Hastings Science and Technology Law Journal

Volume 13
Number 2 *Spring 2022*

Article 4

Spring 2022

A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence

Ruben de Bruin

A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence

RUBEN DE BRUIN*

TABLE OF CONTENTS

* de Bruin, a Dutch and British national, holds a first class law degree from the University of Glasgow and an LL.M. in Technology Law from UCLA School of Law. During his LL.M. de Bruin focused his research on the intersection of antitrust law, technology and data privacy law from a European and U.S. comparative perspective. Upon graduation, de Bruin worked within Government consulting at Accenture in London and is currently a PhD candidate at the University of Luxembourg School of Law. de Bruin's PhD focuses on the Digitalization of EU External Relations Law by analyzing the impact of technology on regulatory developments within the areas of digital disinformation campaigns, data privacy and wider sustainable development goals on the global stage. de Bruin sat for the New York bar in July 2022.

PART I

A. Introduction

This paper provides a comparative critical analysis of the data privacy laws in the European Union and the United States. The first part will provide a descriptive analysis of the EU and U.S. regulatory framework and aims to illuminate the divergent approaches the respective frameworks take in relation to data privacy. By way of demonstrating how these jurisdictions differ, it provides an underlying foundational understanding of the history, rationale, and legal justifications of the respective policy frameworks. This paper recognizes the divergent interpretations both jurisdictions place on the individual as the ultimate bearer of legal rights.[1] Namely, the U.S. places considerable weight on marketplace discourse where the individual is seen as a "privacy consumer." As a participant in the digital market the individual trades her personal information in exchange for "free" services, thereby commodifying data as a way of serving the market's purpose. A lot of this reasoning hinges on the benefits of innovation and the economic flourishing granted by the rise of technology companies, thus in its view worthy of considerable protection. The EU's approach to data privacy places significantly more weight on the individual rights of its "data subjects." The emphasis on dignity and democratic self-rule have been central to the European project since the end of World War II. Although the EU recognizes the economic benefits of international data transfers within the "Digital Single Market," the enacted General Data Protection Regulation[2] places strict limits on such activity. The EU's rights-centred framework provides an interesting comparison to the U.S. "patchwork"[3] of information privacy law, which this paper aims to address in more detail.

With such divergent underlying interests and foundational rationales at play, working towards a harmonized international data transfer framework becomes increasingly difficult to achieve. However, the inter-jurisdictional

1. Paul M Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 115 (2017).

2. General Data Protection Regulation (GDPR) (EU) 2016/679.

3. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 118.

operability of data and the interconnectivity of technology makes the need to devise such a framework inevitable. In order to understand which approach will work, it is essential to go beyond the underlying theoretical explanations provided in the first part of this paper and complement these with the practical realities that shape so many of our bilateral agreements today. Therefore, the second half will delve further into the underlying theoretical rationales underpinning the contemporary data privacy frameworks of the EU and U.S. and attempt to critically analyse the practical coherence of these premises. In doing so, it bridges theory with practice by assessing whether any ulterior explanations exist regarding these jurisdictions' inherently contrasting views to data privacy. It will argue that the different evolutionary trajectories of the data economies in these different parts of the world, should be attributed beyond the divergent regulatory philosophies underpinning them.

In doing so, this paper will demonstrate that these competing trends go beyond the clear-cut distinction that try to place the U.S. in the realm of advancing economic prosperity and the EU within the confines of a mere rights-based context. Namely, competition policy plays an equally important role, one from which privacy cannot be detached. In order to attain a balanced framework that recognises the economic benefit of data transfers on the one hand and privacy on the other, the intellectual debate around the importance of privacy within the confines of competition analysis has become more prevalent than ever. This approach is necessary for the preservation of autonomy, dignity, privacy and competition. Core democratic principles that come hand-in-hand with any regime that focuses on data transfers and innovation. With a coordinated and targeted framework that understands the underlying dynamics of contemporary digital markets, can adequate policy instruments and effective techniques for their implementation at an international level be realized. Something the current transatlantic data transfer regime fails to administer by implementing measures that disregard the inherent complexities of today's data-driven economy. This paper advocates a step-by-step approach to achieving a detailed and sophisticated framework by focusing on both *ex-ante* and *ex-post* regulatory techniques that will, in turn, enable economic growth to take off and privacy concerns to be protected. Thereby bringing the EU's undue attachment to fundamental rights and the U.S.'s obsession with ongoing economic prosperity, within the confines of a balanced and proportionate framework that serves in the interest of both transatlantic competition and data privacy.

B. The United States Framework

In the United States data privacy law is based on the conception of data marketability. This view merits governmental protection in a marketplace marked by deception and unfairness.[4] Therefore, the United States' legal framework in the area of data privacy focuses primarily on the "marketplace discourse" regarding personal information and the safeguarding of individuals participating in the digital market, who are referred to as "privacy consumers."[5] In this view the individual is a trader of a personal commodity, namely her personal data. According to this line of reasoning the individual partakes in market relations within the confines of the digital economy and is placed into this digital market realm without any knowledge or prior intent to participate in it in the first place. To understand the origins and rationales of this version of individual legal identity, it is necessary to understand the historical, cultural and legal understandings of data privacy in the United States and how this view is reflected in the constitutional and statutory protections granted to the privacy consumer in the first place. This in turn depicts the relative legal status of the individual *vis a vis* the entities that collect and process personal data and thus the extent to which the privacy consumer in the U.S. is considered autonomous in relation to the transfer of their personal data.

The underlying rationale for relying on marketplace discourse around privacy is clearly emphasized in the 2012 report, *Consumer Data Privacy in a Networked World.*[6] This report focused on consumer confidence and trust in the technologies and companies that drive the digital economy. The White House notes the positive role of data trade and the governmental role in "promoting innovation."[7] In this regard, the report's view places personal data as the catalyser for the advertising marketplace which in turn "brings many online services and sources of content to consumers for free."[8] It is the bilateral self-interest that holds sway, where personal information is another commodity in the market that contributes to human flourishing to the extent that the individual can maximize her preferences regarding data trades.[9] Information privacy law in the U.S., therefore, follows the logic of the market place as opposed to the protection of privacy rights when policing fairness in exchange of personal data. This line of reasoning bears its foundation from

4. *Id*. at 119.

5. *Id*.

6. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 41-32 (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

7. *Id*.

8. *Id*. at 5.

9. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 132.

the start of the Internet's commercialization, which occurred during the Clinton Administration.[10] The positive economic impact of technology companies shaped the thinking of policymakers around the time and set a rationale for shaping a legal framework that sought to actively protect the technology sector's growth.[11] Namely, the "rights-bearer of U.S. information privacy is a consumer who benefits from the presence of innovative technologies and merits protection from market failures."[12] This conflation of economic progress and individual benefit "is to be expected in an era that does not differentiate too pedantically between what is good for business and what is good for people."[13] As a result, regulators have relied on industry self-regulation within this sphere of economic progress and established the importance of this aim in the 1997 Commerce Department compilation of papers regarding self-regulation of privacy in the information age.[14] More recently, however, the promotion of innovation and the protection of consumer trust were central under the Obama Administration and it hoped that "consumer data privacy could help establish more flexible, innovation-enhancing privacy models among our international partners."[15] Yet, with the strongest constitutional protections in the U.S. being granted to data processors as opposed to individuals, it is undeniably clear that innovation as opposed to consumer privacy won the upper hand in this strive to fairness.

Under the U.S. Constitution, there is no right to information privacy as there is a right to data protection in the EU. The absence of such positive rights granted by the government can be traced back to the underlying foundational principles used for drafting the U.S. Constitution. Namely, the constitution does not oblige the government to take positive steps to create conditions to allow for the existence of fundamental rights.[16] The Constitution's creation of a government of only limited powers reflects the American fear of oppression from governmental power.[17] In particular, the State Action Doctrine demonstrates this limited reach in the area of individual rights. Namely, regardless of how strongly an activity protected as a recognized

10. *Id*. at 137.

11. *Id*.

12. *Id*.

13. Steve Poole, "*To Save Everything, Click Here by Evgeny Morozov – Review*", THE GUARDIAN (Mar. 20, 2013), https://www.theguardian.com/global/2013/mar/20/save-everything-evgeny-morozov-review.

14. U.S. DEP'T OF COM., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (June 1997), https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age.

15. Consumer Data Privacy, 1.

16. *Deshaney v. Winnebago City Department of Social Services*, 489 U.S. 189, 196 (1989).

17. Frank I. Michelman, *The State Action Doctrine*, in *Global Perspectives on Constitutional Law* 228, 234.

individual right has been interfered with, if it occurred though private action the Constitution does not apply at all.[18] One of the main purposes of this doctrine is that "individual liberties shall be protected by ensuring that private action is not subject to constitutional limitations . . . ."[19] This purpose undoubtedly gives way to problems when individual rights infringements occur in private relationships. For example, when a private company collects and processes private data of individuals without the latter's informed and explicit consent, the state action doctrine prevents the application of individual rights because the actors are private. The Supreme Court's reasoning for this doctrine is that it "preserves an area of individual freedom by limiting the reach of federal law and federal judicial power."[20] However, "preserving areas that are free from individual rights does not mean that these areas are free from individual rights infringements."[21] The result may actually be less as opposed to more individual freedom because "state and private actors are free to interfere with people's individual rights, unless limited by other federal or state law."[22] The only freedom truly protected, therefore, is the freedom of the infringer, not the freedom of the infringement's victim. Over time the court has developed exceptions to this principle.[23] In my opinion, the fact that these are exceptions as opposed to matters of principle demonstrate that the lack of any constitutional protection of data collection under the U.S. constitution won't change any time soon.

Disputes around information privacy in the public sector brought before the courts have addressed the availability of the right to privacy in numerous occasions. However, the most recent case concerning the availability of the right proved to be unresolved and therefore any doubts regarding its potential existence have been kept in place.[24] The two most important sources of this interest are the fourth Amendment and the Due Process Clause of the Fourteenth Amendment.[25] The Fourth Amendment protects individuals against the collection of certain kinds of personal information by the government and safeguards the rights of the people to be secure against searches of

18. Stephan Jaggi, *State Action Doctrine*, Oxford Constitutional Law (Oct. 2017), https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e473.

19. *Id*.

20. *Lugar v. Edmondson Oil* Co., 457 U.S. 922 (1982).

21. Jaggi, *State Action Doctrine*, https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e473.

22. *Id*.

23. *Herndon v. Nixon*, 273 U.S. 536 (1927).

24. *Nasa v. Nelson*, 562 U.S. 134 (2011).

25. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 133.

"persons, houses, papers and effects."[26] However, this Amendment fails to accord to "the conditions of modern governmental use of personal data in routinized databases that administer public benefits and services."[27] Namely, "the government's action cannot be limited by a constitutional concept first requiring a search or seizure when referring to information already in its databases."[28] Moreover, Supreme Court precedent does not protect the individual when a "third party", such as a bank, surrenders personal information to the government.[29] Data processors are also using the First Amendment to stop or narrow information privacy laws, which has undoubtedly proven successful.[30] In this capacity, the Supreme Court invalidated a Vermont law that prevented pharmacies from selling prescriber-identifying information without the prescribing party's consent because of its restriction of "speech in aid of pharmaceutical marketing."[31] This once again shows that the free flow of data, not personal privacy, serves as the underlying concern in relation to the most significant constitutional safeguards for information in the U.S. Article III's requirements for standing have also proved to be ill-equipped for effective recourse to the judicial system. A claimant must establish concrete harm in order to demonstrate its case or controversy under Article III.[32] The difficulty for establishing this requirement was further limited by the Supreme Court when it established constitutional parameters for standing in privacy cases.[33] Namely, more than a "bare procedural violation" of a statute had to be shown.[34] A "concrete and particularized" privacy harm resulting from a party's shortcoming needs to be demonstrated.[35] As privacy harms in our digital world tend to be abstract and unquantifiable infringements due to their anonymity and encrypted way of being stored on databases, claimants have a very high burden to convince the court of their "concrete and particularized" injury.

The overarching focus of U.S. data privacy policy is one of continued innovation and economic prosperity. The digital revolution that has proved to be quintessential to the rise in technological development, which in turn spurred economic growth, serves as the foundational rationale of the

26. U.S. Constitution Amendment IV.
27. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 133.
28. *Id*.
29. *Id*.
30. *Id*. at 134.
31. *Sorrell v. IMS Health Care*, 564 U.S. 552, 557 (2011).
32. *Clapper v. Amnesty International USA*, 133 SC 1138, 1155 (2013).
33. *Spokeo v Robins*, 136 SC 1540, 1550 (2016).
34. *Id*. at 1549.
35. *Id*. at 1547.

"patchwork" of the U.S. data privacy rules.[36] The result has been increased policy in favour of further expansion of digital technology giants and seeing the individual as a "privacy consumer" in order to advance the ongoing surge in economic progress. In short, information privacy law in the U.S. envisions privacy interest protections as being embedded within the market structure and specific consumer relationships.[37] The procedural protections in place reflect this notion by setting strict parameters for making a successful data privacy claim. The current framework's failure, or unwillingness, to recognize the privacy cost to consumers in return for "free" online services demonstrates this beyond anything else.

C. The European Union Framework

The EU data privacy framework derives its rationale from a rights-based perspective centred on the individual whose data is processed. Data protection is, therefore, afforded constitutional protection as a fundamental right anchored in interests of dignity, personality, and self-determination.[38] The emergence of fundamental rights and, in particular, the recognition of the right to dignity and personality within the constitutional law of different legal systems begun before World War II. However, it was not until after the war that the constitutions of Italy (1947) and Germany (1949) were at the forefront of entrenching these rights into their legal orders.[39] The continent's terrible experience of fascism, totalitarianism, and authoritarianism emanating from these countries, sparked the foundational elements for the European interest in privacy and data protection.[40] Moreover, the influence of secret police operations conducting large-scale surveillance and data gathering practices in Western and Eastern Europe alike has profoundly increased the sensitivities towards data protection throughout the EU.[41] These experiences coupled with the rise of dignity and personality interests in European Law played vital roles in the development of information privacy rights.

This European wide appeal to the creation of a post-war identity resulted in the development of a supranational system of fundamental rights, which are now protected by institutions such as the European Court of Justice, within the EU, and the European Court of Human Rights, separated

36. Schwartz and Peifer, *supra* note 1, at 132.

37. *Id*. at 136.

38. *Id*. at 123.

39. Grundgesetz (GG) (Basic Law), art. 1-2; art. 2-3 Constituzione (Italian Constitution).

40. Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CAL. L. REV. 1925, 1948-49 (2010).

41. *Id*.

from the EU's realm.[42] The Charter of Fundamental Rights (*hereafter*: the Charter) serves as a key constitutional document of the EU, whereas the European Convention of Human Rights (*hereafter:* ECHR) serves as an international treaty and binds the contracting states as part of its body of international law.[43] Together they function as the two pillars of fundamental rights in Europe. EU law, in contrast, functions as a supranational body to which the 27 Member States shift part of their sovereignty. In turn, the EU issues binding directives and regulations which, once enacted, become binding law within and between the Member States.

Fast-forward in time where the European rights regime "came to include not only privacy, but also an explicit right to data protection."[44] Namely, the ECHR grants the individual a "right to respect for his private and family life."[45] The European Court of Human Rights (*hereafter*: ECtHR), which was established by the ECHR, built on this right to identify specific rights regarding data protection. In *Copland v United Kingdom*[46] the court held that the collection and storage of personal information related to an individual's telephone, e-mail, and Internet usage, without her knowledge, implicated Article 8 rights. Akin to the ECHR, the Charter under the EU protects privacy and also contains an explicit right to data protection under Article 8(1).[47] What becomes evident from our assessment of the institutional guarantees of fundamental rights and data privacy in particular, is that the EU has an overlap of judicial institutions and governance layers for their protection.[48] To go even further, the European Court of Justice (*hereafter*: ECJ) has recognised the debate between the relationship of the right to privacy in Article 7 of the Charter and Article 8 of the Convention, and the explicit right of data protection under Article 8 of the Charter.[49] In the cases *Schecke* and *Eifert v Land Hessen*[50] the ECJ combined both concepts and held that EU law protects the right to respect for private life with regard to the processing of personal data, thereby formally constitutionalizing data protection within EU law. Furthermore, in contrast to the U.S. approach the

42. European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 364/10; United Nations Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222.

43. Council of Europe, European Convention on Human Rights, Nov. 4, 1950, art. 1.

44. Schwartz and Peifer, *supra* note 1, at 125.

45. Council of Europe, European Convention on Human Rights, Nov. 4, 1950, art. 8.

46. Copland v. United Kingdom, No. 62617/00, Eur. Ct. H.R. at 12 (2007).

47. Art. 8(1) reads as follows: "Everyone has the right to the protection of personal data concerning him or her."

48. Schwartz and Peifer, *supra* note 1, at 125.

49. *Id.*

50. C-92/09 and C-93/09, 2010 E.C.R. 662 at Para.52.

rights to privacy and data protection under EU law do not merely constrain the government, but they also require *positive* government action to protect the individual. Beyond these "vertical" rights applications concerning government-on-private matters, rights applications also reach private-on-private relations and thereby have "horizontal" effect.[51]

The above demonstrates that the resulting European data protection framework views the data subject, i.e. the individual, as central to its analysis and places her as the ultimate bearer of rights. In this regard "it views data privacy as part of its legal culture of fundamental rights."[52] However, beyond a historical and descriptive perspective it is also essential to illuminate the foundational legitimacy for the framework's existence and its understanding of where the individual's legal identity comes from when placed in the EU context. Namely, data protection law is leading the effort in the hope of creating a sense of European citizenship through development and enforcement of European constitutional rights. Thus, its aim is to protect individuals from risks to "personhood."[53] What this ultimately means is that adequate protections and limitations on the type of personal information that can be traded is dependent on the preservation of democratic self-rule, the protection of autonomy, preventing the erosion of the capacity of self-determination and avoiding a negative collective impact. The aspiration to create a new model of political cooperation with the goal of bringing lasting peace to Europe, has been the main catalyser and rationale for enabling these functions. According to this line of reasoning adequate protections against the collection, use, or transfer of personal data also serves the wider policy initiative that contributes to the EU's aim of preventing negative impact on democratic values, which in turn serves the framework's underlying principles and rationale.[54]

However, beyond the safeguard of privacy and data protection for the individual, the EU also protects the free flow of information. By establishing an internal market for personal data in which there is "free movement of goods, services and capital," it endeavors to ensure both a free flow or personal data from one member state to another, and "high standards of data protection to protect the fundamental rights of individuals."[55] Therefore, beyond the emphasis on democratic self-rule and dignity, the EU has a profound interest in access to the global information economy and its resulting

51. *Mangold v Helm*, 2005 ECtHR 709, (Nov. 22, 2005).

52. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 126.

53. *Id*. at 145.

54. *Id*. at 171.

55. Council Directive 95/4, art. 3, 1995 O.J. (EC).

economic proliferations.[56] The "Digital Market Initiative" of the EU shows its awareness of the benefits in participating in relations that promote advanced technology and related services.[57] Of course, upon initial reflection this inevitably gives rise to conflicting ideals. But, if these two competing, or arguably complementary interest, conflict, the ECJ undertakes a proportionality analysis. Under this test, the question is whether the law's protection of another relevant interest can be carried out in a way that is least restrictive to the protection of privacy.[58] In contrast to the U.S., the EU's economic interests in information and the potential negative impact on the activities of data processors are not considered to be especially important.[59] In the case of *Google Spain* the ECJ held that the free flow of information matters, but not as much as the safeguarding of dignity, privacy, and data protection under the European rights regime.[60] The General Data Protection Regulation[61] speaks of this importance and sets out the balance between the free flow of information and a high level of protection of personal data within its framework.[62] Under the GDPR, the aforementioned high status of the data subject comes to the foreground once again. Namely, by way of Regulation EU law mandates directly binding statutory protection for the data subject throughout the EU. Furthermore, this safeguard is more than evident in the area of damages following from harms to the individual. No materiality factors in cases of a serious injury of one's sphere of privacy need to be proven and the GDPR explicitly states that it does not depend on harm to a monetary or property interest when personal information is misused.[63] Although data protection is not "boundless" under the EU data protection framework, the above demonstrates that it grants data subjects a privileged position in a way that is substantially different from that of its U.S. counterpart.[64]

56. Schwartz and Peifer, *supra* note 1, at 130.

57. European Commission, *Digital Single Market – Bringing Down Barriers to Unlock Online Opportunities*, https://ec.europa.eu/commission/priorities/digital-single-market_en.

58. Schwartz and Peifer, *supra* Note 1, at 131 (discussing Alec Stone Sweet, *Governing with Judges* (2000)).

59. Commission Regulation 2016/679, art. 7. 2016 O.J. (L119) 1.

60. *Google Spain v Agencia Española de Protección de Datos* (2014) (Case C-131/12) No.80 (Spain).

61. Commission Regulation 2016/679, 2016 O.J. (L119) 1.

62. Commission Regulation 2016/679, arts. 6-7. 2016 O.J. (L119) 1.

63. Jan Philipp Albercht and Florian Jotzo, *Das Neue Datenschutzrecht der EU* (Ger.), 2017, at 126-129.

64. Commission Regulation 2016/679, art. 82. 2016 O.J. (L119) 1.

D. Divergence of Data Privacy Regimes

The first part of this article has demonstrated the divergence in approach towards data protection regulation between the EU and U.S. By way of addressing the underlying history, rationale and legal justifications of the respective jurisdictions, it provides a foundational comparative understanding for how and why these regimes differ. To reiterate, U.S. data privacy law is based on the conception of data marketability where the individual is seen as a market participant by way of trading a personal commodity, namely her personal data. This rationale stems from the view that sees data transferability as essential to the promotion of innovation. The positive economic impact of technology companies, therefore, shaped the thinking of U.S. data privacy law and ultimately serves to protect the technology sector's continuing growth. On the other hand, the EU data privacy framework finds its origins throughout history. Two World Wars and extensive government surveillance and data gathering practices during the Cold War played vital roles in the development of information privacy rights. Therefore, the rise of dignity and personality interests sparked the European wide appeal to the creation of a post-war identity. The adoption of the GDPR and institutions such as the ECJ and ECtHR came as a result and protect the established supranational system of fundamental rights. With an explicit right to data protection under EU law, its framework views the individual as central to its analysis and places her as the ultimate bearer of rights. In this regard, the framework aims to protect the individual's personhood, autonomy and its capacity of self-determination, which serve the aspiration of bringing lasting peace to Europe. This line of reasoning has been transposed into the contemporary framework of data transferability, as can be seen by the limits put in place on such practices. Ultimately, they contribute to the EU's aims by preventing the negative impact on democratic values, and thus serving the framework's underlying principles and rationales.

By way of further expanding on this comparative analysis, the next section of this paper will critically analyse these frameworks by addressing the potential for future harmonisation and cooperation in the area of international data transfers. It gives a fundamental understanding of how underlying political, ideological and competition law (in the U.S. commonly referred to as antitrust la) influenced dynamics all play their respective, mutually reinforcing, roles in understanding both regimes and their potential for convergence. In this capacity, it will demonstrate that the clear-cut "distinction" that tries to place the U.S. in the realm of advancing economic prosperity and the EU within the confines of a mere rights-based context garners further exploration and analysis. Precedent international data transfer frameworks provide constructive context when addressing the question of what a future

international data transfer framework can and should look like. Simultaneously recognizing how technology outpaces the law in this context, the challenge for regulators today will be to adapt their approach in achieving convergence by focusing on the inherent technicalities and complexities that define our digital era.

PART II

A. A Dissemination of the European Union's Approach

The European Union (EU) began as an economic trading zone in 1952 as the European Coal and Steel Community. But, rights talk has always formed an essential part of the European project that brought it beyond the rationalisation of trade in coal and steel or safeguarding the free movement of goods.[65] As the first part of this paper set out, the aftermath of the destruction of the second world war, heavy surveillance practices in Eastern Europe during the Cold War and the continent's overall terrible experience of fascism, totalitarianism, and authoritarianism have played significant roles in the desire for a new model of political cooperation, with the ultimate goal of bringing lasting peace to Europe. From this aspiration led the creation of the Supranational authority we know today as the EU, a body with "the power to bind its constituent member states."[66] This section will outline how the creation of the wider European project has been met with considerable challenges and how the emergence of a rights-based narrative helped overcome these obstacles by propelling the EU's project to what it has become today.

One of the oft-mentioned obstacles faced by the EU project has been the "democratic deficit" of its institutions.[67] This deficit reflects the dynamic that exists until this day where the ordinary citizen feels bound to her national government, but is likely to have a more distant relationship with the EU as a sovereign entity. As Schwartz and Peifer explain, "too often, the EU is considered a distant, inaccessible institution. There are complaints about its transparency, complexity, the dominance of its executive institutions, the inability of its citizens to replace important decision-makers, and the lack of power for more democratic EU institutions."[68] Although the response to this was an increase in the power of the European Parliament in 1979, the problems of "secrecy, impenetrability, accountability, and representativeness"[69] remained and called for a more suitable response to be made at the

65. Schwartz and Peifer, *supra* note 1, at 145.

66. Paul Craig and Grainne de Burca, *EU Law: Texts, Cases, and Materials*, at 5 (4th ed. 2008).

67. *Id*. at 133.

68. Schwartz and Peifer, *supra* note 1, at 145.

69. Craig and de Burca, *supra* note 66, at 58.

constitutional level. One commentator brings this further and argues that constitutionality is the fundamental key to Europe's future and its attainment of a post-World War pan-European identity.[70] Under this view, the development and enforcement of European constitutional rights was seen as the bridge between its citizens' distant affiliation with its institutions and the creation of a sense of European citizenship. This line of reasoning goes on to say that by blurring the lines between the current "double fashion" in which each individual participates as both a European citizen and through a role in her home nation, can its goal in achieving a fully integrated European culture be realized.[71] Habermas goes even further and argues that rights talk forms a critical part of the post-war European project of creating the identity of the European citizen, and states that this is "central to the EU's survival".[72] What this demonstrates is that the EU's development of a shared political identity is premised on the creation of a common fundamental rights framework. This in turn provides additional context for understanding the emphasis on data protection throughout the EU. In this vain, EU data protection policy serves as an underlying political smokescreen, which seeks to further the EU's prominent and most important objective of establishing a pan-European identity.[73] Both the GDPR[74] and early caselaw of the ECJ interpreting the earlier Data Protection Directive[75], emphasize similar foundational rationales that focus on an approach in attaining a so-called "common public sphere".[76] This reflects the notion of an integrated environment in which citizens of Europe will engage in democratic deliberation out of which further social and market integration takes place.[77] The European rights-oriented project serves a politically salient motive that is undoubtedly premised on the idea of bringing ever-lasting peace to Europe through an active citizenry engaged with her European identity. To a large extent, this also provides a politically motivated ulterior understanding of the 'lack' of innovation and divergence in approach towards its digital economy, in comparison to its U.S. counterpart. Namely, its desire to focus on and form a cohesive pan-European community in which its citizens feel socially, ideologically and economically connected explains its reasons for advancing privacy rights in

70. Jeremy Waldron, *The Vanishing Europe of Jürgen Habermas*, N.Y. REV. BOOKS, at 70 (Oct. 20, 2015).

71. Jürgen Habermas, *Zur Verfassung Europas* (2011), 66.

72. Id.

73. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 146.

74. General Data Protection Regulation (GDPR) (EU) 2016/679.

75. Data Protection Directive, 95/46/EC.

76. Habermas, *Zur Verfassung Europas*, 59-61.

77. Abraham L. Newman, *Protectors of Privacy Regulating Personal Data in the Global Economy*, Cornell University Press (2008), 75.

the way it has done. Thereby, using its emphasis on human rights as a façade for the myriad of other politically underlying objectives it aims to achieve. Although a rights-based approach carries highly important rationales and certainly functions as a policy reason in and of itself, the following section will demonstrate how its influence, coupled with burdensome EU competition rules, sacrificed the attainment of a balanced data privacy framework that recognizes the benefits of both innovation and privacy in accomplishing the bloc's ideological aspirations. Before doing so, it will start with a similar dissection of the U.S.'s approach to data privacy regulation before turning to that of the EU.

B. Understanding the U.S. Approach

As the previous section of this article lined out, the U.S. data privacy framework accords very weak constitutional status to information privacy. For clarification purposes I will briefly recall some of the principles underpinning the U.S. regime. The U.S. constitution is one of "negative rights" in which the reach of government action into private sector activities and disputes between private persons is significantly constrained.[78] Despite existing constitutional protections under the Fourth Amendment and Fourteenth Amendment, they prove to be poorly fitted within the digital information age in which governmental databases' have outpaced the law's outdated provisions. The widespread sharing of data by individuals is what drives the U.S. data privacy framework and the U.S. constitution serves as a force for strengthening the rights of data processors, above anything else.[79] What places the U.S. approach in such stark contrast to that of its European counterpart is the underlying belief that the privacy consumer is far more promising than a "rights model" for privacy, because it ties into deep-rooted ideas.[80] For Americans it is the sovereignty of the consumer that holds sway as the key individual identity, in which the notion of progress is tied to technology and innovation.[81] This line of reasoning accords significantly to technology platforms' way of thinking in which the "tech gurus in Silicon Valley and policymakers in Washington, D.C.", in particular, cherish anything associated with innovation.[82] Schwarz and Peifer expand on this by saying that "from the start of the Internet's commercialization, it has been associated with benefits to consumers as well the creation of great wealth for the U.S.

78. Alec Stone Sweet, *Governing with Judges: Constitutional Politics in Europe*, Oxford Scholarship Online (2000), 98.

79. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 155.

80. Id.

81. James G. Whitman, *Consumerism Versus Producerism*, 117 YALE L.J. 340, 394 (2007).

82. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 155.

economy."[83] The above makes clear how the American modern capitalist market economy has taken full-fledged advantage of the rapid rise in innovatory capacity and significant technological advancement. As a result, this clearly defends the notion that "technology linked to mass consumption is a modern American hallmark."[84] The narrower conception of U.S. data privacy, therefore, embraces a marketplace discourse in which the privacy *consumer* is afforded particular attention. Thus, factors that touch upon the area of personal autonomy, individual privacy and dignity are given significantly less weight. According to this view, data transfers catalyse the very notion of this industry's success and placing any limitations on promoting progress and innovation would go contrary to the very values underpinning not only the current framework's rationale, but also American society's belief in the advantages of their current approach.

The foregoing paragraphs endeavoured to delve deeper into the rationales underpinning, arguably, two extreme examples of frameworks within the data privacy context. My reason for doing so, is to understand what ulterior and contextual dynamics are at play in shaping the respective frameworks that go beyond conventional theoretical explanations provided in the first part of this paper. This will in turn enable this study to conduct a further critical analysis of these frameworks and assess their potential to achieve a mutually beneficial and balanced international data privacy regime. Namely, understanding the pitfalls of both frameworks will enable us to identify a suitable middle-ground, in which reasoned and realistic analysis drives us to a more pragmatic view to attaining a privacy framework that serves the needs of both business, individuals, competition and a myriad of other stakeholders. In my opinion, the conflict of jurisdictions within this novel area of law should be seen as a unique opportunity in that it has provided the necessary context and legal parameters to experiment with technologically influenced policy that could serve in the interest of nations and generations to come. The next section delves further into the influence of past and contemporary competition analysis on the U.S. and EU data privacy frameworks. It aims to demonstrate that modern competition policy should be updated for the age of digitalisation and big data. Namely, privacy and competition policy form interconnected parts within the wider policy debate that envisages a framework that takes into account privacy's vital influence on competition analysis in the data driven economy.

C. Digital Economies of Scale: First-mover Advantages v. Stifling

83. *Id*.

84. Thomas P. Hughes, *American Genesis: A Century of Innovation and Technological Enthusiasm* 1870-1970, (1989), 471.

Competition Rules

In the U.S., EU data protection is considered by some to be a form of "trade protectionism, or the result of misguided jealousy toward successful U.S. Internet companies."[85] President Barack Obama's analysis on European investigations into Facebook and Google depicts this clearly: "Oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."[86] The feeling in the U.S. that its approach promotes innovation more effectively than EU data protection does come to the foreground here. The U.S. sees the EU's framework as encapsulating stifling rules for tech firms. However, on the EU's side there are similar doubts regarding the confines of American privacy. Namely, as the EU Parliament's rapporteur for the GDPR has argued: "In the USA, the handling of our personal information is governed solely by the very vague rules of fair competition and by considerations regarding the image of the company that will be created amongst consumers themselves."[87]

Schwartz and Peifer refer to Andreas Börding's opinion when assessing U.S. information privacy when he calls to attention its "structural deficits"[88] and the former data protection commissioner of a German state who argues that U.S. companies rely on a "Violation-of-Data-Protection Business Model."[89] The EU's view that the stagnation of U.S. privacy law has made this possible accords to a broader view, which contends that the understanding of fundamental rights for the digital age in U.S. privacy law "has failed to advance beyond the 1970s."[90] Where U.S. commentators have argued that Congress is not to be trusted to craft privacy legislation and should therefore not venture into the inner complexities of online privacy issues, EU policymakers view fundamental data protection rights as something that cannot be left to the market.[91] Therefore, policymakers and academics on both sides of the Atlantic have casted doubt, and even a sense of disbelief on their respective data privacy framework counterparts.

In my opinion, the U.S.'s contention that EU data protection is the result of "misguided jealousy" is a relatively simplistic account of the

85. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 157.

86. Id.

87. Jan Philipp Albrecht, *Hands Off Our Data!*, Knaur Taschenbuch (2015), 47.

88. Andres Börding, *Ein neues Datenschutzschild für Europa*, Computer und Recht 431, 434 (2016), in *Transatlantic Data Privacy Law*, 157.

89. Thilo Weichert, *Datenschutzverstoß als Gesch. . .ftsmodell –der Fall Facebook, Datenschutz und Datensicherheit* (2012), 716.

90. Thilo Weichtert, *Globaler Kampf um digitale Grundrechte*, 47 Kritische Justiz 124 (2014), 127.

91. Thomas Davenport, *Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL ST. J. (2013), https://www.wsj.com/articles/SB10001424127887324338604578328393797127094 (last accessed Nov. 14, 2019).

underlying historical, cultural and ideological factors discussed thus far within a union of 27 individual member states. Moreover, the complexity of digital markets and their data-driven business model encapsulate highly complex structures that even detailed and targeted government regulation would fail to understand and place under its auspices. Thus, according the lack of innovation within the EU's tech industry solely to an 'emotionally influenced' reaction, in my opinion, fails to capture the total picture. Namely, data privacy frameworks alone could not have stopped the amalgamation and development of similar big technology platforms. Especially under their preliminary stages of implementation, e-commerce giants like Amazon would have ample room to refine their practices that spurred their growth in the first place and avoid basic regulation. Essentially, data privacy regulation as it currently stands is an *ex post* regulatory intervention. It emanates from the need to place dubious practices under its supervision after the fact that these previously unforeseen, novel, practices have taken place. It is the firm or business that is able to capture this market first that benefits from such advantages and grow exponentially in light of its ability to capitalize on being the only one entering a newly created market. This is, in conceptualized terms, referred to as the "first-mover advantage"[92] The next paragraph will provide a brief explanation of this phenomenon and take Amazon as an example in order to demonstrate how competition law (or antitrust law) in the U.S. created the breeding ground for such firms to grow and dominate in an otherwise novel market. This section will in turn provide a basis on which to understand the EU's initial acceptance of mergers within the digital economy before recognising the need for EU competition law to catch up with technological progress.

D. U.S. Antitrust Law

Amazon's ability to maintain its unique competitive advantage and rise to become one of the most successful online e-commerce platforms starts with the importance of this "first-mover advantage" in industries with network effects.[93] Network effects come to be defined as a phenomenon whereby a product or service gains additional value as more people use it.[94] The importance of this concept makes two important conclusions. Firstly, the existence of a network effect means that one firm, or standard, controls the market, "since bigger was always better in the eyes of consumers."[95] Secondly, these markets are, therefore, seen as winner-take-all markets and in

92. David S. Evans & Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms*, HARV. BUS. REV. (2016), 23.

93. *Id*.

94. *Id*.

95. *Id*. at 24.

becoming a winner you had to be the first to start and keep your lead.[96] For example, Amazon's business model depicts such a model by maintaining low prices and investing heavily in leveraging lines of business, thereby creating a variety of network effects to attract as many consumer as possible. The uniqueness of this model gave it its first-mover advantage and not only attracted significant consumer, but more importantly, investors' interest.[97] Amazon's investment in its integrated platform was done at the expense of profits, therefore, running consecutive losses on its operations, year upon year.[98] However, its success defies contemporary antitrust analysis as, despite, or because, of its predatory pricing and vertical integration techniques, it has become one of the most dominant e-commerce platforms in the world.[99] By taking a long-term profit maximization approach its investment ultimately paid off by its significant rise in market share and consumer attraction, which has led it to become the digital platform behemoth it is today. U.S. antitrust law failed to capture these 'first-mover' practices due to the law's inherent contradictory rationale and outdated regulatory approach.[100] The U.S.'s 'success' in enabling the creation of some of the largest and most influential technology platforms in the world goes beyond the U.S. conception of data marketability and the view of the individual as a trader of a personal commodity. Namely, it recognizes that U.S. antitrust law serves as a catalyser in enabling these firms to grow in undoubtedly anti-competitive ways.[101] The current narrowly defined "consumer welfare" test and the large influence of Chicago School thought[102] have served as underlying reasons out of which policy protection of data transferability arose. What becomes evident here is that antitrust law, therefore, serves a critical role in the expansion and regulation of the digital economy. From this, just as much as the U.S. antitrustframework 'encourages' first-mover advantages, synergies and economies of scale within the technology industry, the EU competition law framework plays a similar, albeit juxtaposed, role by constraining the ability

96. *Id*.

97. Lina M. Khan, *Amazon's Antitrust* Paradox, 126 YALE L.J. 710, 770 (2017).

98. *Id*.

99. *Id*. at 771.

100. Robert H. Bork, *The Antitrust Paradox: A Policy at War with Itself* 425 (New York: Basic Books, 1978).

101. Emily Steel, *Under Regulators' Scrutiny, Comcast and Time Warner Cable End Deal,* N.Y. TIMES (Apr. 25, 2015), http://www.nytimes.com/2015/04/25/business/media/comcast -time-warner-cable-deal.html [http://perma.cc/H4XS-9LMY.

102. Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 932 (1979).

for similar dominant European behemoths to grow.[103] Understanding the respective jurisdictions' antitrust and competition laws in turn provides yet another way to understand the deeper grounds for differences between the systems. This explanation complements the theme throughout this article by recognizing the ulterior motive analysis provided above and supports the view that not one, but several inter-connected factors contribute to these systems' divergent regulatory approaches to data privacy. However, it must be noted that due to the inherent nature of our digital economy being driven by the transfer and sale of large swaths or personal data, it is privacy and competition that warrant our particular focus throughout the remainder of this study.

E. EU Competition Law

The EU's competition rules as they stand hinder the emergence of comparable "European Champions" capable of taking on rivals from China and America.[104] The example of telecoms in the past has shown that Europe often blocks mergers that would give an operator a dominant position in a single member state. Contrastingly, American competition counterparts "tend to look at the effects of a merger across all 50 states."[105] As a result, Europe has approximately 100 operators, whereas the U.S. is shifting to three. In order for European companies to increase their profit margins and international ambitions, European competition rules need to provide more freedom for businesses to transact. The merger of the railway arms of Germany's Siemens and France's Alstom serve as a test in striving towards the creation of European Champions. Its aim was to create a "Railbus" able to compete globally much as Airbus does in aircraft. However, the European Commission seems to be hesitant towards the deal, stating the combination would yield too much power in Europe.[106] In comparison, the U.S. is already home to national champions that contribute significantly to the wider economy. The question remains why the EU's protectionist stance prevails in light of its failure to create similar European iconic companies. As one author put it, "much of the corporate lethargy is down to archaic labour rules, anaemic capital markets and a balkanised single market".[107] Beyond EU-wide

103. *The EU's industrial-policy fans want to go back to the '70s'*, THE ECONOMIST (Dec. 22, 2018), https://www.economist.com/europe/2018/12/22/the-eus-industrial-policy-fans-want-to-go-back-to-the-70s.

104. *The EU's industrial-policy fans want to go back to the '70s'*, THE ECONOMIST (Dec. 22, 2018), https://www.economist.com/europe/2018/12/22/the-eus-industrial-policy-fans-want-to-go-back-to-the-70s.

105. *Id.*

106. *Id.*

107. *Id.*

economic advantages, a merger friendly approach with concomitant privacy protections in place will enable European companies to compete at a global scale.

What this demonstrates is how the EU competition framework serves as another underlying reason for its retarded growth in the digital world. Therefore, this dynamic cannot be solemnly explained due to the divergent underlying theoretical rationale underpinning the collection and use of personal data and the EU's politically underlying motives in advancing this narrative. But, data privacy, political underlying motives, competition law, ideological and cultural understandings all play their respective roles in framing the digital market landscapes of the U.S. and EU that we know today. In particular, the relationship between competition law and privacy regulation cannot be overlooked and are increasingly being considered as part and parcel in contemporary EU competition analysis. As Wasastjerna states "data is the price consumers pay for access to various online offerings and to platforms like Facebook and Google. How that personal information is treated by businesses is becoming a competition issue."[108] According to conventional thinking competition law is interested in data for its economic value, whereas data protection rules deal with personal rights, but not necessarily the market value of data.[109] However, the value that individuals place on the protection of their personal data carries equal weight to businesses, the legal community and policy makers alike.[110] It is the EU's conventional price-centred competition analysis that has drawn it to view data as an economic value and categorised it as such in the myriad of merger control cases throughout the last decade. The Facebook-Cambridge Analytica scandal in which data from 87 million Facebook users was illegally taken from the platform for electoral manipulation fuelled citizens' awareness of the data gathering practices undertaken by large corporations and governments by way of gathering, analysing and selling their personal data. This in turn catalysed the intellectual discourse of the complex and highly fascinating intersection between competition law and data privacy.[111] As the next section will demonstrate, by incorporating privacy as a non-price element in competition analysis can it serve in the interests of the consumer by way of fostering a competitive market for data privacy solutions amongst market actors. This will in turn enable Europe to set the right standard to effectively compete in a market that is mostly dominated by American technology giants.

108. Maria C. Wasastjerna, *The Implications of Big Data and Privacy*, 30 EUR. BUS. LAW REV. 337, 338 (2019).

109. *Id.*

110. Alessandro Acquisiti et. Al., *What is Privacy Worth?*, 42 J. OF LEGAL STUD. 249, 249 (2013).

111. Wasastjerna, *supra* note 108, at 338.

F. Privacy and Competition

The increased expansion of U.S. firms such as Google, Facebook, Amazon and Apple into the EU demonstrate how privacy and competition law are substantially interlinked concepts. Although an economic cost analysis makes sense when considering potentially anticompetitive behaviour, non-price dimensions are equally important due to the very fact that citizens' personally identifiable data is being managed, processed and sold for a profit. Therefore, if the price effect of a transaction is the only factor competition authorities take into account it will inevitably lead to some anticompetitive mergers being approved "unconditionally, with a significant future costs potentially imposed on consumers."[112] Due to the fact that these U.S. tech firms are being challenged in the EU for potential anticompetitive behaviour one would expect privacy to play a prominent role in striking down their anticompetitive practices. But, to a large extent competition authorities have not been successful in explaining why privacy is and ought to be a relevant factor for purposes of competition law. Ever since the merger case of *Google/DoubleClick*[113] the debate on the relationship between competition and privacy in the context of data has been ongoing. The reason for the more gradual transition towards a more accepting approach towards privacy being a vital component of competition policy comes partly from the polarized nature of the debate. Namely, there are those who strongly advocate for competition enforcement to prevent consumer harm in the form of privacy violations, "whereas others see data as just another type of input or strategic asset, and view privacy concerns as falling outside the scope of intervention by competing enforcers."[114] Although a gradual shift is identifiable in the approach towards privacy playing a role in merger cases, this has only been gradual and relatively recent. When looking at the competition analysis in *Google/DoubleClick* and *Facebook/WhatsApp*[115], compared to *Microsoft/LinkedIn*[116] in 2016 and *Apple/Shazam*[117] in 2018, the former cases dismissed concerns related to privacy and held that "privacy harms form the increased concentration of data resulting from the transaction were outside the scope of competition law."[118] In the *Microsoft/LinkedIn* case, however, the European Commission explicitly noted that data privacy is an important component of competition and held that "by getting commitments from Microsoft that it will keep the market open, we've helped to allow companies

112. Wasastjerna, *supra* note 108, at 342.
113. Wasastjerna, *supra* note 108, at 336.
114. Wasastjerna, *supra* note 108, at 346.
115. Wasastjerna, *supra* note 108, at 346.
116. Wasastjerna, *supra* note 108, at 346.
117. Wasastjerna, *supra* note 108, at 346.
118. Wasastjerna, *supra* note 108, at 346.

to compete to protect privacy more effectively."[119] It is the ability of firms to compete in a market focused on the adequate provision of consumer privacy protection that that will set the European Commission apart from its U.S. market counterpart. Allowing U.S. technology firms to enter the EU and entrench their novel business practices that conventional EU competition rules have as of yet failed to catch up on has enabled them to accelerate the their presence as data-opolies on the continent. This in turn prevented equivalent European data-driven businesses to enter and compete with incumbent market actors.

Moreover, the import of U.S. firms that favour data transfer practices to advance economic benefit and "consumer choice", coupled with the EU's cost-based analysis of data transactions in competition policy, neglect the foundational principles of preserving dignity, self-preservation and democratic values. What becomes evident is that a certain disconnect can be found between the human rights-based privacy narrative and the practical application of EU competition law in the digital market. The EU's constitutionally entrenched privacy protections are undoubtedly crucial for preserving adverse encroachments of public and private actors on our everyday lives. But, by addressing it in silo the European Commission has come to realise that this approach renders these protections as mere theoretical safeguards that fail to grasp the realities of technological advancement. Not only was it necessary for the law to catch up, but it was vital for it to recognise privacy's inter-connectedness with the word of business and competition. The Commission aptly demonstrates this in the *TomTom/Tele Atlas*[120] case in 2018 where it noted that "confidentiality concerns can be considered as similar to product degradation in that the perceived value of the map for PND [personal navigation device] manufacturers would be lower if they feared that their confidential information could be revealed to TomTom".[121] As Wasastjerna states:

> "According to the Commission, confidentiality concerns as to the customer information question could lead to reputational damage and customers considering switching products. Here, privacy was looked at as a sort of quality component in the competitive assessment of the merger."[122]

119. Margrethe Vestager, Comp. Commissioner, What Competition Can Do – And What It Can't (Oct. 25, 2017).

120. Case Comp/M.4854 *TomTom/Tele Atlas*, C(2008) 1859.

121. *Id.* at 274-276.

122. Wasastjerna, *The Implications of big data and privacy*, 347.

Enabling firms to utilize privacy as a quality component in essence replicates the consumer welfare test by taking into account moral and non-price considerations that reflect both the all-encompassing psychological and economic facets of competition policy. Continuing on the trajectory of recognising privacy as a competition analysis element is the right way forward as it not only promotes the privacy narrative underpinning the European project as a whole, but it will enable European firms to establish themselves as legitimate competitors within the digital economy by simultaneously setting a precedent for recognising privacy as a core component of their business model. The EU and U.S. regulatory frameworks depict two extremes on a scale of protection afforded to privacy and innovation, respectively.

This further demonstrates how the contrasting approaches to privacy on both sides of the Atlantic reflect their respective cultural, economic, historical and political philosophies and rationales. Not one model is better or more equipped than the other and it is vital for policymakers and businesses alike to understand that achieving a balance between economic prosperity and privacy is the right way forward.

The above analyses provide a deeper understanding of the profounder grounds for differences in the systems and have, in turn, greatly assisted our ability in finding a way forward in devising a transatlantic data transfer framework. By recognizing both regimes' pitfalls and sacrosanct cultural and ideological interests, are we able to discern a viable middle-ground that potentially serves as an exemplary framework for countries in the future. The last section of this paper will address and provide a recommendations on the most effective regulatory approaches that enable the development of a sophisticated future transatlantic data transfer framework. In doing so, it will touch on the methods that businesses and consumers should start adopting to protect their privacy, whilst simultaneously recognising the benefits that data transfers bring to the wider economy as a whole. Before doing so, it will start by providing some context by offering a brief overview of the "Safe Harbor Agreement" and "EU-U.S. Data Privacy Shield" that serve as precedent transatlantic data transfer agreements between the U.S. and EU.

G. Safe Harbour and the EU-U.S. Data Privacy Shield

The path towards creating a harmonized transatlantic data privacy framework is not one of unchartered waters. The "Safe Harbour" was the most important first-generation solution to the issue of international data transfers.[123] Global data flows were already present in the pre-internet age and by the late 1980s European policymakers realized that their efforts to

123. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 158.

create strong safeguards for data protection necessitated transborder policies for the data of EU citizens.[124] In 1999 the influential group of national data protection commissioners already identified what can be seen as the EU skepticism about the sufficiency of U.S. information privacy law.[125] However, with the vast amounts of valuable data trade between the EU and the U.S. taking place, both sides recognized the necessity to find policy solutions to bridge the gap between their different legal approaches to citizens' data protection.[126] The result of this policy initiative was the Safe Harbor Agreement, a bilateral treaty negotiated by the U.S. Department of Commerce and the Commission of the EU that:

> "transplanted EU data protection concepts into U.S. law in a fashion beyond the willingness of Congress or the ability of the FTC and other regulatory agencies. Its principles were intended to be close enough to those of EU data protection so that the U.S. companies in following them would provide 'adequate' data protection."[127]

The initial functioning of the Safe Harbour agreement can be described as receptive on both sides of the Atlantic. The main reason that made the agreement acceptable in the U.S. was that the negotiated standards weakened classic EU principles to such an extent to make the agreement tolerable to the Americans.[128] But, it did not make them indefensible in Brussels to the extent that the EU viewed these standards as excessively watered down.[129] However, on October 6, 2015, we saw the demise of the Safe Harbour agreement's promising future as a result of the Snowden revelations, which detailed widespread collaboration by American companies with the NSA.[130] Inevitably, this called into doubt the adequacy of the protection of European citizens' data in the U.S. The European Court of Justice's opinion in *Schrems v. Data Protection Commissioner*[131] voided the Safe Harbour agreement and identified a violation of Article 7 of the Charter by the Safe Harbour's provision that enabled access to the U.S. government of the data of EU citizens.[132] Notably, the court made clear its strong criticism of the NSA's

124. *Id*.

125. *Working Party on the Protection of Individuals with Regards to the Processing of Personal Data, Opinion 1/*99, 2 DG MARKT Doc. 5092/98, WP 15 (Jan. 26, 1999), 2.

126. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 158.

127. *Id*. at 158-59.

128. Chris Connolly, *EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance*, (2013), [https://perma.cc/BAX6-PUUZ] (last accessed Nov. 7, 2019).

129. *Id*.

130. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 159.

131. Case C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. 650 (2015).

132. *Id*. at para.93.

massive suspicionless data dragnets and bulk storage of information.[133] As Schwarz and Peifer point out, the *Schrems* case marked a turning point in EU-U.S. relations and showed the EU judiciary's willingness to invalidate the main vehicle for transatlantic data flow and establish constitutional requirements for this activity to occur.[134]

With the continuing need for a transatlantic data transfer framework between the EU and the U.S. post *Schrems*, the two sides negotiated a new treaty called the "EU-U.S. Privacy Shield".[135] The Privacy Shield essentially incorporated the respective models of EU and U.S. data privacy and, therefore, is best understood as a mixture of EU and U.S. standards.[136] The EU's perspective hinged on the need to protect individuals from the state and private data processors alike. The U.S. maintained its strong market orientation and favored open choice for consumers regarding data use and their ability to retain broad access to "innovative American data services and products."[137] The mixture of EU and U.S. standards simultaneously enabled the EU to influence the agreement to resemble its fundamental principles while allowing the U.S. to argue for weaker forms of core EU data privacy principles. The Privacy Shield's balanced approach culminated in establishing four core Privacy Shield Principles; "data integrity and purpose limitation, choice, enforcement, and oversight."[138] Essentially, the Privacy Shield displays concessions by both sides regarding their conceptions of an adequate data privacy framework. However, with the European Court of Justice as the ultimate arbiter of the constitutionality of the Privacy Shield and the *Schrems* opinion in the aftermath of the Snowden revelations, the position of EU negotiators during its development phase was immeasurably strengthened.[139] Therefore, despite both sides' concessions the bilateral agreement depicts strong moves into the direction of EU data privacy principles more than the Safe Harbour agreement did.[140]

133. *Id*.

134. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 160.

135. *Remarks by U.S. Secretary of Commerce Penny Pritzker at EU-U.S. Privacy Shield Framework Press Conference*, U.S. DEP'T OF COM. (July 12, 2016), https://useu.usmission.gov/joint-press-statement-from-commissioner-vera-jourova-and-secretary-of-commerce-wilbur-ross-on-the-third-annual-eu-u-s-privacy-shield-review/ (last accessed Nov. 12, 2019).

136. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 161.

137. *Remarks by U.S. Secretary of Commerce Penny Pritzker* in *Transatlantic Data Privacy Law*, 161.

138. U.S. DEP'T OF COM., *EU-U.S. Privacy Shield Framework Principles* (2016), https://www.privacyshield.gov/Program-Overview (last accessed Nov. 12, 2019).

139. Case T-670/16, *Digital Rights Ireland v. Data Prot. Comm'r* (2016) (General Court filed Sept. 16, 2016).

140. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 163.

Arguably convergence in Europe and the United States around data privacy has occurred "within a common technological context"[141] and different countries have "converged around statutory principles of data protection, but diverged in policy instruments selected to implement and enforce them."[142] The continued bilateral effort by the EU and U.S. demonstrates their willingness to identify adequate policy instruments to implement and enforce these statutory principles effectively. However, I aim to demonstrate that underlying discrepancies remain visible in relation to these jurisdictions' approaches to data privacy that, in turn, undermine the effective and targeted realisation of a transatlantic data privacy framework. An ideal depiction of such a framework would encapsulate "the key forces for convergence in data privacy", which constitute "the shared technological environment, increased political agreement around the benefits of personal data flow, and common security and law enforcement concerns."[143] However, giving the EU the upper hand in enforcement enables such principles and balanced objectives to be compromised. This becomes increasingly evident within the confines of understanding the benefit of personal data flow between the two countries. To the same extent that U.S. companies are taking a more EU-friendly approach regarding the international flow of data, should European policymakers deploy policy initiatives to modify its law to accommodate aspects underpinning U.S. information privacy law.[144] In November 2016 the German Chancellor Angela Merkel, called for a balanced approach to data protection that accords to the age of Big Data.[145]

Rightly so, the continent benefits vastly from the flow of data within our interconnected global digital market. European industry should take advantage of the benefits that accompany the use of personal information within the confines of reasonableness, but more "than data protection currently permits."[146]

As per my above analysis, the success and growth of European industry is dependent on access to personal data and the current state of affairs places too much weight on the protection of fundamental rights. By recognising the importance of digital economic transactions, will such a framework be able to manage and balance both the economic relations and the

141. Colin, J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, CORNELL U. PRESS (1992), 150.

142. *Id*. at 6.

143. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 165.

144. *Id*. at 167.

145. *Merkel Calls for Balanced Approach to Data Protection,* Register, 2016, https://www.theregister.co.uk/2016/11/22/merkel_data_protection_big_data/ (last accessed Nov. 19, 2019).

146. *Id*.

protection of fundamental rights. In turn, this will enable both European data protection and competition law to serve as an interconnected, accommodating and advantageous framework for European business *vis-à-vis* its competitors in the U.S. and beyond.[147] Such lobbying has already started to take place and should be seen as a welcome development in devising an adequate and balanced approach to international data transfers.[148] The final section of this paper will go into more detail regarding the regulatory approach such a framework should take and endeavours to recommend the way in which the EU can use its capacity "to solve problems in a pragmatic and focused manner without sacrificing its strong fundamental rights values and traditions."[149] In doing so, it emphasizes the need for an *ex ante* regulatory approach to tackling dominant market actors that aims to understand the underlying dynamics that define today's complex digital markets. Based on this understanding we will be able to establish an effective data privacy framework that places more control within the hands of the individual regarding her personal data. As a result, such a framework will adequately address both the desire for increased data privacy and the economic benefit of data transfers to the consumer and wider economy, albeit within the confines of reasonableness.

H. A Step-By-Step Approach: Understanding Digital Market Dynamics as the Right Way Forward

The theme this paper emphasizes above is how privacy and competition law are highly related concepts in high-tech industries. By recognizing the benefit of compromise between the U.S. and EU frameworks this paper therefore argues that an effective international data transfer framework must address both market dominance and data privacy as interconnected concepts. The current digital climate enables firms such as Amazon, Google, Apple and Facebook to capitalize on data to develop better services, which attracts more users, which as a result generates more data. Finding the right balance between the benefits of data use to spur innovation and the protection of fundamental rights will aid towards the reduction of these firms' dominant market position and, therefore, serves as the right place to start. Limiting their ability to collect swaths of data, places more power in the hands of consumers and enables a more equal playing field for other market entrants to

147. Schwartz and Peifer, *Transatlantic Data Privacy Law*, 167.

148. Derek Scally, *Minister 'Heartened by Merkel Shift on Data Privacy Law*, IRISH TIMES (2016), https://www.irishtimes.com/business/technology/minister-heartened-by-merkel-shift-on-data-privacy-laws-1.2882211 (last accessed Nov. 19, 2019).

149. *Communication from the Commission to the European Parliament and Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards*, COM (2016) 117 Final (Feb. 29, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A117%3AFIN (last accessed Nov. 19, 2019).

compete. Such a framework will, in turn, enable the creation of an effective approach to regulating what information can and cannot be used by companies in their pursuit of growth. Devising such clear boundaries will, however, be much harder to accomplish in practice. Therefore, this section will demonstrate how *ex ante* regulatory enforcement, as opposed to *ex post* antitrust techniques, in combination with an effective data privacy framework can prevent the accumulation of vast amounts of data and prove beneficial to privacy and innovation. Whilst recognizing that reform is needed in competition policy, it is vital for regulators to act earlier when simpler methods or regulation can prevent the entrenchment of a dominant monopolist. Namely, "the complexity of disentangling Google's dominance emphasizes the more general point that earlier intervention is more warranted in technology markets because dislodging incumbents requires more complex remedies than traditional antitrust divestiture solutions."[150] This proposal endeavours to lay out the core principles that should serve as the foundation of a sophisticated transatlantic data transfer framework that places power back in the hands of the consumer. The precise contours and content of provisions goes beyond the scope of this paper, but it enables them to be discerned from the broader techniques and solutions it will put forward.

1. Data Portability

One approach towards achieving a harmonised international data transfer regime emphasises the need for "data portability."[151] This approach recognizes the inadvertent impossibility of circumventing data monopolists and as a result argues for "incumbents to be required to give start-ups access to some of their data and thus create more competition."[152] However, attempting to simply transfer swaths of data garnered over the years by these firms into a coherent, accessible and logical framework for the regulator to quantify is a near impossible task to undertake.[153] What type of data should be shared, in which format and "how the tension between data-sharing and privacy" can be resolved are pertinent questions in this regard.[154] The GDPR in Europe serves as an example, where bringing personal data back into the hands of the user is mandated. Such a proposal is made more complex due to the inevitable international operability of data transfers. Simply requiring

150. *Id*.

151. *Id*.

152. *Id*.

153. Frank Pasquale, *Privacy, Antitrust and Power*, 20 GEO. MASON L. REV. 1009 (2013), 1022.

154. *A New School in Chicago: How Regulators can prevent excessive concentration online*, THE ECONOMIST (June 28, 2018), https://www.economist.com/special-report/2018/06/28/how-regulators-can-prevent-excessive-concentration-online (last accessed Dec. 16, 2021).

spin-offs or imposing data sharing requirements in one jurisdiction forgets this inter-jurisdictional element. Such a proposal firstly requires a harmonized approach between the EU and U.S. that understands the fundamental workings of the digital market. Only then will this enable effective enforcement measures and implementation techniques to be developed. Namely, break-ups of tech giants and the divvying up of all the data the tech giants have collected becomes an obsolete practice in a market place composed of businesses with network effects. That is not to say that this proposal should be entirely disregarded. As one commentator argues, a better approach is to ensure that divestitures are complemented by regulation that weakens the ability of these tech giants to grow into completely new creatures once broken up, commonly referred to as the "starfish problem".[155] As will be argued below, reasoned and targeted *ex ante* regulation in combination with a privacy-oriented framework, in my opinion, serves the needs of combatting the pitfalls the regulatory landscape currently has.

2. Regulatory Sophistication

Essentially, the harms from data-opolies exceed that of conventional monopolies. Beyond the financial consequences to consumers these harms also affect our "privacy, autonomy, democracy, and well-being."[156] Contrary to Chicago School economic thought, it is evident that the data-driven market dominated by these firms will not necessarily correct itself. As explained above, antitrust law itself has proven to be ill-suited in its current form and must adapt to the current digital market landscape in order to prove the undoubtedly key role it can play in enforcement. Moreover, antitrust law serves as an *ex post* enforcement mechanism that merely enables regulators to capture firms once their dominance has already been established and practically places them one step behind these firms every time they detect anticompetitive behaviour. In my opinion, placing increased emphasis on the ability for consumers to control their personal data, thereby reducing technology companies' dominance over such data, is an effective way in accomplishing such intervention.[157] This would encourage a market where users can vote with their data and demand greater share of a company's "profits based on that data, switch to competing providers for a better deal, or withhold their data altogether after learning about the use of their data by third parties."[158] Other proposals surround "Do Not

155. *Breaking Up is Hard To Do: Dismembering Big Tech*, THE ECONOMIST (Oct. 24, 2019), https://www.economist.com/business/2019/10/24/dismembering-big-tech (last accessed Nov. 23, 2021).

156. Maurice E. Stucke, *Should We Be Concerned About Data-Opolies?*, 2 GEO. L. TECH. REV. 275, 323 (2018).

157. Ira S. Rubinstein & Nathaniel Good, *Privacy By Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1333 (2013).

158. Nathan Newman, *Search, Antitrust, and the Economics of the Control of User* Data, 31 YALE J. ON REG. 449 (2014).

Track" rules and "opt-in" consent to be required for the use of data by third parties.[159] Proposals solely focusing on this area propose to adopt greater transparency requirements regarding how tech giants monetise data. Therefore, this approach must be complemented by a technically detailed regulatory framework akin to Newman's analysis, which combines the proposals of bringing data back to the consumer with pre-determined techniques that are able to discern how data is collected, analysed and used. The *ex-ante* regulations that bring the power to control what happens with data back into the consumers' hands are vital for holding big tech companies accountable. The next section highlights how such data ownership models, flexibly applied solutions and trust mechanisms offer consumers and businesses alike the ability to achieve a sophisticated and technologically advanced approach to preserving data privacy and the advancement of innovation.

3. Data Ownership Model

One way of ensuring individuals' empowerment is by supporting the creation of a data ownership model in which consumers can be fairly compensated for their personal information which is being traded.[160] This goes contrary to those that state that "data is often considered a resource, like oil, to be traded, ideally by equally well-informed parties to the transaction."[161] In order to get to this degree of awareness, personal control over data must be offset against equally important concerns such as public interest and the rights and freedoms of others.[162] Thus, "absolute control over personal data" is difficult to guarantee and providing control is also more necessary than it is sufficient in the overall scheme of data privacy protection.[163] It forms one part of a larger puzzle of the proposed regulatory solutions and goals. One method of ensuring increased 'prosumerism' is through the creation of so-called 'data vaults'.[164] This method allows individuals to better control who can access their data and for what purpose, and requires security mechanisms that ensure that "only those entities authorized by the data subject can access the data and only those parts for which they are authorized."[165] These "personal data stores"[166] are considered to be most effective where they concern current and constantly updated information, such as geospatial data or signs of life.[167] Those that have been granted access are not only obliged to respect

159. *Id*. at 448.

160. European Data Protection Supervisor, *Opinion 4/2015, Towards a new digital Ethics* 11 (2015).

161. *Id*.

162. *Id.* at 12.

163. *Id*.

164. *Id.* at 11-12.

165. *Id*.

166. *Id*.

167. *Id*.

the rules about data sharing and use, but are also bound by the technical safeguards underpinning these systems. On the long term, this system paves the conditions for true consumer choice to be achieved as it enables data portability choices to be placed in the hands of individuals. In particular, the possibility for a consumer to change the service one is using is the "single most effective power of a consumer to influence the market of services available to them."[168] Data portability's practical possibility to transfer most of one's own data from one service provider to another, therefore, serves as an "effective starting point for creating the conditions for true consumer choice."[169] In practice this transferability is harder to achieve, which this paper will expand upon below in the section on 'Data Trusts'. Before doing so, the next section will address what exact form and shape the regulator's tools and mechanisms should take, and how they contribute to the objective of making them suited for regulating the complexity of today's technologically sophisticated market actors.

4. Technological Solutions and the Need for Flexibility

In particular, one such technological solution is the creation of 'practical data sharing models' that can combine various legal and technical approaches to data releases, that together with robust disclosure limitation techniques, can be designed to provide public access to some data without restriction.[170] This way data is able to be transformed into differentially private statistics. Thereby, restricting the use of data by data processors according to the terms of a data use agreement and accessible only though a secure 'Data Enclave' akin to the Data Vaults referred to above. Data Enclaves employ "strong data security measures, maintain operational logs, incorporate vetting of individual researchers who seek access, engage in disclosure review of outputs before data release and publication, and follow strict requirements for data retention and destruction."[171] Whenever data processors require a substantial amount of data, they would be instructed to submit an application to a review board, whose outcome would identify the permitted and restricted uses of the data. Such proposals make use of auditing procedures in which secure public ledgers, such as blockchain technologies, implement secure records of transactions, enabling robust auditing and review procedures.[172] Kagal and Pato have gone even further by introducing a system "that can express realistic data-use policies, and automated reasoning

168. *Id*.

169. *Id*.

170. *Id*.

171. *Id*. at 21.

172. L. Kagal, J. Pato, *'Preserving Privacy Based on Semantic Policy Tools'*, IEEE SEC. & PRIV. MAG. 25 (2010).

engines that can interpret those policies and automatically determine whether particular uses of data are policy-compliant."[173] By giving data processors machine-readable representations of policies it facilitates automatic compliance with those rules and enables users to preserve privacy while sharing sensitive data.[174] A data processor's job in determining which policies are applicable to a particular query is difficult to understand, but this system automatically enforces policies and lets consumers understand what kinds of queries are allowed under those policies if a request has been denied.

This aptly demonstrates the potential for technology to not only embrace the innovatory capacity of data transfers, but also embed its function into the preservation of privacy through highly sophisticated semantic policy tools.[175] However, this system functions on explicit and rigidly applicable policies to ensure that data processors can accurately ascertain whether they are using data in compliance with usage policies. In reality, many enquiries or data transfer requests will not conform to these readily ascertainable risk-benefit analyses or policy goals and as a result, require cross-sectional review by experts through flexible, universal, and consistent policy tools. Not only do these type of solutions provide stronger privacy protection for individuals, but they enable the adaptability to respond to new and sophisticated privacy leaks and attacks that "were unforeseen by regulators at the time that legal standards were drafted."[176] This systematic approach will, therefore, allow data collection and release mechanisms to "be tailored to the threats and vulnerabilities associated with a given set of data, and the uses desired by different users."[177] Furthermore, as alluded to above, new computational methods, such as secure multiparty computation andsecure public ledgers, such as Blockchain technology and executable policies, provide the ability to limit the direct operation that can be performed on data. Thereby limiting the inferences that can be made about individuals.[178]

What the above demonstrates is that constant data review "in combination with a data use agreement restricting future uses and re-disclosures of the data, as well as data privacy and security" technologies, can all be used to address many of these concerns. They touch on many foundational requirements around which an effective data infrastructure should be built.[179] By utilizing traditional tools together with more sophisticated and developed

173. *Id*.

174. *Id*.

175. *Id*.

176. Altman *et al*., *'Practical approaches to Big Data privacy over time'*, INT'L DATA PRIV. L. 10, 23 (2018).

177. *Id*. at 16.

178. *Id*. at 21.

179. *Id*.

technical tools that place control on the computation, inference, and use of data, companies can provide more systematic, regular and up-to-date review of privacy risks and appropriate practices. The conflicts of interest between the protection of data subjects on the one hand and the company's concomitant fiduciary duty towards their shareholders' profit sharing motives on the other, demonstrate that internal policy tools and mechanisms, with well-intended values and criteria, still have their limitations. Nevertheless, the awareness and consciousness within companies of their responsibility and accountability in creating the necessary infrastructure that supports the creation of a balanced data privacy framework is one step in the right direction. Yet, in the absence of a larger guiding framework the presence of these conflicts regarding ethical uses of data are likely to lead to inconsistent practices. Therefore, the need for a technological independent supervisory mechanism serves to address these deficiencies to which this paper turns to next. Namely, the inherent complexities of the underlying structural composition of our modern digital market make it nearly impossible for businesses to control, audit, and review information relating to a significant amount of individuals by themselves in an independent and fully impartial manner.

5. Trust Mechanisms as a Tool for Individual Empowerment

The data Trust proposal is an 'express Trust'[180] that requires the appointment of independent trustees who are essentially bound by the Trust's purposes and terms. These purposes and terms can vary from one trust to another according to the particular type of data sharing/protection interests data subjects have. Most important in this regard, is that this mechanism allows for:

> "[A]n ecosystem of Trusts, where a variety of data sharing policies across Trusts gives data subjects a range of choices that reflect their personal trade-offs: the resulting diversity also allows society to explore different principles for data sharing within the same digital ecosystem."[181]

A reason for arguing that a third-party independent Trust serves in the interest of both data portability and protection, as opposed to company 'in-house' review and supervisory mechanisms, emanates from the fiduciary duty of data controllers that independent trustees do not have. According to Balkin, economic and tax incentives ought the be offered to data controllers

180. L. Roderick, *'Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry'*, 40 CRITICAL SOCIO. 729, 241 (2014).

181. *Id*.

in exchange for their accepting 'fiduciary obligations'[182] towards data subjects. The problem with this proposal is that data controllers cannot fulfill their 'undivided loyalty'[183] towards data subjects as doctors or lawyers do towards their patients or clients. Namely, if a data controller has a business interest in the data provided by data subjects, this will result in a conflict "between that interest and her duty towards data subjects."[184] The fiduciary obligation towards data subjects becomes incompatible with the controllers' responsibility towards shareholders, as they would be obliged to both maximize the value of the personal data they collect whilst fulfilling their fiduciary obligation of data minimisation towards the data subjects at the same time. Delacroix and Lawrence state that the honouring of a fiduciary obligation not only demands independence from profit maximization, but also requires "an ability to relate to the complex and multi-faceted nature of the vulnerability inherent in the data subject/data controller relationship."[185] This serves as a foundational starting point from which the use and purpose of a data Trust can be determined. Instead of using ex-post compensatory tools or direct 'data processor-data subject' processing restrictions to be implemented by organisations themselves, the data Trust challenges the data governance framework 'from the ground-up.'[186] By focusing on the source of the data this framework can function on the terms and conditions its data subjects impose, without the interference of conflicting parties or interests. As a result, it also empowers data subjects right from the start.

This paper does not go into the inherent technicalities underpinning the functioning of data trusts. But, it is important to note that Trusts may specialise or generalise according to the type of data administered on behalf of the beneficiaries. For example, one Trust may specialise in health data whereas another Trust might focus on geospatial data sharing. The primary purpose is to enable an ecosystem of data Trusts to emerge that recognizes the innovatory capacity underlying data processing practices, while simultaneously providing data subjects with the ability to make independent and informed choices that reflect their political and moral aspirations.[187] The need to choose among different Trusts encourages data subjects to actively think about their sharing preferences before they are placed in a potentially vulnerable position. This not only allows the data subject to form a personal preference and conscience about his or her own values and interests in this

182. J. M, Balkin, *Information Fiduciaries and the First Amendment*, 49 UC DAVIS L. REV. 1183, 1196 (2016).

183. Delacroix and Lawrence, *Bottom-up data Trusts*, 241.

184. *Id*.

185. *Id*. at 242.

186. *Id*.

187. *Id*. at 248.

realm of privacy but also influences Trusts to accommodate those requirements with tailored approaches to data governance. As more people join data Trusts over time, the terms and conditions will also change according to the participants' particular interests. As a result, this will enable Trusts to develop stronger leverage when negotiating with data processors. Instead of agreeing to particular terms of services, users will "simply state which data Trust they belong to."[188] Only this way can we truly enable data subjects to regain control over their personal 'self' and be empowered to control public perception within the realm of our rapidly changing digital world.

This *ex-ante* policy approach forms part of an overarching inter-dependent, stakeholder approach to data governance. It is, therefore, not a 'one-size-fits-all' tool as it allows data subjects to choose a Trust that "reflects their aspirations, and switch Trusts when needed."[189] Most notably, trustees are able to exercise data rights conferred by top-down regulation (e.g. the GDPR)[190] on behalf of the Trust's beneficiaries, and are bound by a fiduciary obligation of undivided loyalty to the Trust's purpose. The way this system works is in line with the foundational legal mechanisms underpinning the functioning of traditional legal Trusts. Namely, the data trustees would "be placed in a position where they can negotiate data use in conformity with the Trust's terms, thus introducing an independent intermediary between data subjects and data collectors."[191] On the one hand, it recognizes the balance between data subjects' informed consent and on the other the ability for these Trusts to remove key obstacles to the realisation of the economic and innovative potential underlying large datasets.

I. The Need for Transparency

The techniques and solutions outlined above are a strong step in the right direction and provide regulators with a sense of the technological sophistication required in order to take the job seriously. Enforcers will ultimately need to "coordinate with privacy and consumer protection officials to ensure that the conditions for effective privacy competition are in place."[192] This in turn serves a more appropriate and balanced *ex ante* approach to regulating the data driven economy. To achieve this, we need coordinated government action to determine exactly how data mining and behavioural profiling by technological behemoths strengthens their dominance and harms consumer welfare.[193] It will take time for exact techniques to be

188. *Id*. at 249.

189. *Id*.

190. GDPR (EU) 2016/679 OJ L 119.

191. Delacroix and Lawrence, *Bottom-up data Trusts*, 236.

192. *Id*.

193. *Id*. at 446.

developed and must, therefore, be preceded by a transparent data collection framework from which more sophisticated techniques can be developed. Making information about data collection available routinely will help develop the infrastructure and analytics necessary to eventually adapt antitrust enforcement to the contemporary digital landscape.[194] It is therefore vital to work towards a rapid understanding of the actions taken by corporations that serve as the underlying complaints of potential entrants that find it impossible to enter the digital market.[195] Bringing control over users' data back to the consumer itself will, in turn, complement the development of an approach to privacy that helps create a monitoring infrastructure that systematically studies, categorises, and characterises technology firms' behaviour (as much as it happens the other way round right now). The development of such a sophisticated framework must, however, first be led by governmental entities and experts outside agencies in order to provide the fundamental structure upon which the consumers themselves can operate on the long term. Not until such a foundational regime is in place can competition law authorities as well as citizens hold large firms accountable and mandate the contours under which these firms are permitted to make use of personal data. As Bennett argues, Europe and the United States have "converged around statutory principles of data protection, but diverged in policy instruments selected to implement and enforce them."[196] The regulatory approach this paper proposes, elucidates how this ongoing convergence can accelerate both from an *ex-ante* and *ex-post* standpoint. It lays the foundation for a sophisticated and balanced framework from which more targeted policy instruments can be formulated. Only with a clear sense of how data is being collected, analysed, and used can an adequate international data transfer framework be deployed that accommodates both privacy interests, healthy competition and the economic desire to innovate.

J. Conclusion

This paper addressed the ongoing data privacy debate by delving deeper into the respective data privacy frameworks of the U.S. and EU in order to understand what underlying dynamics are shaping their inherently contradictory approaches to our digital market landscape. In doing so, it started in the first part by identifying the philosophical theories underpinning their respective rationales in an attempt to discern what ulterior motives and contextual dynamics play a role in shaping this dichotomy. It argues that the European rights-oriented project serves a politically salient motive that is

194. Pasquale, *Privacy, Antitrust, and Power*, 1022.

195. *Id*.

196. Bennett, *Regulating Privacy*, 150.

undoubtedly premised on the idea of bringing ever-lasting peace to Europe. But, to some extent it also functions as a façade to encourage the wide-scale roll-out and adoption of a European identity that is framed through a rights-based narrative. Thereby, using its emphasis on human rights as a red herring or smokescreen for the myriad of other politically underlying objectives the European project set out to achieve. Furthermore, the EU's competition rules as they stand hinder the emergence of comparable "European Champions" capable of taking on rivals from China and America. Thus, contradicting the simple notion that its anaemic capital markets are due to "misguided jealousy" towards the U.S. and that numerous factors, such as culture, ideology, history and competition policy all play a role in shaping the framework's understanding. The exact same analysis can be made in relation to the myriad of reasons underpinning the U.S.'s 'success' in creating some of the largest and most influential technology platforms in the world. Beyond the U.S. conception of data marketability and the view of the individual as a trader of a personal commodity, namely her personal data, U.S. antitrust law serves as the catalyser in enabling the ability of these firms to grow, in undoubtedly anti-competitive ways. The above analyses have enabled us to garner a deeper understanding of the profounder grounds for differences in the systems and demonstrate how a balanced framework, functioning within the bounds of reasonableness, is beyond desirable. By recognising both regimes' underlying shortcomings and potential for convergence has this paper been able to discern a regulatory approach that will serve as an exemplary model from which effective policy instruments and implementation mechanisms can be developed. The starting point must be the recognition of privacy and competition as highly related concepts in high-tech industries. Making information about data collection available routinely will help develop the infrastructure and analytics necessary to eventually adapt enforcement to serve the contemporary digital landscape. The conflict of jurisdictions within this novel area of law should be seen as a unique opportunity that has provided the necessary context and legal parameters to experiment with technologically influenced policy that could serve in the interest of nations and generations to come.

The international operability of data transfers is a depiction of the digital revolution that is shaping the way consumers, businesses and governments play their part in the contemporary digital market. The digital saturation of reality has granted companies with extraordinary capabilities and advantages to understand their customers and business with a new depth of granularity.[197] Industry lines are no longer a boundary to growth. The disruption of increasingly sophisticated technological developments enables those

197. Accenture Technology Vision 2019, https://www.accenture.com/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf#zoom=50 (last accessed Nov. 20, 2019).

early to the game to bypass competition by changing the way the market itself works. This has come in waves and it is now up to regulators to crawl under the skin of how their dynamics are changing the inherent structure of the markets. The rise of the next set of new technologies such as distributed ledger technology, artificial intelligence, extended reality, and quantum computing will catalyse the way businesses are reimagining entire industries to yet another level. The insurmountable benefits of this rapidly evolving technological era is not unencumbered by equally important and complex challenges. The ability of regulators, businesses and consumers to anticipate the impact of these changes calls for an equally sophisticated regulatory framework that addresses the needs and interests of all relevant stakeholders in the market. Only through such an approach can we take full advantage of this challenge and strive to set an example for the wider community when addressing current and future privacy concerns.

***