The Legal Debate on The Commercial Use of Personal Data - A Discussion of The EU GDPR Precedent

Senanayake, H. R. C. T.

Lecturer in Law, Faculty of Law, Horizon Campus, Sri Lanka
chiranthi.senanayake.academic@gmail.com, chiranthi@horisoncampuus.edu.lk

ABSTRACT

Although the adoption of the Personal Data Protection Act No. 9 of 2022 in Sri Lanka marked a significant milestone in the commercial use of personal data, the regulation of data use is often debated among international policymakers due to the inherent controversy of the subject. This is especially seen in the European Union (EU) which has a stringent data protection scheme. In light of this legal debate, the discussion in this study centres around the key concern of appropriate regulation and balancing between two competing rights, namely, the freedom to commercially utilise user data in the digital economy, and the protection of the right to privacy and protection from unlawful processing of personal data of the consumer/user. Such an academic conversation is engaged in by deliberating on the legal implications of commercial use of personal data. To this end, the essay will first examine the existing legal systems for commercially processing personal data with specific attention to the EU General Data Protection Regulation (GDPR) of 2016 and the associated case law. Next, the essay will discuss three concerns on the present protectionist trajectory of the law, and its impact on the dual role of the law in the digital economy, i.e. as a facilitator of lawful commercial use of personal data and a guardian of privacy rights of data subjects. Thereafter, the essay will discuss three concerns on the present protectionist trajectory of the law, and its impact on the dual role of the law in the digital economy, i.e., as a facilitator of lawful commercial use of personal data and as a guardian of privacy rights of data subjects. The legal analysis is centralised on the EU personal data protection regime because it is a microcosm of development in general data protection law, which is widely accepted as a global persuasive precedent on the regulation of transnational commercial use of personal data.

Keywords: Data protection; Personal Data; Data Protection in Sri Lanka; GDPR; EU

Introduction

The digital economy and its normalisation since the latter half of the 20th century, have thrown conventional economics and law into an existential crisis by contesting established notions of value-based transactions. Though

the digital economy has progressively intertwined with offline physical economic activities to achieve a state of co-existence, there are obvious lacunae in systematisation and regulation. An area with such gaps is the global commercial processing in personal data, of digital economy users or consumers (data subjects). There are two main points of consensus on the commercial use of personal data, which is noted from the onset for a productive discussion on the subject. The first point is that trade in data is essential, in a reality where every breathing moment of an individual with the technical means to access the internet, is touched or even governed by the digital economy. The second point of consensus is, commercialisation of user data should be regulated, because laissez faire trade in such data has negative externalities. Therefore, the pressing question is not whether user data should be commodified because the digital economy would cease to exist without the commercial use in personal data. It is whether suitable systems and regulatory frameworks exist to allow for an lawful commercial use of personal data without unduly hindering its free flow. Hence, the central concern is one of appropriate regulation and the balancing between two competing rights, namely, the freedom to commercially utilise user data in the digital economy, and the protection of the right to privacy and protection from unlawful processing of personal data of the consumer/user.

This is the contentious question which the essay attempts to answer, through a discussion on the legal implications of commercial use of personal data. To this end, the essay will first examine the existing legal systems on commercially processing personal data with specific attention to the European Union (EU) General Data Protection Regulation (GDPR) of 2016[1] and the associated case law. The aim of such an examination is to map the present approach to protectionism in the law. Next the essay will discuss three concerns on the present protectionist trajectory of the law, and its impact on the dual role of the law in the digital economy, i.e. as a facilitator of lawful commercial use of personal data and a guardian of privacy rights of data subjects. The aforementioned legal analysis is centralised on the EU personal data protection regime, because it is a microcosm of development in general data protection law, which is widely accepted as a global persuasive precedent on the regulation of transnational commercial use of personal data.

The EU Regulatory Framework: A Snapshot of the Legal Dilemma of Data Protectionism

The commercialisation and cross border commercial use of personal data takes place through every search on Google, online purchase on Ali Baba, share on Facebook and download of Microsoft Office. This sentence alone highlights four key facets

[1] Regulation (Eu) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/33.

regarding the commercialisation of personal data. The first facet is the speed of cross border exchange of user data. Unlike trade in physical goods, which require both time and manual systems, most commercial transactions on user data are completed instantaneously. The second facet is the liquidity and free flowing nature of user data which enables its commercialisation. This is aptly captured by John Perry Barlow when he characterised data as a "-highly liquid-pattern of ones and zeros"[2]. The third facet is a presupposition of ownership over the data by the data subject. Stepanov observes that though the economic value of data is widely accepted, the legal question on ownership of data is yet to be solved[3]. The fourth facet is the concentration of data control on a handful of commercial digital service providers due to the essentiality of the services supplied by these conglomerates. Sands (2017) notes that the infamous American tech giants are able to retain their market leadership due to their capacity to access "vast amounts of data from their users/customers and employ them with their algorithms"[4]. These four facets are amongst many other unique characteristics of personal data, which are transacted globally on a commercial scale. This section will provide a critical overview of the European regulatory framework on the commercial processing of data, as a brief case study on the legal implications of the expanding international commercial use of such user data.

The EU user data protection regime is composed of codified regulations and rulings of the Court of Justice of the European Union (CJEU) on the cases brought before it. In the case of the former, the General Data Protection Regulation (GDPR) of 2016 which succeeded the Data Protection Directive (DPD) of 1995[5], sets out the framework for the commercial use of personal data and privacy of data subjects within the EU and the European Economic Area (EEA). Since the essay focuses on the legal implications of commercial (ergo profitable) use of personal data, a preliminary question is whether such a use of data falls within the ambit of the GDPR, as a regulation which oversees the general processing of personal data? Article 4(2) of the GDPR provides a wide definition for the term 'processing', as "any operation or set of operations" carried out on personal data either manually or through automation, which includes a spectrum of actions ranging from collection to destruction[6]. This exhaustive list of operations also includes

[2] Barlow, J. P., 'The Economy of Ideas: Selling Wine without Bottles on the Global Net' (2019) 18 *Duke Law & Technology Review* 8, 11.

3 Stepanov, I., 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (2019) 34(1) *International Review of Law, Computers & Technology* https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621 accessed 23 March 2021, 65.

[4] Sands, M., 'Customer Data Is The Secret To Silicon Valley's Success' *Forbes* (USA 29 November 2017) < https://www.forbes.com/sites/mikesands1/2017/11/29/customer-data-is-the-secret-to-silicon-valleys-success/#135386886c3b> accessed 26 March 2021.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[6] General Data Protection Regulation (n 1) 33.

the word 'use'. Whether or not such a processing (use) of personal data can be commercial is implicitly mentioned in the Regulation and can be interpreted through the reading of two provisions. Firstly, the definitions provided in Article 4 recognises that any party to the processing of personal data can be "a natural or legal person"[7]. This identification proves that the Regulation applies to profit seeking commercial entities. Secondly, Preamble paragraph 18 states that for the Regulation to apply the processing must be connected to either a "professional or commercial activity" [8]. Hence, commercial processing (including use) of personal data by profit seeking entities is within the jurisdictional scope of the Regulation.

Before further delineating the EU legal framework on the commercial processing of user data, it is essential to contextualise the framework's approach to data protectionism. Preamble paragraph 01 [9] of the GDPR recognises that "natural persons" have a fundamental right to be protected from personal data processing under two statutes, namely, Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') [10] and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)[11]. In light of this fundamental right, Article 1(1) notes that the sole objective of the GDPR (similar to that of DPD 1995) is to set out the rules "relating to the protection of natural persons with regard to the processing of personal data" and "the free movement of personal data"[12].

However, Article 1(3) states that the free flow of user data within the Union will not be hindered by the right to be protected from processing of personal data [13]. These two provisions reflect an attempt to strike a balance between economic progress and human rights, which is further resonated in Preamble paragraph 04 of the GDPR which states that "the processing of personal data should be designed to serve mankind"[14]. The Article further states that the right of data subjects to be protected from personal data processing, is not an absolute right but one that has to be viewed in relation to its social function (benefit) and other fundamental rights, through a lens of proportionality[15].

A collective reading of these provisions confirms three aspects of the EU's principle on data protectionism. The first aspect is that the GDPR prioritises the conversion of the EU into a free trade digital market for user data. Yet the same commitment of facilitation would not apply to the commercial flow of user data outside of the EEA, possibly because of differences in standards of data protectionism within and outside the Association. Secondly, the right of a data subject to be protected from personal data processing, is of equal importance as the free flow of such data in the digital economy. Thirdly, this fundamental right must be guaranteed unless

[7] Ibid.
[8] General Data Protection Regulation (n 1) 3.
[9] General Data Protection Regulation (n 1) 1.
[10] Charter of Fundamental Rights of The European Union [2000] C 364/01 art 8(1)
[11] The Treaty on the Functioning of the European Union [2012] C 326/47 art 16(1)
[12] General Data Protection Regulation (n 1) 32.
[13] Ibid.
[14] General Data Protection Regulation (n 1) 3.
[15] Ibid.

such a guarantee has undue social costs and harms the protection of other basic human rights. Therefore, on a first level of analysis, the GDPR attempts to diplomatically capture and provide a viable solution to the legal dilemma of user data protectionism i.e. the tension between unhindered commercial use of personal data as the lifeline of the digital economy, and the right to be protected from the processing of personal data. On a second level of analysis, the viable solution proposed by the GDPR is a homogenous, right centric framework of necessary data processing which aims to facilitate commercial use of personal data only to the extent that it is necessary.

A brief breakdown of the GDPR provisions and associated case law, on the transfer and commercial transactions of user data, will further prove the aforementioned analysis on the EU's homogenous framework of necessary data processing. Article 3(1) of the GDPR confirms that the Regulation caters to the commercial processing of personal data at two stratas [16]. The first strata is the commercial processing of user data amongst Member States of the EEA, and the second strata is that between Member States of the EEA and other countries outside of the Association. In terms of the internal commercial processing of user data, Article 5 lays down several important principles[17]. In a nutshell, the Article requires Member States to collect necessary data for specific purposes and process personal data lawfully, fairly and transparently whilst maintaining accurate records of such user data[18]. Here the legal standard to be met by Member States of the EEA in the commercial use of personal data is one of necessity, where what is necessary is what is lawful. Hence it can be argued that the GDPR protects data subjects within the EEA from unnecessary processing of user data.

This raises the question of what necessary processing of data in commercial and professional terms is. Article 6(1)(b) to (f) of the GDPR sets out an exhaustive list of what constitutes necessary processing of personal data by Member States of the EEA[19]. The terminology of this list is purposefully broad to incorporate a myriad of situations ranging from contractual performance to the "legitimate interests" of parties to a commercial processing of data[20]. Article 06 further deems that where the commercial processing of data falls within one of these circumstances of necessity, such processing is lawful[21]. Another important dimension to legal processing of data is presented in Article 6(1)(a), which states that where the data subject has provided consent for the commercial processing of their data, then such a processing is lawful[22]. This provision must be read together with Article 7, which stipulates that the data controller must obtain provable consent from the data subject where it is required for the processing of their personal data (Article 7(1))[23]. Consent must be obtained through a "distinguishable" form in cases where the consent is written (Article 7(2)) and the data

[16] General Data Protection Regulation (n 1) 32.
[17] General Data Protection Regulation (n 1) 35-36.
[18] Ibid.
[19] General Data Protection Regulation (n 1) 36-37.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] General Data Protection Regulation (n 1) 37.

subject has the right to withdraw such consent at any time (Article 7(3))[24]. It is noteworthy that Article 6(1)(a) on the consent of the data subject, is included as one of the six contexts in which the processing of personal data is lawful. This contests the notion that user data is the 'personal property' of the data subject within the EEA and as such it can be used only with the consent of the owner as other personal properties. Stepanov argues that the GDPR read together with the Charter, recognises personal data as "rights, subject to special consideration over which no property rights could be exercised"[25]. Therefore, the GDPR views the processing of personal data from a fundamental rights angle as opposed to an intellectual property angle.

It is apparent from the above analysis, that the GDPR's legal approach to internal commercial processing of personal data is a homogenous, rights centric, personal data protection framework, based on necessary processing within the EEA; achieved through the standardisation of national laws. However, in the case of the second strata of commercial processing of personal data, taking place outside of the EEA in a third (non-EEA) country, the GDPR sets out three separate frameworks for data exportation. Bu-Pasha argues that such frameworks extend the territorial scope of the Regulation beyond the EEA and thereby provides the GDPR with extra territorial jurisdiction, making it an international data protection law[26]. The case of *Bodil Lindqvist*[27] examined the term 'transfer of data to a third country' and held in favour of the UK Government's submission that for such a transfer to take place personal data must be "directly transferred"[28] from one party to another, thereby confirming the necessity of intention to transfer. Therefore, there was a distinction drawn between mere accessibility of personal data by a party outside the EEA and the actual transfer of data to such a party.

In light of this legal interpretation of the CJEU, Murray observes that Chapter 05 (Articles 44-50) of the GDPR presents three main data exportation (transfer) frameworks[29]. The first is the 'Adequacy Decision Framework' contained in Article 45 of the GDPR, where it is stated that transfer of personal data to a non-EEA country is possible without "specific authorisation" if the country under consideration "ensures an adequate level of protection" for the transferred data[30]. Article 45(2) provides an expansive list of elements which should be considered by the European Commission (EC), when assessing the adequacy in data protection of a non-EEA data recipient country[31]. Murray notes that practically this means extensive negotiations with the EC to obtain a full or partial

[24] Ibid.
[25] Stepanov (n 3) 68
[26] Bu-Pasha, S., 'Cross-border issues under EU data protection law with regards to personal data protection' (2017) 26(3) *Information and Communications Technology Law* https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740 accessed 30 March 2021, 214.
[27] Case C-101/01 *Criminal Proceedings Against Bodil Lindqvist* [2003] ECR I-12971.
[28] Ibid 27.
[29] Murray, A., *Information Technology Law: The Law and Society*, (4th edn, Oxford University Press 2019) 624
[30] General Data Protection Regulation (n 1) 60-61.
[31] Ibid.

adequacy decision[32]. It can be observed that the list of elements for adequacy, sets a high benchmark which can only be met by countries with a similar data protectionist philosophy as the EU and possess the necessary systems to implement that philosophy. However, the controversial adequacy decisions on personal data transfer between the EU and the USA, which was contested in the *Schrems* Cases (discussed in the next section) is proof that the approval process is not purely a legal one.

Murray states that a country which does not obtain an adequacy decision, may rely on the 'Appropriate Safeguards Framework' provided in Article 46 of the GDPR[33]. He further notes that Article 46(2) provides an exhaustive list of measures amounting to appropriate safeguards, to ensure that both the EEA data controller and the recipient of data outside the Association, are legally bound to protect the data subjects' rights on processing of personal data[34]. There are two common forms of appropriate safeguards provided for from Article 46(2)(b)-(d), namely, Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs)[35]. Murray defines BCRs as "internal codes of conduct" which manage controlled transfer of personal data from EEA entities of a multinational group, to its non-EEA entities[36]. The legally binding nature of such BCRs and their capacity to confer enforceable rights to data subjects, along with the requirements of such Rules, are provided in Article 47 of the GDPR[37]. The Article further provides that a BCR must be approved by an EEA Supervisory Authority of a Member Country in which a company of the multinational group is based[38].

Where a conglomerate cannot apply BCRs or are transferring data outside of the group, to third party entities not based in the EEA, it (data exporter) may incorporate SCCs in agreements with such external entities (data importer). Murray notes that in the present regime, SCCs refer to four standard clauses introduced in the DPD of 1995, which must be adopted without amendment, to provide enforceable rights to the data subjects.[39] The CJEU judgement in *Schrems II* case enforced stricter requirements for SCCs, by requiring data controllers and exporters relying on such clauses to provide a level of protection to the data subjects which is "essentially equivalent" to that guaranteed by the GDPR and the Charter[40]. Where necessary, "additional measures" of protection must also be taken by the parties to compensate for lacunae in the data protection law of recipient countries outside the EEA[41].

The third data exportation framework is 'Derogations for Specific Situations', contained in Article 49 of the GDPR 2016[42]. This Article provides an exhaustive list of exceptional circumstances in which data can be exported outside of the EEA, where there is no adequacy decision and an absence of

[32] Murray (n 29) 626
[33] Murray (n 29) 627
[34] Ibid
[35] General Data Protection Regulation (n 1) 62.
[36] Murray (n 29) 627.
[37] General Data Protection Regulation (n 1) 62-63.
[38] Ibid.
[39] Murray (n 29) 627.
[40] C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* [2020]
[41] Ibid.
[42] General Data Protection Regulation (n 1) 64-65.

appropriate safeguards. Attention must be drawn to the second subparagraph of Article 49(1) which provides a last resort scenario for data exportation outside of the EEA. It states that where relevant authorisation has not been obtained under any of the three frameworks, a data controller may only export personal data outside the Association under limited circumstances; such as non-repetitive transfers and transfers in pursuant of legitimate interests of the data controller, after having assessed the need for "suitable safeguards" for personal data protection and having provided them[43]. Therefore, where data exportation takes place outside of the three frameworks, complete onus falls on part of the data controller to ensure the apt protection of the transferred personal data.

It is apparent from the above analysis on the three frameworks for data exportation outside the EEA, that the legal approach of the EU for transfer of data to third countries is one of adequate protectionism through standardisation. This is different from the legal approach for commercial processing of personal data within the internal market, which is a homogenous, human rights centric framework based on necessary processing. The data exportation frameworks allow for greater flexibility than the internal processing framework, possibly in consideration of varying standards in data protectionism outside the EEA. Though such flexibility fosters greater exportation of data, it is being challenged by several activist groups under the claim of inadequate assurance of data subject rights to privacy and protection from processing of personal data.

Politicisation, Riskification and Complication of the Law

The United Nations Conference on Trade and Development (UNCTAD) data confirms that 66% of countries in the world possess some form of data protection and privacy legislation[44]. Not only are such legislation based on different approaches to data protectionism, they are also living frameworks which change frequently. The EU framework for regulating the commercial processing of personal data is so dynamic, that the analysis in this essay will be rendered obsolete in a few months. However, the overview of this legal framework provided in the preceding section, prompts critical thought on the present protectionist direction of the law and its impact on the dual responsibility of the law in the digital economy, as a facilitator of lawful commercial use of personal data and a protector of data subject rights. Hence, this section will focus on the need to remedy three concerns of the EU's legal system on the commercial processing of personal data, which negatively impacts its ability to promote cross border data flow whilst providing needed protection to data subjects.

The first concern is the politicisation of the data exportation authorisation processes set out by the GDPR. This is evident from the controversial adequacy decision for data transfer between the EU and USA which was

[43] Ibid.

[44] United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide' < https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 10 April 2021

successfully contested in two accounts by the *Schrems* Cases. Movius and Krup (2009) notes that the EU and USA have vastly different approaches to data protectionism, because it is heavily regulated in the former whilst the latter adopts a "industry self-regulation and reactive legislation" approach[45]. Despite this difference, USA adopted the Safe Harbour Agreement in 2000 which allowed for a complete adequacy decision and consequential commercial transfer of personal data. The Snowden revelations on the Prism programme prompted the CJEU hearing *Maximillian Schrems v Data Protection Commissioner*[46]. The Court ruled that the EC Adequacy Decision 2000/520 is invalid, as the existing framework for data protection in the USA is inadequate to sustain Article 01 of the Decision, which states that the Safe Harbour Agreement together with supportive implementation frameworks, "are considered to ensure an adequate level of protection for personal data transferred"[47]. This Agreement was replaced by the Privacy Shield Agreement which introduced two remedies to issues identified by the CJEU in its predecessor, namely, the EU–US Privacy Shield Ombudsperson and greater transparency on the access of transferred personal data by the US public authorities.

The CJEU in the *Schrems II* case declared the Privacy Shield Agreement invalid, on account of "disproportionate interference with the rights to protection of data and privacy" [48] through programmes such as PRISM and UPSTREAM. There is no intermediate provision in place for data exportation from the EU to USA, and Wojciech Wiewiorowski who is the European Data Protection Supervisor, informed Reuters that a new transatlantic data transfer pact would not be introduced anytime soon[49]. Reuteurs further reported that the lack of a legal data exportation mechanism, has left more than 5000 companies who signed the Privacy Shield Agreement vulnerable to business disruption and privacy law suits. The Schrems Cases reveal that authorisation decisions for the cross border commercial use of data, is as much a closed-door political decision as a legal one. Such a politicisation erodes the efficacy of the EU legal framework to prevent the undue infringement on the rights of data subjects, and transforms the framework into a reactive one which responds to legal challenges by pro-protectionist movements.

The second concern is what Spina recognises as the progressive "Riskification" of the EU data protection framework[50]. This is the shift of the legal approach to data protectionism from a limited legal regulation

45 Movius, L. B., and Krup, N., 'U.S. and EU Privacy Policy: Comparison of Regulatory Approaches' (2009) 3 *International Journal of Communication*, 169

46 Case C-362/14. *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

47 Ibid

48 Schrems II (n 40)

49 Foo Yun Chee, 'New EU-U.S. data transfer pact? Not any time soon, says EU privacy watchdog' (Online 4 December 2020) < https://www.reuters.com/article/eu-privacy-idUSKBN28E2JQ> accessed 15 April 2021

50 Spina A., 'A Regulatory Mariage de Figaro: Rica Ethics' (2017) 8 European Journal of Risk Regulation 88

model to one based on "enforced self-regulation for managing technological innovation in uncertain scenarios"[51]. Spina further argues that such self-regulation will take place through varying governance measures, ranging from data protection impact assessments to the introduction of default data protection mechanisms into the commercial processing of user data [52]. Macenaite supports Spina's argument by noting that the GDPR "relies heaving on risk" and has introduced a considerable number of new provisions around risk regulation[53]. Whilst risk regulation is one avenue for bridging the gap created by the disproportionate development of technology in comparison to the parallel development in the law on technology, heavy reliance on sectoral self-regulation (as seen in the USA) is counterproductive as data controllers who benefit by big data analysis, decide the nature and extent of the commercial processing of user data.

The third concern is the complexity and ambiguity of the composition and impact of the GDPR. Cool notes in an article to The New York Times, that the "staggering complexity" of the GDPR; which received 4000 amendment proposals since a draft was submitted by the European Parliament, is attributable to differences in national values on data collection [54]. Undoubtedly, this creates practical costs for businesses, as they must invest in expensive internal frameworks and additional processes for data protection. Though the EU legal framework cannot be simplified due to the versatile nature of personal data and growth in cross border commercial processing, greater clarity can be achieved through the streamlining of such legal systems and via greater investment on support systems provided to commercial data controllers.

Conclusion

The key legal implication of the commercial use of personal data, is the dual role served by the law as a facilitator of lawful cross border transfer of such data within the digital economy, and as a champion of the right to privacy and protection from unlawful processing of user data. On the surface these two roles may appear contradictory to one another, as data protectionism hinders the freedom of user data markets. However, for the growth and sustenance of transnational commercial use of personal data, data subjects (consumers and users) must have trust in firms operating as data controllers and confidence in the legal regulatory framework on data protectionism. Therefore, this dual role of the law is essential for the existence of safe international user data markets and increased commercial processing of such data for economic activities.

[51] Ibid.
[52] Ibid.
[53] Macenaite, M., 'The "Riskification" of European Data Protection Law through a two-fold Shift' (2017) https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/riskification-of-european-data-protection-law-through-a-twofold-shift/A91B3E7A0A1EF4E6889FD54F941D83D3 accessed 24 April 2021
[54] Cool, A., 'Europe's Data Protection Law Is a Big, Confusing Mess' (USA 15 May 2018) < https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html> accessed 4 April 2021.

In order to maintain this tricky balancing act of the law, national and regional legislatures adopt varying legal frameworks based on, subjective philosophies to data regulation and existing local privacy rights cultures. Though local user data control mechanisms are a positive step towards safe commercial use of personal data, they obstruct the global flow of data due to the varying regulations requirements and often bureaucratic processes imposed. The difference in the EU's legal approach to internal market, commercial processing of personal data and the data exportation outside of the EEA, which are is set out in the GDPR, is proof of the difficulties that arise out of the lack of uniformity in global data regulation. This is why an international convention on the control of commercial use of personal data, which is proposed by academics and practitioners alike, is a viable option. However, such a international law framework must be one based on a philosophy of necessary protectionism, as opposed to the present human rights culture of the international political arena.

References

Barlow J P, 'The Economy of Ideas: Selling Wine without Bottles on the Global Net' (2019) 18 *Duke Law & Technology Revie*w 8, 11

Bu-Pasha S, 'Cross-border issues under EU data protection law with regards to personal data protection' (2017) 26(3) *Information and Communications Technology Law* < https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740> accessed 30 March 2021, 214.

C-101/01 *Criminal Proceedings Against Bodil Lindqvist* [2003] ECR I-12971

C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* [2020]

Case C-362/14. *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

Chee F Y, 'New EU-U.S. data transfer pact? Not any time soon, says EU privacy watchdog' (Online 4 December 2020) < https://www.reuters.com/article/eu-privacy-idUSKBN28E2JQ> accessed 15 April 2021

Cool A, 'Europe's Data Protection Law Is a Big, Confusing Mess' (USA 15 May 2018) <https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html> accessed 4 April 2021

Macenaite M, 'The "Riskification" of European Data Protection Law through a two-fold Shift' (2017) < https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/riskification-of-european-data-protection-law-through-a-twofold-shift/A91B3E7A0A1EF4E6889FD54F941D83D3> accessed 24 April 2021

Movius L B and Krup N, 'U.S. and EU Privacy Policy: Comparison of Regulatory Approaches' (2009) 3 *International Journal of Communication*, 169

Murray A, *Information Technology Law: The Law and Society*, (4th edn, Oxford University Press 2019) 624

Regulation (Eu) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/33

Spina A, 'A Regulatory Mariage de Figaro: Rica Ethics' (2017) 8 *European Journal of Risk Regulation* 88

Stepanov I, 'Introducing a property right over data in the EU: the data producer's right – an evaluation' (2019) 34(1) *International Review of Law, Computers & Technology* <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621> accessed 23 March 2021, 65

United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide' < https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 10 April 2021