.[142] While, the right to withdraw consent is provided for, given the utmost importance of many GOS and their conditionality on consent, this right is effectively void. In 7(4) the lawgiver asserts that in assessing whether a consent is freely given it shall be considered whether the requested service is 'conditional on consent to personal data processing that is not necessary for the performance of that contract'. This provision echoes the moral arguments elaborated above, however, it is

[136] Ibid.
[137] GDPR Article 6 (1)
[138] Ibid.
[139] See Figure 1 below concerning Facebook. The same is applicable when attempting to create a Google account.
[140] For example GOS's role in education and work are prime examples.
[141] GDPR Article 4(11)
[142] GDPR Article 7(2)

difficult to interpret the exact meaning of 'not necessary for the performance of that contract'. Afterall, one might argue that whatever purpose is included in the contract and hence consented by the data subject, such as automatic profiling for marketing purposes using cookies, is thus necessary for the performance of that very contract. Nevertheless, an opposing argument could be developed from the fact that one uses Facebook or Google for specific communicative purposes and additional services such as personalised marketing are not necessary for the primary function of GOS (as reasonably expected by users).[143] As such, making the use of services conditional on such profiling cookies for marketing purposes would render the consent constrained. If the first interpretation is applied, the provision fails to be effective in data protection amid surveillance capitalism, while in the second case it does provide an effective safeguard.

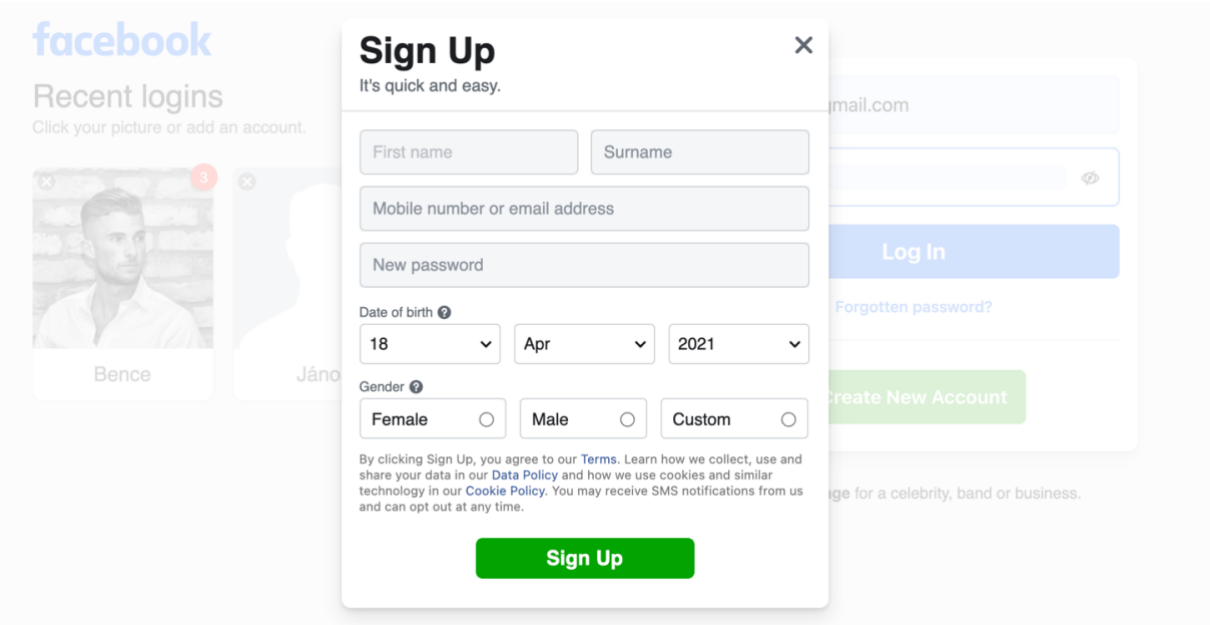

Figure 3.[144]

[143] This is a reasonable expectation from data subjects as GOS corporation advertise their service not with reference to its marketing capabiloities, rather its communicative ones.

[144] Attempting to Register for Facebook in 2021. 'Sign up It's quick and easy' while the contract you must agree to is well-hidden. A typical example of the many levels of nudging exerted by GOS corporations. One is required to accept the Terms, the Data Policy and the Cookie Policy which together comprise of 10786 words. Or of course avoid Facebook. Thus, 10786 words that one must agree to. No negotiation. Say on average, one

Further sophistication is provided by the recitals: 'Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.'[145] Additionally, if there is a 'clear imbalance between the data subject and the controller', the consent should not provide a lawful basis for processing.[146] Similarly, if 'the provision of a service, is dependent on the consent despite such consent not being necessary for such performance', then the consent is presumed not to be freely given.[147] While one should treat these recitals with due limitations given their interpretative nature, they clearly support the second interpretation of GDPR Article 7(4). Finally, to consider a counterargument from the perspective of the GOS providers, some might argue that automated profiling for marketing is necessary for the provision of the contract, since it generates the capital inflow that provides for the primary function without monetary fees. Nevertheless, 'necessity' implies that something cannot be otherwise. Is it necessary that the primary communicative function of GOS must be financed by automatic profiling for marketing? I must decline a positive answer and remark that at least one possibility comes to mind, namely a subscription based system. Thus, I maintain that the second interpretation of Article 7(4)GDPR should be applied in judging the legitimacy of consents and therefore, I argue that the qualification of consent under the GDPR could provide a meaningful privacy protection amid surveillance capitalism.

The utmost importance of the requirements for free consent is also underlined by Article 9 GDPR, which actually prohibits the processing of 'special categories of data' revealing

needs a second to process the meaning of two words. (I derived this rate from reading to myself a sentence of 55 words which took 22,16 seconds.) Thus, by dividing 10786 by 2 we get 5393, or the amount of seconds one would need to read the above contract. Dividing this number by 60 we find that roughly a person would need 89,88 minutes to read these terms, 1,5 hours. Of course my estimated second/word processing rate might be inaccurate, but this calculation does not include any required stops to reflect upon and interpret whole sentences or paragraphs.

[145] Recital to the GDPR §42

[146] Racital to the GDPR §43

[147] Ibid.

among others ‘ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership’, person's sex life or sexual orientation. The reason why this provision underlines the previous discussion is that the prohibition of the exploitation of such special data is inapplicable, if the data subject consented to such practices.[148] This reveals that lawmakers are entirely aware of the threats posed by the exploitation of sensitive data, however, they trust the decision-making capabilities of data subjects and avoid paternalistic prohibition. From the liberal philosophical standpoint this is not a manifestly mistaken agenda. However, recalling GOS providers extensive manipulative capabilities, the utmost importance of their services and their conditionality upon consent, the legitimacy of relying on user consent even regarding such sensitive data is severely undermined as there exists no substantive choice.

While there are further provisions of the GDPR that are worth analysing, for practical reasons of space and for the overriding nature of consent,[149] I omit them from the analysis. Rather, I revisit the salient issue regarding the GDPR’s protective scope. The regulation protects data relating to identifiable people, which according to the recitals covers pseudonymised data, IP addresses, cookie identifiers and so on. To continue this enquiry I invite the reader to reconsider the earlier distinction made between User-Generated Content (UGC) and User-Generated Traces (UGT). The main difference between the two kinds of data is that UGC is intentionally and ‘manifestly made public by the data subject’, while UGT are data that are generated automatically, ‘out of dint of its (the GOS’s) operation’, without any affirmative act from the user besides using the service.[150] Users do not voluntarily expose their online

[148] GDPR Article 9(2)a
[149] See for example GDPR Article 22(2)c. While the right not to be subjected to automated decision-making seems like a very useful one for the present analysis, user consent makes it inapplicable.
[149]
[150] GDPR Article 9(2)e and Carpenter (2) see below at note 161.

traces, rather GOS providers position this feature as a necessity for the provision of the service. However, as argued by Zuboff, this algorithmic architecture follows from a conscious choice for GOS providers aiming to maximise engagement and profits, not from a technological necessity.[151] Usually, problematic data processing practices such as automated profiling use both kinds of data, however while one's reasonable expectation of privacy concerning UGC is basically non-existent, as UGC is shared publicly and intentionally. In the case of UGT one's expectation of privacy is intact, for that data is not manifestly shared, rather it is 'hunted aggressively' by means of surveillance techniques such as cookies, without the understanding of many users consenting to privacy policies out of need or fatigue.[152] The only basis for the exploitation of UGT data is the consent of the data subject fabricated by the pressure of having to use the service and its conditionality on consenting to purposes such as profiling for marketing which is not necessary for the primary aim of the service. However, crucially for the GDPR's scope, UGT data are not completely anonymous rather, as far as my technical knowledge goes, they are pseudonymised datasets, since their exploitation for profiling logically presupposes that the knowledge derived from them could be reapplied to the very person analysed. Nevertheless, to decide this issue with high certainty requires a level of technological expertise I do not claim to have. Therefore, in case the CJEU would find otherwise and UGT data or part of it would not be covered by the scope of the GDPR, one can still turn towards the ePD due to its supposedly wider scope.

The ePD provides that 'Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly

[151] Shoshana Zuboff (2019) Ch. 3.
[152] Zuboff page 94. and Botta and Wiedemann p432 referring to German Monopolies Commission (2015) 'Competition Policy: The Challenge of Digital Markets',74, Special Report No.68, www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf.

available electronic communications services, through national legislation.'[153] In this provision 'communication' refers to 'information exchange between a finite number of parties by means of a publicly available electronic communications service',[154] and 'traffic data' to data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[155] Thus, its scope seems to allow for the protection of data that might not be strictly speaking related to identifiable people. Furthermore, reinforcing the abovementioned second interpretation of GDPR Article4(2), the Directive provides that any processing of information that is non-essential for the provision of the service, but is used for some 'value added service' such as marketing, should be contingent on the informed consent of the user. The ePD defines value added services as any service that 'requires the processing of information beyond what is necessary for the transmission of a communication or the billing thereof'.[156] Thus, the ePD reinforces the distinction between what processing is necessary and what might be referred to as processing for value added services.

Nevertheless, there seems to be one problem with the ePD in the protection of privacy amid surveillance capitalism: directives fail to have direct horizontal application. Fortunately, the CJEU precedents of the *Kücükdeveci*[157] *and Mangold*[158] cases imply otherwise. In the context of anti-discrimination based on age the court asserted that a directive giving specific expression to a fundamental right can have a direct effect in horizontal disputes.[159] As Muir put it, 'it is difficult to see why the 'Kücükdeveci effect' would not apply to data protection

[153] ePD Article 5(1)
[154] ePD Article 2(d)
[155] Ibid. (b)
[156] ePD Article 2 §g
[157] Seda Kücükdeveci v. Swedex GmbH & Co. KG Case C-555/07
[158] Werner Mangold v. Rüdiger Helm Case C-144/04
[159] Elise Muir (2014) The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges', *Common Market Law Review,* 51: 219–246.

legislation giving specific expression to the corresponding fundamental right.'[160] Indeed, Article 1 ePD asserts that it attempts to harmonize the approaches of member states for the protection of privacy. Moreover, recital §2 provides that the ePD 'seeks to ensure full respect' for Article 7 and 8 of the CFR. Thus, in agreement with Muir, I maintain that the ePD should be interpreted as specifying the scope of such fundamental rights and thus applying directly to horizontal disputes.

IV. Conclusion: Towards an ideal regulatory framework of privacy protection

To evaluate the compared jurisdictional frameworks' capability of providing an effective privacy protection amid surveillance capitalism two crucial questions should be answered: 1) Does privacy protection have a horizontal effect or is there a positive duty for the government to protect citizens' privacy in private contractual relationships? 2) Does the material scope of privacy protection cover the kinds of data exploited by private corporations? Based on the above analysis, I briefly evaluate the legal frameworks and then I conclude the project with an initiative for reform.

As for horizontality, in the USA the theoretical foundation of fundamental rights in natural law is perhaps the only grounds upon which a radiating effect could be argued for. Nevertheless, as far as I can judge, the intention of the framers of the Amendments and the textual basis arguments pointing to the opposite direction outweigh the natural law argument. The 'state action doctrine' established that individual rights provisions, except the Thirteenth Amendment, 'bind only governmental actors and not private individuals'.[161] The doctrine is

[160] Ibid. p232.
[161] Stephen Gardbaum (2003) 'The "Horizontal Effect" of Constitutional Rights', *Michigan Law Review*, Volume 102, Issue 3, UCLA School of Law.

derived from the language of the Fourteenth Amendment: 'No state shall (…) deprive any person of life, liberty, or property, without due process of law.' Nevertheless, Gardbaum argues that the state action doctrine does not rule out indirect influences of the Constitution to horizontal disputes, exemplified by the cases *NYTimes v. Sullivan*[162] and *Shalley v. Kramer*[163]. Gardbaum continues that all US law including private law is 'directly and fully subject to the Constitution' and individual rights provisions have a substantive indirect effect on the lawful behaviour of individuals. [164] Thus, Gardbaum concludes that from a comparative perspective, this indirect effect places the US closer to the horizontal than the vertical end of the spectrum.[165] While this argument does allow for a more positive view of US as for the first question, it is also clear that by no means could the Fourth Amendment be used as grounds for litigation in a horizontal dispute against a GOS provider.

Moreover, as far as the protective scope is concerned, the third party doctrine 'allows for very far reaching access to private data that is much more restricted in other legal systems'.[166] The US Supreme Court seemed reluctant to extend the otherwise progressive logic of *Carpenter*[167] to cover the relationship between GOS providers and their users, although *de facto* there are various similarities between CSLI data and UGT data. They are both generated automatically, without an affirmative act of the user and as far as my argument goes, access to Facebook or Google is similarly to a mobile phone 'indispensable for participation in modern society'.[168] Therefore, I conclude that the third party doctrine would probably in most cases render user's expectation of privacy unreasonable, while the Fourth

[162] 376 U.S. 254 (1964).
[163] 334 U.S. 1 (1948).
[164] Gardbaum (2003) p.390
[165] Ibid.
[166] Matthias Mahlmann (2017) 'Normative Universalism and Constitutional Pluralism', In: Iulia et al., (eds): *Liber amicorum András Sajó: Internationalisation of Constitutional Law*,
[167] Carpenter (2)d
[168] Carpenter (2)

Amendment would not be applicable to a dispute between a data subject and a private GOS corporation. Thus, the current US system fails to provide effective protection amid surveillance capitalism.

As for the EU, it seems that despite the ECHR's explicit requirement of positive obligations, the margin of appreciation resulting from the intergovernmental nature of the court and the emphasis on the principles of conferral and subsidiarity, would preclude a meaningful, short-term protection of privacy amid surveillance capitalism. While the standards of the court resemble that of EU community law, leaving the construction of the precise legislative frameworks to domestic legislatures would not provide a short term solution to the pressing issue of surveillance capitalism. Nevertheless, my limited analysis found that EU citizens could rely on the GDPR for a meaningful protection against GOS providers and thus, the GDPR could function as an effective gatekeeper of democracy and protector of individual dignity.

The reasons for this position include the qualification of free consent provided for in Article 7(4). According to its adequate interpretation, GOS providers' requirement of consent to unnecessary data processing, from the perspective of the primary purpose of the service, provides grounds for regarding that consent constrained. Hence, such consents should fail to be legal bases for data processing. Additionally, as I argued in section II. there seems to be clear information and power asymmetries between the actors which further reinforce the constrained nature of consents.[169] Concerning the EU framework I conclude that if the CJEU pays due attention to the crucial importance of GOS for realizing one's potential for social flourishing, if the CJEU recognizes that consent for processing of value added services is often required for the use of GOS, that both refusing to use the services and consenting to the exploitation of one's most intimate and sensitive data impose an undue burden on individuals

[169] See the tests elaborated in recitals §§42-43

and that GOS corporations exploit their dominant position resulting from the previous premises, then, the Court should enforce the legal bases of the GDPR by not accepting forced consents to privacy policies such as the one exemplified by Figure 3. above.

Reflecting about the 'ideal' data protection framework for an international community properly committed to the protection of individual dignity and the integrity of the democratic process, while also aiming to provide a reasonable capital inflow for innovative GOS providers. I argue that the GDPR's framework with the focus on qualified user consent should be institutionalized as an effective international practice in relation to the investigated jurisdictions. However, the GDPR should be updated with the reform initiative expressed below to approach the tripartite aim of the 'ideal' framework and to facilitate its acceptance in the USA. Thus, the Brussels effect[170] and the EU's normative power could receive a crucial reinforcement in times of fierce competition for digital supremacy and an otherwise stumbling EU.[171]

From a practical feasibility perspective, given the GDPR's extraterritorial effect most GOS providers already have to comply with its framework, thus its migration to the US as a new federal privacy bill would not cause a huge disruption in the market, assuming that domestic SMEs would have to implement proportional safeguards to their size. Also, provided the meddling with the 2016 elections facilitated by GOS, the necessary political momentum is also not inconceivable for a comprehensive privacy bill. While, the lobbing capability of GOS corporations against the legislation could present an insurmountable obstacle,[172] it is also possible that the fragmented legislative landscape of the states is not as efficient for corporations as one might think.[173]

[170] Anu Bradford (2012) 'The Brussels Effect', *Northwestern University Law Review*, Vol. 107, p. 1, 2012; Columbia Law & Economics Working Paper No. 533.
[171] Here I merely refer to Brexit and the internal crisis of fundamental values and illiberalisation.
[172] Mendez and Mendez (2009) p625.
[173] Ibid. p626.

More importantly, from the perspective of data protection amid surveillance capitalism, the qualifications of consent under the GDPR supplied by the thresholds of Article7(4), the 'genuine choice without detriment'[174] and the 'clear imbalance between actors'[175], should function as effective protections of citizen's privacy. Effectively, the qualified consent approach (if adequately implemented taking into account the discussions in Section II.) leaves citizens with the freedom to decide for themselves what data are they willing to share for exploitation, while it secures GOS corporations capability to reap profits from providing personalized marketing for users who truly freely consent to it. Moreover, this approach marries data protection law to competition and consumer protection law, since it applies the logic of Article 102 TFEU under the rules of competition, prohibiting abusing a dominant position by imposing unfair trading conditions.[176] Similarly, the USA has a long history of antitrust laws[177] and a powerful Federal Trade Commission protecting both competition and consumers.[178] Therefore, achieving data and privacy protection through sanctioning unfair and deceptive trading practices, like the one illustrated in Figure3., by jointly enforcing data protection, competition and consumer protection laws should be the strategy adopted in both jurisdictions.

However, an objection to this framework might arise from the perspective of the third aim of the 'ideal' approach. Assuming that merely a fraction of users would agree to personalized marketing, provided a substantive choice, GOS corporations would lose substantive revenue. While it is conceivable that many people would still prefer receiving personalized marketing recommendations on their social media, I see some legitimacy to this remark. Hence, finally I

[174] Recital in §42
[175] Recital in §43
[176] Botta and Wiedemann (2019) p429.
[177] See the 1890 Sherman Act
[178] Mendez and Mendez (2009) p625. and FTC (2009) 'A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority', retrieved from: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

argue that in line with the reasonable expectation of privacy test and the distinction introduced between UGC and UGT, GOS corporations should be allowed to use UGC data for profiling and other value added purposes, based on a consent required for the use of the service. Afterall, data subjects share such information intentionally making it publicly available and they have an effective control over what they share as UGC. However, GOS providers should not be able to exploit one's online traces only contingent on user consent that one can decline without detriment and that meets the strengthened consent qualifications of the GDPR interpreted through the lenses of competition and consumer protection law. This implies a slight reform of the GDPR since relating to Article 7(4) the processing of UGC data would be acceptable as necessary for the provision of the service. This framework is I think the one - from the alternatives that I could conceive of - that maximises overall expected utility for our societies. Data exploitation and manipulative capabilities would be substantively lower as a considerably lower number of users would allow the exploitation of online traces. Citizens would continue with unprecedented communication capabilities without monetary fees and they could effectively decide what information they allow for exploitation, coinciding with the information they intentionally share online. Meanwhile, GOS providers would still secure stable revenues. Moreover, if the GDPR incorporates the reasonable expectation of privacy logic with the UGC-UGT distinction, the US could more easily internalize this framework as a federal privacy bill. With this conclusion I hope the paper could somewhat contribute to an ideal data protection framework for the international liberal democratic community. As for further research, the demarcation line between UGC and UGT should be further detailed, taking into account the notion of communal privacy or a community's reasonable expectation of privacy and its implications for decreasing the scope of UGC.

BIBLIOGRAPHY:

Adam D. I. Kramer, Jamie E. Guillory, Jeffrey T. Hancock (2014) 'Emotional contagion through social networks', *Proceedings of the National Academy of Sciences*, 111(24)

Airey v. Ireland, No. 6289/73,

Amos v. United States, 255 U.S. 313

András Sajó, Renáta Uitz, (2017) *'The Constitution of Freedom, An introduction to legal constitutionalism'*, New York, OUP, 87.

Anu Bradford (2012) 'The Brussels Effect', *Northwestern University Law Review*, Vol. 107, *Columbia Law & Economics Working Paper* No. 533.

Barbulescu v. Romania 61496/08

Bence Juhász, (2019) 'Manipulation, Exploitation and Information', Texas A&M University, unpublished.

Bond, R., Fariss, C., Jones, J. et al. (2012) 'A 61-million-person experiment in social influence and political mobilization', *Nature* 489**,** 295–298. https://doi.org/10.1038/nature11421

Bumper v. North Carolina, 391 U.S. 543

Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523

Carpenter v. USA 585 US ___.

Charles S. Desmond (1953) 'Natural Law and the American Constitution', *Fordham Law Review*, Volume 22 Issue 3 Article 1.

Christina Sagioglou and Tobias Greitemeyer (2014) 'Facebook's emotional consequences: Why Facebook causes a decrease in mood and why people still use it'. *Computers in Human Behavior*. 35. 359–363.

Christine Goodwin v. The United Kingdom, no. 28957/95

Cinelli et al. (2020) 'Echo Chambers on Social Media: A comparative analysis', Cornell University https://arxiv.org/abs/2004.09603v1

Claudio Celis Bueno (2016) *The Attention Economy: Labour, Time and Power in Cognitive Capitalism*, Rowman & Littlefield International.

Costa v. Enel 6/64.

D'Arienzo, M.C., Boursier, V., Griffiths, M.D., (2019) 'Addiction to Social Media and Attachment Styles: A Systematic Literature Review'. *Int J Ment Health Addiction* 17, 1094–1118.

Dan M. Kahan (2017) 'Misconceptions, Misinformation, and the Logic of Identity-Protective Cognition', *Cultural Cognition Project Working Paper Series* No. 164, Yale Law School, Public Law Research Paper No. 605, Yale Law & Economics Research Paper No. 575.
Dieter Grimm (2010) 'The Basic Law at 60 – Identity and Change', *German Law Journal*, vol. 11, no. 1, 33–46., p 43.
E-Privacy Directive 2002/58/EC
Eleni Frantziou (2020) 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle', *Cambridge Yearbook of European Legal Studies*, vol. 22, 2020, pp. 208–232.
Elisabeth Lambert Abdelgawad (2008) 'The execution of judgments of the European Court of Human Rights', CoE Publishing,
Elise Muir (2014) 'The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges', *Common Market Law Review* 51: 219–246.
Emma Dorn et al., (2020) 'New evidence shows that the shutdowns caused by COVID-19 could exacerbate existing achievement gaps', McKinsey, accessed from: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/covid-19-and-student-learning-in-the-united-states-the-hurt-could-last-a-lifetime#
Facebook on Predicting by Machine learning: https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads
Fernando Mendez and Mario Mendez (2009) 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States', *The Journal of Federalism*, vol. 40 (4), pp. 617-645.
FTC (2009) 'A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority', retrieved from: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Gelijn Molier and Bastiaan Rijpkema, (2017) 'Germany's New Militant Democracy Regime: National Democratic Party II and the German Federal Constitutional Court's 'Potentiality' Criterion for Party Bans, Bundesverfassungsgericht, Judgment of 17 January 2017, 2 BvB 1/13, National Democratic Party II.', *European Constitutional Law Review*, vol. 14, no. 2, 394–409.
General Data Protection Regulation 2016/679

Gráinne De Búrca (2011) 'The road not taken: the European Union as a global human rights actors', *The Americal Journal of International Law*, Vol. 105, No. 4, pp. 649-693.
Immanuel Kant, (1785) [1983]. 'Grounding for the Metaphysics of Morals', in I. Kant, *Ethical Philosophy*, James W. Ellington (trans.), Indianapolis, IA: Hackett Publishing Co.
J. Celement (2020) 'Facebook: advertising revenue worldwide 2009-2019', Published Feb 28, 2020 https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/
J. Clement (2020) 'Google: annual advertising revenue 2001-2019', Published Feb 5, 2020 https://www.statista.com/statistics/266249/advertising-revenue-of-google/
Jean-François Akandji-Kombe (2007) 'Positive obligations under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights', CoE, Human rights handbooks, No. 7.
Jeremy Waldron, (1989) 'Autonomy and Perfectionism in Raz's Morality of Freedom', 62 *S. CAL. L. REV.*
John Rawls, (1980) 'Kantian Constructivism in Moral Theory: The Dewey Lectures 1980', Journal of Philosophy 77. 515-572. In Will kymlicka (2002) *'Contemporary Political Philosophy, an Introduction'* Oxford, OUP.
John Stuart Mill, (1859) [1975] *'On Liberty'*, David Spitz (ed.), New York: Norton.
Johnson v. United States, 333 U.S. 10, 13.
Jürgen Habermas (1992) 'Citizenship and National Identity: some reflections on the future of Europe', Praxis International, 12/1: 1-19. 1992:7 in Will Kymlicka's (2002) *'Contemporary Political Philosophy an Introduction'*, Oxford University Press,
Jürgen Schmidhuber (2015) 'Deep learning in neural networks: An overview', *Neural Networks*, Volume 61, Pages 85-11 ISSN 0893-6080,
Katz v United States 389 US 347
Linda Martin Alcoff, (2007) 'Epistemologies of Ignorance, Three Types' In: Shannon Sullivan and Nancy Tuana (Eds.) *Epistemologies of Ignorance*, State University of New York Press.
Lynn Mather (2008) 'Law and Society', In: Gregory A. Cladeira, R. Daniel Kelemen, Keith E. Whittington (Eds.), *The Oxford Handbook of Law and Politics*, Oxford University Press.,
Marbury v. Madison 5 U.S. 137. (1803)
Marco Botta and Klaus Wiedemann (2019) 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook

Odyssey', *The Antitrust Bulletin*, vol. 64, no. 3, pp. 428–446, doi:10.1177/0003603X19863590.
Mark Tushnet (2015) *The Constitution of the United States of America A Contextual Analysis*, 1. An Overview of the History of the US Constitution, Hart Publishing,
Matt Zwolinski and Alan Wertheimer, 'Exploitation', *The Stanford Encyclopedia of Philosophy* (Summer 2017 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/sum2017/entries/exploitation/
Matthias Mahlmann (2017) 'Normative Universalism and Constitutional Pluralism', In: Iulia et al., (eds): *Liber amicorum András Sajó: Internationalisation of Constitutional Law*.
Matthias Mahlmann (2012) 'Human Dignity and Autonomy in Modern Constitutional Orders', In: *The Oxford Handbook of Comparative Constitutional Law* (Eds): Michel Rosenfeld, András Sajó, Oxford, OUP. 371-393.
McCrudden, (2006) 'Legal Research and the Social Sciences', 122 *Law Quarterly Review* pp. 632-650.
Mirjam de Mol (2011) 'The novel approach of the CJEU on the horizontal direct effect of the EU principle of non-discrimination: (unbridled) expansionism of EU law?', *Maastricht Journal of European and Comparative Law*. 18(1-2):109-135.
of the European Court of Human Rights', CoE Publishing,
Oreste Pollicino (2021) ' Digital Private Powers Exercising Public Functions:
Proceedings of the National Academy of Sciences 111 (24) 8788-8790.
Renato Nazzini (2011) 'The Objective of Article 102', In: Renato Nazzini, *The Foundations of European Union Competition Law: The Objective and Principles of Article 102*, Oxford Studies in European Law, OUP Oxford, pp. 109-110.
Robert Leckey (2017) 'Review of Comparative Law', *Social & Legal Studies*, pp. 3-24, (p. 16)
S. Vosoughi, D. Roy, S. Aral. (2018). 'The spread of true and false news online', *Science*. Vol. 359, Iss 6380.
Seda Kücükdeveci v. Swedex GmbH & Co. KG Case C-555/07
Shoshana Zuboff (2019) *The Age of Surveillance Capitalism*, Public Affairs Books, New York.
Shoshana Zuboff (2020) 'You are now remotely controlled', NY Times, https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html
Smith v. Maryland, 442 U.S. 735

Statista (2021) The 100 largest companies in the world by market capitalization in 2021 https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

Stephen Gardbaum (2003) 'The "Horizontal Effect" of Constitutional Rights', *Michigan Law Review*, Volume 102, Issue 3, UCLA School of Law.

The Constitutional Paradox in the Digital Age and its Possible Solutions', ECHR, accessed from: https://echr.coe.int/Documents/Intervention_20210415_Pollicino_Rule_of_Law_ENG.pdf

The Guardian (2013) 'Tech giants may be huge, but nothing matches big data', https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Unesco, Global Monitoring of School Closures, accessed from: https://en.unesco.org/covid19/educationresponse

United States v. Jones, 565 U.S. 400

United States v. Miller, 425 U.S. 435

Vicki C. Jackson (2012) 'Comparative Constitutional Law: Methodologies' In: Michel Rosenfeld and Andras Sajo (Eds.), *The Oxford Handbook of Comparative Constitutional Law*, OUP.

Viktor Vanberg, (2011) 'Consumer welfare, total welfare and economic freedom: on the normative foundations of competition policy'. Competition Policy and the Economic Approach: Foundations and Limitations, Freiburg Discussion Papers on Constitutional Economics, 09/3.

Werner Mangold v. Rüdiger Helm C-144/04

X and Y v. Netherlands, no. 8978/80