Towards an Optimal Regulatory Strategy for Data Protection: Insights from Law and Economics

by **Donatas Murauskas and Raminta Matulytė ***

Abstract: In this paper, we examine data protection regulation from the standpoint of Law & Economics. Specifically, we analyze the advantages and disadvantages of the two distinct data protection regulation frameworks in the EU and the US. We compare these regulatory frameworks based on the criteria set by S. Shavell in his seminal work "Liability for Harm Versus Regulation of Safety". We utilize Shavell's model to compare the *ex ante* regulatory approach to data protection in the EU with the *ex post* liability approach of the US. This comparative analysis helps us explore whether the focus in the field of data protection should be on proactive (*ex-ante*) regulation or reactive (*ex-post*) liability. We find difficulties in comparing the regulatory frameworks, considering the dominant conceptual framework of human rights in the data protection field. However, the comparison provides valuable efficiency-based arguments on ways to optimize both regulatory frameworks.

Keywords: Data Protection Regulation; GDPR; Law & Economics; Ex-ante Regulation; Ex-post Liability

Recommended citation: Donatas Murauskas and Raminta Matulytė, Towards an Optimal Regulatory Strategy for Data Protection: Insights from Law and Economics, 15 (2024) JIPITEC 269 para 1

A. Introduction

1 The dawn of the internet promised the loss of control of our privacy – "You have zero privacy anyway," according to the CEO of Sun Microsystems in 1999.[1] Yet, political and civil mobilisation has tried to 'get our privacy back'[2]. The emergence of AI-based tools focuses discussions on the privacy price paid to receive AI-based services. The European supervisory authorities target tech-giant Meta for non-compliant data protection practices, including unjustified data transfers to the US.[3] How can we reconcile the demand for privacy in the

* Donatas Murauskas is Associate Professor at Vilnius University Law Faculty, donatas.murauskas@tf.vu.lt. Raminta Matulytė is PhD student at Mykolas Romeris University, raminta.matulyte@stud.mruni.eu.

1 Polly Sprenger, 'Sun On Privacy: "Get over It"' (Wired, 26 January 1999) < https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> accessed 19 December 2023.

2 Timothy Garton Ash, *Free Speech: Ten Principles for a Connected World* (Yale University Press; Reprint edition, 2017).

3 European Data Protection Board, '1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision' (EDPB, 22 May 2023) <https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en accessed> 14 August 2024.

age of AI with the growing need for data-driven services and international data flows?

2 The normative analysis sometimes ignores one of the crucial features of 'good' regulation: its efficiency.[4] In this paper, we do not want to analyse the advantages and disadvantages of data protection regulatory frameworks by looking at the wording of norms of legal acts. On the contrary, we aim to consider whether regulators should rely on economic efficiency in deciding which data protection regulatory approach is more preferred by society. Using Steven Shavell's economic analysis of law, which contrasts *ex-ante* regulation with *ex-post* liability, we assess the efficiency of the US and the European regulatory approach in protecting data rights.

3 First, we examine the concept of economic analysis of law and what models may be useful for lawmakers to measure the economic efficiency of planned regulation. Then we provide introductory insights to privacy economics, which is important considering our goal to discuss particular human rights (i. e. the right to private life and the right to data protection) in the context of efficiency (i. e. economic domain). Third, we chose the data protection regulatory frameworks in the EU and the US to show how economic analysis of law may be applied in practice to determine economic efficiency and to compare the chosen regulatory approaches in different jurisdictions. Finally, we discuss recent developments in the field of data protection that show the search for a balance between economic efficiency and the need to set data protection standards while maintaining constitutional national security and data privacy safeguards.

B. Economic Analysis of Law and Its Applicability to Emerging Regulatory Fields

4 Among other significant ideas in the realm of law and economics, scholars develop models to determine the social costs of selected regulatory approaches. In the field of social preference for *ex-ante* regulation and *ex-post* liability, S. Shavell's model depicted in his seminal work "Liability for Harm Versus Regulation of Safety"[5] is the most suitable to measure the economic efficiency of chosen data protection regulation frameworks.

5 Shavell analyses why society prefers to strictly regulate some fields or leave others unregulated, ensuring tort liability. He describes that tort liability (*ex-post* liability) is private in nature and works not by social command, but by the effect of legal damage actions that may be brought once harm occurs. Standards, prohibitions, and other types of safety regulation (*ex-ante* regulation), on the other hand, are public in nature and modify behaviour immediately through requirements imposed before, or at least independently, of the occurrence of harm.[6]

6 Are there any factors implying a preference for one or the other model? Shavell indicates four determinants of the relative desirability of *ex-post* liability and *ex-ante* regulation. According to Shavell, to identify and assess the factors determining the social preference for liability and regulation, one should set out a measure of social welfare. He assumes that this measure equals the benefits that parties derive from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control. The formal issue is to employ control mechanisms to maximise the welfare measure. Shavell outlines four factors that impact the solution to this issue (Image 1).[7]

4 Robert Baldwin, Martin Cave, Martin Lodge, 'Understanding Regulation. Theory, strategy, and Practice' (Oxford University Press; 2nd edition, 2012, 31.

5 Steven Shavell, 'Liability for Harm versus Regulation of Safety' (1984) 13(2) The Journal of Legal Studies 357.

6 Ibid 357.

7 Ibid 358-359.

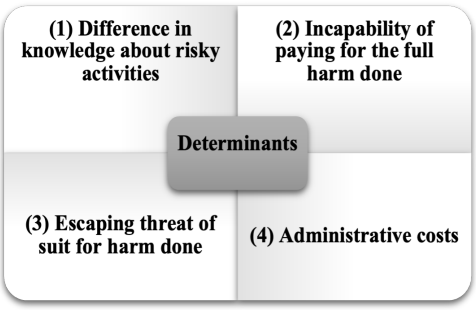

Image 1. Shavell's Determinants Defining Social Preference for *Ex-Ante* Regulation and *Ex-Post* Liability[8]

7 Shavell considers that giving the regulator the power of control when private parties have complete information about risky behaviour about which the regulator has little knowledge will lead to a high probability of regulation errors. The regulator's standard will be excessively strict if it overestimates (1) **the possibility of harm caused by risky activity**. In the opposite case, if the regulator makes contrary errors, its requirements may be overly lenient.[9] Shavell suggests that because the private parties are the ones who are engaged in and benefit from their actions, they should have an inherent advantage in knowledge. Obtaining such information for a regulator would usually need near constant surveillance of parties' conduct, which would be practically impossible. However, in some specific fields, information about risks may not be evident and will take effort or particular competence to analyse, which the regulator may supply in these situations by dedicating social resources to the task.[10]

8 Next, (2) **the capacity to pay for the harm caused** would be irrelevant under regulation, assuming that parties would take steps to reduce risk as a precondition for engaging in their activities; therefore, any harm will be less likely to occur.[11]

9 (3) **The possibility of avoiding a lawsuit** for the damage done might be another important factor. First, a defendant may avoid *ex-post* liability because the harms caused are widely dispersed, making it difficult for any single victim to pursue legal action. Second, there could be a significant period of time before any harm occurs; therefore, it could be impossible to gather the evidence needed for a successful suit. Third, it is challenging to assign guilt for harm to those actually accountable for it, as actual harm often may not be directly linked to certain actors.[12]

10 Finally, (4) **the tort system's costs** must be widely defined to cover private parties' time, effort, legal fees, and public expenses such as trial costs. Similarly, administrative costs of regulation encompass expenses of maintaining the regulatory establishment and the private costs of compliance. In this scenario, liability has the benefit because, in such cases, most administrative expenses are incurred only if harm occurs, while administrative costs are always incurred under regulation.[13]

11 In conclusion, administrative expenses and difference in knowledge, according to Shavell, favour social preference for *ex-post* liability. The inability to pay for the harm done and the opportunity to avoid lawsuits, on the other hand, support *ex-ante* regulation. Shavell argues that these two approaches should not be seen as mutually exclusive. Instead, a comprehensive legal solution to any social problem should include *ex-post* liability and *ex-ante* regulation, with the balance reflecting the significance of the determinants.[14] In this article, we consider whether Shavell's model can suggest the most efficient methods for balancing regulatory approaches, especially in the data protection field.

C. The Economics of Privacy

12 Before exploring a comparison of different data protection regulatory frameworks, it is imperative to first address the challenge of discussing human rights – such as the right to private life and the right to data protection—within the context of economic considerations. This interplay often raises complex

8 Compiled by the authors based on Shavell (n 5).

9 Shavell (n 5) 359.

10 Ibid 360.

11 Ibid 360-361.

12 Ibid 363.

13 Ibid 363-364.

14 bid 365.

questions about the monetary value that may be ascribed to human rights.

13 The discussion of rational individual decision-making can be situated within the context of human rights. While human rights involve inherent trade-offs between individual autonomy and public needs, their monetary value is inherently challenging to quantify. Human rights are fundamental, universal, and inviolable, representing intrinsic values grounded in respect for human autonomy and dignity. Privacy and data protection, in particular, are enshrined as fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU. This raises the question: what are the conceptual foundations for examining human rights within the framework of economic analysis of law?

14 Similar to other goods and services, individuals hold preferences and make assessments regarding human rights. While it is impossible to objectify human rights in purely monetary terms, this does not preclude the possibility of determining their relative value. Human rights safeguard specific aspects of human autonomy and can be viewed as both final and instrumental goods.[15]

15 Economic studies imply that no definitive conclusions can be made about whether there are actual costs / benefits of individuals or societal privacy protection.[16] If we imagine data protection rights as property rights, with personal data as an object of transactions, it enables a more economically driven approach to assessing data protection. This perspective allows for the examination of trade-offs between maintaining privacy and sharing data with service providers.

16 If companies are collecting data of private individuals, they can make their goods and services better aligned to the preferences of these individuals. In this context, collected data that includes individual attributes might be regarded as business asset "that can be used to target services or offers, provide relevant advertising, or be traded with other parties."[17] Individuals may incur various costs as a result of sharing excessive amounts of data. For instance, reputational damage could occur due to the loss of sensitive information. Additionally, individuals may suffer financial losses stemming from information asymmetry, where a service provider, leveraging collected data, charges personalised prices aligned with the individual's aggregated preferences. Acquisti et al. also provide examples of positive externalities in cases of data sharing such as personalized services and discounts.[18] They also underline the specific nature of information privacy as maintaining characteristics of public and private goods.[19]

17 Privacy, like other human rights, is sometimes conceptualized as a public good due to its characteristics of non-excludability and non-rivalry. These rights are non-rivalrous because one person's enjoyment of them does not diminish the ability of others to enjoy them as well. However, they are only partially non-excludable, as access to these rights can be restricted or obstructed by legal or social discrimination or a lack of economic resources.[20]

18 Individuals maintain specific preferences regarding their privacy and behavioural constraints such as bounded rationality.[21] Farell underlines that "there is also a dysfunctional equilibrium in which few consumers devote much attention to disclosures, disclosures are vague, noncommittal, or even if explicit, mostly ignored; and the privacy policies chosen are

15 "[H]uman rights can be final goods (that is, goals to be achieved for themselves) or intermediate goods (that is, means to realize other goods or rights)." (Georges Enderle, 'Human Rights as Public Goods'. In: *Corporate Responsibility for Wealth Creation and Human Rights* (Cambridge University Press, 2021 152). Farrel suggests that privacy has elements of both (Joseph Farrell J, 'Can Privacy Be Just Another Good?' 10 Journal on Telecommunications and High Technology Law, 2012 252).

16 Alessandro Acquisti; Curtis Taylor; Liad Wagman, 'The Economics of Privacy', 54(2) Journal of Economic Literature 2016, 444.

17 Ibid 444.

18 Ibid 445.

19 Ibid 446.

20 Enderle, (n 15) 151–152.

21 Wolfgang Kerber, 'Digital markets, data and privacy: competition law, consumer Law and data protection', 11(11) *Journal of Intelectual Property Law & Practice*, 2016 849.

inefficiently non-protective".[22]

19 Therefore, while a traditional law and economics approach would seek the economically efficient (i.e., welfare-maximising) specifications of these property rights, the normative choice to regard privacy as a fundamental individual right might result in stronger protection of privacy and personal data than what would be justified by an economic efficiency standard.[23]

20 Determining the economic value of data or privacy remains a challenging task. Our attempt to apply the Shavell framework to data protection regulation inevitably raises questions about the appropriate conceptual framework for data protection. While we endeavor to treat data protection as an asset within the law and economics paradigm, this approach offers limited contributions to the broader and more complex discourse on the value of data and privacy within the context of fundamental rights. This is the trade-off of maintaining a consistent yet narrow focus—restricting the analysis to a single dominant framework, namely law and economics. With this limitation in mind, we now turn to the search for a more efficient standard in data protection.

I. Example of Data Protection Regulation Models

21 Almost no technology-driven field nowadays can operate without at least some kind of relation to the processing of personal data. Over the last few decades, rapid technological development has resulted in the need to search for options for data protection regulation. However, with the introduction of different data protection standards, discussions on which standard to follow or how to improve existing ones are as relevant as ever.

22 The General Data Protection Regulation (GDPR)[24] is the EU data protection standard that sets numerous obligations to companies and a list of rights of individuals. The opposite of such comprehensive and strict regulation enshrined in one legal act is the US data protection framework, that is fragmentary and does not foresee obligations for organisations or rights to individuals in every case concerning data processing. These different jurisdictional approaches are the subject of our further analysis. In the table below (Table 1), we summarised the main features of data protection regulation models in the EU and US.

22 Farell, (n 15) 259.

23 Kerber, (n. 21) 864.

24 Regulation of the European Parliament and of the Council 2016/679 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 [2016] OJ L 119/1.

Jurisdiction	Legislation	Centre of the regulatory framework	Supervisory authority	Enforcement
EU	One comprehensive personal data protection regulation - GDPR	A data subject who is granted a list of certain rights	A well-established network of supervisory authorities in the EU member states	Administrative fines for infringement up to 20 million euros or 4 % of the annual turnover GDPR allows individuals to seek damages
US	Sectoral federal legislation; comprehensive legislation adopted on a state-level	Business freedom and its right to choose the best way to protect individuals' data by way of contractual obligations	No clearly designated supervisory authority on a federal level (Federal Trade Commission operating as *de facto* authority)	No unified system of administrative fines Allowed possibilities to bring claims before courts regarding privacy infringements

Table 1. Main features of the EU and the US data protection regulation frameworks

23 While the EU and US have different approaches to data protection, both jurisdictions attempt to combine *ex-ante* regulation and *ex-post* liability in their data protection regulation models. We further analyse the social costs of the EU's and US's data protection regulation models and preference for either *ex-ante* regulation or *ex-post* liability based on the previously described Shavell's economic approach, by applying the four determinants that, according to Shavell, influence preference for *ex-ante* regulation and *ex-post* liability.

1. Difference in Knowledge about Risky Activities

24 We consider the data protection field to be a good example of how private parties and state institutions can have very different understandings, knowledge, and approaches towards personal data and the necessary level of protection. In his model Shavell refers to regulatory authorities, which in the data protection field should also include Supervisory Authorities.[25] Supervisory Authorities interpret the data protection legislation and can *de facto* expand or narrow down the data protection rules. Technological neutrality of the data protection laws results in their equal applicability to big-tech companies and organisations that process data in a non-complex manner. This presupposes that while it is not too difficult to have knowledge of basic operation principles and set standard rules for simple cases, this is not true if we talk about processing data using emerging tech-

25 Referring to Article 51(1) of the GDPR ("Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')").

nologies. The complicated technological solutions used for data processing may cause a significant difference in the information that companies and state actors possess. Additionally, the human rights lens taken by regulatory authorities could be considered a difference in knowledge because private parties in the data protection field often follow the approach that consumers choose to give up their data to receive services or purchase goods. Therefore, companies consider themselves the ones that should know better, how to efficiently serve their customers.

25 **Europe**. The GDPR is constructed as a technologically neutral legislation.[26] Hence, the abstract provisions apply to different actors operating in different business fields. The neutral nature of the GDPR causes Supervisory Authorities to possess different knowledge on the applicability of the GDPR depending on differences in data processing performed by various actors. Big-tech companies often process data in a complex way; for example, technical characteristics may not directly indicate whether particular data may be related to an identified or identifiable natural person in the way that is defined under Art. 4(1) of the GDPR (e.g., data logs, encrypted data). These technical characteristics may become an issue when Supervisory Authorities investigate organisations and apply GDPR principles to specific data processing operations. In such cases, the Supervisory Authority may lack expertise and resources to thoroughly analyse and understand the actual technical setting. This may result in fines that do not necessarily ensure the factual protection of personal data.

26 Another factor proving the differential knowledge is the asymmetry of the burden that lies with global corporations and small and medium enterprises. The latter, in most cases, are obliged to comply with requirements that are exactly similar to those imposed on the big companies. However, they often do not extensively process massive datasets or cause a significant threat to individuals. Such regulatory asymmetry may be considered what Shavell describes as "a chance of regulatory error", where the EU regulation overestimates the potential for harm in small and less intrusive data processing operations and sets too stringent data protection standards.

27 **The US.** The US model is based on the premise that private parties should generally enjoy an inherent advantage in knowledge of their risky activities. For a regulator to obtain the same information would often be practically impossible, especially when the information concerns complex technological solutions. The US approach corresponds with the fact that regulators usually possess less information than private parties in the data protection field. However, the fragmented sectoral regulation is an example of what Shavell describes as better knowledge possessed by the regulator due to the specifics of the field that require special protection. For example, children's privacy protection under the Children Online Privacy Protection Act[27] or health data protection under the Health Insurance Portability and Accountability Act[28] shall be considered areas where private parties do not enjoy the same knowledge as the regulator – the areas are so sensitive that the regulator is considered as a greater incentive to ensure data protection compliance due to the ease of ensuring a higher level of expertise in very specific fields. Following Shavell's notions in these areas, substantial regulation is not a coincidence but rather a need, both because liability alone would not adequately reduce risks and because the usual disadvantages of regulation are not as severe as in the tort context.

28 It is fair to state that the US model reflects the difference in knowledge about risky activities better than the EU model as it leaves most data protection-related decisions[29] to organisations and to liability, accordingly. The US fragmentary approach to federal regulation reflects specific fields that require a higher standard of protection and provides examples where the regulator possesses more knowledge than private parties. On the opposite note, with technological neutrality, the GDPR obliges Supervisory Authorities to possess more information than private parties on technological aspects to enforce the regulation. This often is impossible due to limited resources and expertise. At the same time, the GDPR

26 GDPR (n 24) recital §15.

27 Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (Pub. L. 105–277), 112 Stat. 2681-728.

28 Health Insurance Portability and Accountability Act of 1996 (HIPPA), Pub. L. 104–191, 110 Stat. 1936.

29 Shavel (n 5) 369.

does not provide specific implementation guidelines, making it difficult for companies to interpret the regulation and establish appropriate data management practices to ensure compliance. [30]

2. Incapability to Pay for the Full Harm Done

29 Harm under the data protection regulation is not straightforward to define. Possible administrative fines influence preference for regulation or liability even greater than the risk of paying damages. This determinant shall be adjusted for the data protection field as data actors often measure risks relating to imminent administrative fines and not harm-related costs. Shavell states that the party's assets are crucial in establishing whether this determinant favours more regulation or liability – the greater the likelihood of harm being much larger than assets, the greater the appeal of regulation. However, such presumptions shall be altered considering the importance of fines in the data protection field.

30 It is crucial to consider how harm is interpreted under the data protection legislation. While it is relatively easy to determine harm in cases of data breaches when a financial loss occurs (e.g., cases of identity theft), there are difficulties in measuring such harm when the loss is intangible (e.g., mere disclosure of personal data) or not related to data breaches (e.g., refusal to grant access to personal data held by an organisation) – although the claimants could invoke a non-pecuniary loss, "there is hardly any other issue in tort law which is assessed so differently throughout Europe".[31]

31 What we can agree upon is that privacy, in general, and data, in particular, hold certain economic value. If privacy is regarded as a specific type of property owned by an individual, a market emerges that defines the value of privacy (or data) loss. In this context, it is reasonable to conclude that various combinations of regulatory interventions, technological solutions, and economic incentives could effectively balance protection and sharing, thereby enhancing both individual and societal welfare.[32] However, the content of such 'balance' is not certain due to too divergent views on the value of privacy itself.

32 **Europe.** The inability to pay relates more to the failure to pay a fine than to pay for the harm done in the context of the GDPR. Usually, when organisations to whom the GDPR applies assess the risk, they consider the possibility of being fined, not the damages that could be required to pay for the harm caused. However, the GDPR allows a Supervisory Authority to impose a fine for up to 20 million EUR or 4 % of the annual turnover, whichever is higher.[33] The second limit proved useful for fining major corporations – the top 10 fines imposed under the GDPR exceed the 20-million limit, with 1.3 billion EUR being the highest fine imposed.[34]

33 Some national jurisdictions in the EU may be considered stricter than others. For example, in 2023, the French Supervisory Authority issued 42 sanctions, including 36 administrative fines for a total amount of 89 million EUR,[35] the Irish Supervisory Authority issued 19 fines for a total amount of 1.55 billion EUR,[36] the Spanish Supervisory Authority issued 367 decisions, including the imposition of fines for a total amount of more than 29 million EUR.[37] In

30 Clément Labadie and Christine Legner, 'Building data management capabilities to address data protection regulations: Learnings from EU-GDPR,' 38(1) *Journal of Information Technology*, 2023, 17.

31 Jonas Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases', 13(2) *Journal of European Tort Law*, 2022, 135.

32 Acquisti et al., (n 16) 484.

33 GDPR (n 24) Article 83(5).

34 Until 23 August 2024, more than 2100 fines, reaching more than 4.5 billion euros overall, were imposed by Supervisory Authorities across Europe (GDPR Enforcement Tracker, 2023) <https://www.enforcementtracker.com/?insights> accessed 23 August 2024.

35 *See* CNIL 'The 2023 Annual Report of the CNIL' <https://www.cnil.fr/en/cnil-publishes-its-annual-report-2023 > accessed 23 August 2024.

36 *See* Data Protection Commission 'Data Protection Commission Publishes 2023 Annual Report' < https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2023-annual-report > accessed 23 August2024.

37 *See* AEPD 'The AEPD receives for the third consecutive year

comparison, in 2023, the Lithuanian State Protection Inspectorate issued 13 fines for a total amount of 64,060 EUR.[38] To date, in Lithuania only one major fine was issued for GDPR violations of almost 2.4 million EUR.[39] However, close cooperation between the Supervisory Authorities and the one-stop-shop principle allows to, in general, keep the enforcement practice unified. While some of the fines do not cause a significant burden, there are examples when even a small administrative fine under the GDPR is too hefty for small organisations.[40] The possibility for courts to reduce fines functions as a safeguard for organisations to receive fair sanctions. However, the GDPR imposed approach of rigorous fines could generally propose that Shavell's determinant – incapability to pay – favours the liability more than the regulation.

34 **The US**. In contrast to the EU's regulatory model, the US model presents challenges in assessing an organization's incapability to pay fines or compensation for harm. The Federal Trade Commission (FTC) has a mandate to charge organisations with violation of Section 5 of the FTC Act, which prohibits unfair and deceptive actions and practices in or affecting commerce. While the FTC also enforces various federal consumer privacy and security laws, such as COPPA and GLBA, the frequency of enforcement actions remains limited, typically focusing on large technology firms rather than a broader range of organizations handling personal data.[41] However, the number of such actions is insignificant according to the publicly available information – in other words, while the FTC has the discretion to impose significant fines to the extent it relates to consumer protection, the number of launched investigations is very limited and usually targets tech giants rather than all organisations that in one way another process personal data.

35 Although other federal institutions can impose fines under sector-specific laws, these actions are relatively infrequent. However, when fines are imposed, they tend to be substantial, acting as a deterrent and encouraging compliance within regulated sectors. Despite this, a primary concern in the US remains the actual financial exposure faced by organisations if privacy-related lawsuits are successful. This aligns with the distinct litigation culture in the US, where companies often rely on self-regulation and precautionary measures to avoid substantial liabilities, as highlighted by Shavell.[42] Small and medium-sized enterprises, in particular, perceive less urgency in assessing their capacity to pay fines or face litigation – the data shows that in the US, targets for hefty fines are usually big tech companies, which are also at higher risk of facing a class action.[43]

---

the highest number of complaints in its history' < https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-recibe-por-tercer-anno-consecutivo-mayor-numero-reclamaciones-historia > accessed 23 August 2024.

38 *See* Valstybinė duomenų apsaugos inspekcija 'The State Data Protection Inspectorate has published its 2023 activity report', < https://vdai.lrv.lt/lt/naujienos/valstybine-duomenu-apsaugos-inspekcija-paskelbe-2023-m-veiklos-ataskaita/ > accessed 23 August 2024.

39 *See* Valstybinė duomenų apsaugos inspekcija 'A company operating an online second-hand clothing trading and exchange platform is fined under the General Data Protection Regulation', < https://vdai.lrv.lt/lt/naujienos/internetine-devetu-drabuziu-prekybos-ir-mainu-platforma-valdanciai-bendrovei-skirta-bauda-pagal-bendraji-duomenu-apsaugos-reglamenta/ > accessed 23 August 2024.

40 For example, the Lithuanian division of the International Council of Monuments and Sites (ICOMOS) was fined 3000 euros for lack of legal basis for data processing under the GDPR. However, the court reduced the fine to 1500 euros, considering the annual budget and the ICOMOS activity in the cultural heritage field. *ICOMOS* case (Judgment of the Vilnius Regional Administrative Court), No. EI2-1249-789/2020 (2020-04-08).

41 Federal Trade Commission, "Privacy and Security Enforcement" <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> (accessed 10 October 2024).

42 Shavell (n 5) 363.

43 According to data published by the FTC, over the last five years, actions for different types of privacy violations have been brought before tech giants such as Miniclip, Microsoft Corporation, Facebook, Amazon.com, Google, Epic Games (see: Federal Trade Commission, 'Protecting Consumer Privacy and Security', <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa> and <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 26 August 2024). The latter, for example, recently resulted in Epic Games agreeing to pay $520 million - a $275 million fine for violating the Children's Online Privacy Protection Act and $245 million in refunds for using "dark patterns" that misled customers

36 While Shavell's theory suggests that incapacity to pay favours *ex-ante* regulation, this concept proves to be complex in data protection. The development of this field shifted towards fines as a preferred way to incentivise market participants. Therefore, organisations evaluate possible fines in different jurisdictions. Unlike more abstract US approach to fines, the EU's harmonised enforcement across Member States has resulted in a consistent and rigorous application of fines. Furthermore, the ability to assess incapacity to pay in both jurisdictions hinges on differing interpretations of harm within the context of data protection.

3. Escaping the Threat of Suit for Harm Done

37 The possibility of escaping the threat of a suit for harm done is very likely in the data protection field. Shavell indicates that the importance of this aspect is partly determined by why a lawsuit may not be filed.[44] First, the harm that may occur in the data protection field is hardly measured. Therefore, the possibility of escaping the suit is relatively high. Second, usually, in cases of massive data breaches, the harms a company generates are widely dispersed, making it unattractive for any victim individually to initiate legal action, especially against big-tech companies. This may be overcome by the possibility of maintaining class actions. We focus on the possibility of class actions rather than individual claims, as we consider class actions to be more relevant for evaluating organisations' preference for either regulation or liability. Third, difficulties for suing may occur due to a long period of time before actual harm related to a data breach occurs, meaning that the necessary evidence can be ineffective by the time the lawsuit is filed. Fourth, it could be challenging to attribute harm to responsible parties. For example, malicious action that causes harm is performed by a third party that accessed data online and not by an organisation that was in possession of the data.

38 **Europe.** GDPR sets not only a mechanism for imposing fines but the right to claim damages for anyone who has suffered material or non-material harm due to a violation of the GDPR (Article 82(1) of the GDPR). This means that a breach of the GDPR may have consequences under both private and public law. Data subjects can seek compensation before national courts for material or non-material damage that results from the infringement of their rights under the GDPR. The regulation also sets the principle of full compensation for the plaintiffs, which is very protective of data subjects' rights. Some of the potential damages, such as costs incurred due to fraudulent spending, credit card charges, and so on, are straightforward to identify (and for companies to reimburse individuals for). In contrast, "non-material damage" is a more abstract concept under the data protection legislation that is difficult to define.

39 While filing individual actions before corporations for causing harm may not look very promising, the GDPR and EU Regulation on Collective Redress[45] provides for the possibility of class actions.[46] Spreading the cost of litigation across many plaintiffs creates a greater likelihood of challenges being brought in court. However, the situation of bringing collective action is not uniform across the EU. Even though the GDPR states that the data subject "shall have the right to" initiate actions, it does not provide the data subject with an actionable tool. Instead, EU Member States are responsible for this. In other words, because the GDPR does not cover the procedural elements of a data subject's claim, a reference to national procedural legislation should be made. This raises the issue that there could be as many personal data collective action procedures as the EU Member States, contrary to the GDPR's objective of consis-

into making unwanted purchases (see: Federal Trade Commission 'FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges' <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making>, accessed 26 August 2024).

44 Shavell (n 5) 363.

45 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

46 According to Article 80 of the GDPR, a data subject has the right to appoint a non-profit entity, organisation, or association with statutory objectives in the public interest and activity in the field of data protection to file a complaint on their behalf.

tency across Europe.

40 Significant developments in the right to damages under GDPR infringement were recently provided by the CJEU. A request for a preliminary ruling regarding the case between *UI v. Österreichische Post AG* challenged whether compensating a claimant requires, in addition to a GDPR violation, that the claimant has experienced damage or if the infringement of GDPR provisions is sufficient itself (referral for a preliminary ruling by the Supreme Court of Justice of the Republic of Austria). The CJEU concluded that Art. 82 of the GDPR requires establishing (i) "damage", either material or non-material; (ii) an actual infringement of the GDPR; and (iii) a causal link between the two."[47]

41 **The US.** US tech giants are also not immune from class actions, and the possibility of evading a lawsuit in case of massive data-protection relation issues is relatively high. There are successful examples. For instance, video conferencing platform Zoom faced a class action for allegedly sharing users' data without their consent and providing false information about their software being end-to-end encrypted. Inc. Privacy Litigation sued Zoom, claiming that such alleged conduct violated California state and federal laws. Zoom denies these allegations of any liability whatsoever. The parties agreed to the settlement. The court has decided that everyone who fits the set description is a settlement class member and can submit a claim form and receive payment. Zoom has agreed to pay 85 million dollars to settle the action.[48] The same situation happened with the video-sharing app TikTok, which faced a lawsuit for using and collecting users' data in connection with their use of the app without the proper notice or consent, a violation of state and federal law. TikTok has agreed to pay 92 million dollars to eligible claimants to settle the action.[49]

42 However, recent case law confirmed difficulties faced by privacy class actions brought in the US. The US Supreme Court judgment in *TransUnion LLC v. Ramirez case*[50] confirmed that there is no standing without concrete harm in federal court. The issue stemmed from the Fair Credit Reporting Act, which mandates that credit reporting agencies follow reasonable processes to ensure that customer records are as accurate as possible. According to the Fair Credit Reporting Act,[51] any individual who willfully fails to comply with the rules "is liable to that customer" for damages. Due to database errors, TransUnion has wrongly identified thousands of law-abiding Americans on the government's list of terrorists, drug traffickers, and serious criminals in their credit reports, which made (or could have made) obtaining financial services impossible or very hard to achieve. In this case, the court held that only 30 per cent of the class action members experienced an actual injury from the errors. The remaining 70 per cent lacked standing because the mere presence of inaccuracy in an internal data file, if it was not disclosed to a third party, caused no concrete harm. As a result, the US Supreme Court remanded the case, stating that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm."[52]

43 There are certain differences between the litigation cultures in Europe and the US. While there has yet to be a wave of GDPR-related class actions in Europe, the long tail of these kinds of cases makes it impossible to establish if this is because they do not exist or because they are still making their way through the system. However, the risks of facing a class action are relatively low in the data protection field

47 Case C-300/21 *UI v Österreichische Post AG* [2023].

48 In re: Zoom Video Communications, Inc. Privacy Litigation, 'Settlement Agreement' (US District Court for the Northern District of California, Case No. 5:20-cv-02155-LHK, 28 July 2021) <https://www.zoommeetingsclassaction.com/Content/Documents/Settlement%20Agreement.pdf> accessed 14 August 2024.

49 In re: TikTok, Inc., Consumer Privacy Litigation, 'Order and Final Judgment' (US District Court for the Northern District of Illinois, Case No. 1:20-cv-04699, 1 December 2022) <https://angeion-public.s3.amazonaws.com/www.TikTokDataPrivacySettlement.com/docs/264-Order+and+Final+Judgment.pdf> accessed 14 August 2024.

50 *TransUnion LLC v. Ramirez* (Supreme Court of the United States), No. 20–297 (2021-06-25).

51 Fair Credit Reporting Act, Pub L No 91-508, 84 Stat 1114 (1970), 15 U.S.C. § 1681n.

52 *TransUnion LLC v Ramirez* [2021] USSC 16, 594 US 413 (2021), p 436 <https://www.supremecourt.gov/opinions/20pdf/594us2r59_197d.pdf> accessed 14 August 2024.

due to the nature of the activity that could cause harm. Courts both – in the EU and the US – put forward a general tendency that future harm that may occur as a result of a violation of data protection is not enough, and incurred harms shall be tangible. Having this in mind, the data protection field under Shavell's determinants does not necessarily prefer regulation to liability, as risks of facing class actions that could exceed the fine are relatively low because courts tend to critically evaluate harm under data protection regimes.

4. Administrative Costs

44 Administrative costs are one of the first things that organisations take into account while considering privacy-related risks and compliance policies. Therefore, it is crucial to understand administrative costs for estimating efficiency and social preference for the EU or US data protection models. The cost of the liability system must be broadly defined to include the time, effort, and legal expenses borne by private parties in the litigation or settlements and public expenses for trials. The administrative costs of regulation include the expense of maintaining state institutions performing regulatory functions and the private costs for compliance. The main difference is that, unlike under liability, administrative costs are incurred under regulation regardless of whether or not harm is caused.

45 Litigation costs in the EU and US differ significantly according to the International Comparisons of Litigation Costs report by NERA Economic Consulting.[53] Under this report, the US has the highest liability costs as a percentage of the gross domestic product of the countries surveyed, with liability costs at 2.6 times the average level of the Eurozone economies. In addition, US liability costs are four times higher than those of the least costly European countries in the performed study – Belgium, the Netherlands and Portugal. Considering this, it is fair to admit that the EU seems to be a more favourable jurisdiction in terms of litigation costs in the data protection field. However, as litigation costs depend on a number of factors outside of the scope of this article, further analysis focuses on the administrative costs of the data protection regulation models.

46 The background paper by Chander et al.[54] summarises a number of studies regarding the costs of compliance with data protection frameworks in the EU and the US. Chander et al.[55] show that the amount of incurred administrative costs favours *ex-post* liability to *ex-ante* regulation as administrative costs under compliance are always incurred while under liability, incurred only when the harm is done. Furthermore, compared to the EU, the US-chosen sectoral approach creates less overall administrative costs in terms of compliance. However, for actors in specific sectors (e.g., healthcare or finance), these costs are significantly higher than for actors in other fields in the US. Enforcement costs in the EU also supersede the costs in the US due to mandatory funding for Supervisory Authorities and excessive workload due to complaints and investigations under the GDPR.

47 It seems that Shavell's provided model of preference for *ex-ante* regulation and *ex-post* liability is applicable to compare the EU and US-chosen data protection frameworks if the reservations explained above are taken into account. The four determinants may not be applied blindly and have to be adjusted for each legal issue to benefit the evaluation of social preference. In terms of this research, we adjusted the general contents of Shavell's determinants and compared how each of them is reflected in the EU and US data protection regulation models:

53 U.S. Chamber of Commerce Institute for Legal Reform <https://instituteforlegalreform.com/wp-content/uploads/media/ILR_NERA_Study_International_Liability_Costs-update.pdf> accessed 22 December 2023.

54 Chander, Anupam and Abraham, Meaza and Chandy, Sandeep and Fang, Yuan and Park, Dayoung and Yu, Isabel, Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation (April 15, 2021). Policy Research Working Paper 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. 2021. Georgetown Law Faculty Publications and Other Works. 2374., Available at SSRN: < https://ssrn.com/abstract=3827228 > or < http://dx.doi.org/10.2139/ssrn.3827228 >.

55 Ibid.

Determinant	The difference in knowledge about risky activities	The incapability of paying for the full harm done	Escaping the threat of suit for harm done	Administrative costs
Adjustments in the data protection field	-	The data protection field is closely related to imposing fines; therefore, organisations assess not only the sum of possible damages but also possible fines in different jurisdictions.	The risks of facing a class action are relatively low in the data protection field due to the nature of the activity that cxxould cause harm	-
EU	GDPR obliges Supervisory Authorities to possess more information than private parties on technological aspects to enforce the regulation. The regulator is often considered to have created too stringent rules for organisations that usually do not possess significant threats to individuals regarding their data.	Has established a more or less unified practice of imposing fines across the EU Member States	Courts both – in the EU and US – put forward a general tendency that future harm that may occur as a result of a violation of data protection is not enough, and incurred harms shall usually be tangible.	Enforcement costs in the EU supersede the costs in the US due to mandatory funding for Supervisory Authorities and excessive workload due to complaints and investigations under the GDPR.
US	The chosen US fragmentary approach to federal regulation reflects specific fields that require a higher standard of protection and provides examples where the regulator possesses more knowledge than private parties	The US jurisdiction is more abstract in terms of the possibility of fines		The US chosen sectoral approach creates less overall administrative costs in terms of compliance; however, for actors in specific sectors (e.g., healthcare or finance), these costs are significantly higher than for actors in other fields in the US

Table 2. S. Shavell's model applicability to EU and US data protection regulation models

48 The assumption that regulatory authority in the EU is omnipotent within the field of data protection is questionable. There are areas where the costs of accessing information are demonstrably lower for companies, challenging the notion of absolute regulatory control. In contrast, the fragmented regulatory approach of the US, particularly its emphasis on protecting more sensitive areas such as children's privacy, may offer a preferable model. Both jurisdictions face significant challenges in striking a balance between regulatory oversight and liability models, particularly in light of the complexities involved in determining optimal damages. This difficulty is exacerbated by the inherent challenges in quantifying harm within the data protection domain.

49 The nature of data breaches often allows entities in both the EU and the US to evade litigation for the harm caused, largely because proving tangible harm in this field is inherently difficult. Additionally, the high threshold for initiating class action lawsuits, especially in the EU, further complicates the pursuit of redress. The wide disperse of harm done in data breaches may be an argument for a regulatory approach such as in the EU. The overall administrative costs associated with data protection are relatively higher in the EU, particularly when compared to the more fragmented and less stringently monitored regulatory environment in the US. With these considerations in mind, we turn to the central question of this paper: can the application of the Shavell model to data protection regulatory frameworks in the US and the EU provide any valuable policy-oriented insights?

D. Can Economic Analysis of Law Solve the Rising Challenges in the EU and the US Data Protection Regulation Frameworks?

50 Our study shows that neither the data protection frameworks in the EU nor in the US perfectly balances *ex-ante* regulation and *ex-post* liability. On the contrary, recent proposals and policy changes in both jurisdictions suggest that the pursuit of social efficiency, alongside its compatibility with privacy protection, remains an on-going challenge.

I. What are the Challenges that Data Protection Regulation Models are Facing?

51 Both current data protection regulation models in the US and the EU face some severe criticism. As in any other disputable area of regulation, data protection raises concerns for both sides: privacy activists who claim that imposed regulation (or no regulation at all) is not sufficient to protect individuals from abuse of their data and companies operating in the data-related field, claiming that burden imposed on them regarding privacy cause more damage than adds to sufficient protection of persons.

52 Although the GDPR made a big shift in EU society's understanding of data protection, it still faces significant challenges. There is a widely spread opinion that GDPR has shown to be a costly and challenging burden on Europe's digital economy rather than functioning as a "golden" standard data regulation for the rest of the world to follow. Even though it is agreed that the GDPR has drawn significant attention to privacy-related issues, it has "proven to be costly, unmanageable, or prohibitively expensive without providing a commensurate privacy benefit".[56] Considering that the GDPR shortcomings are of core importance to demonstrate whether the chosen economic efficiency model in the EU is the most desired by the society, there are several GDPR issues highlighted by its critics that are relevant to our analys: (i) Most rules in the GDPR are formed as abstract principles and contain vague terminology;[57] (ii) The GDPR's complexities and responsibilities are carried most easily by the market's largest players;[58]

56 Canadian Marketing Association (CMA), 'Privacy Law Pitfalls. Lessons Learned from the European Union' (2022) <https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6> accessed 22 December 2023.

57 Heiman argues that such vagueness is the opposite of the well-drafted law, in his view – this major data protection law lacks clarity surrounding its terms and, therefore, has fallen short, especially when it parallelly imposes a significant rise in the fine's regime. See Matthew R. A. Heiman, 'The GDPR and the Consequences of Big Regulation' [2020] Pepperdine Law Review, vol. 47, no. 4, 945.

58 Compliance expenses are insignificant for a major

(iii) GDPR creates complexity for consumers.[59]

53 GDPR may even be viewed as a protectionist instrument. "It has been noted that lifting restrictions, such as in data protection, would foster growth, including by increasing imports of digital services".[60] Such growth may lead to greater reliance on large non-EU businesses. In this way, stricter data protection laws could give domestic companies a competitive edge, aiding their global expansion.[61]

54 What are the concerns about the balance of efficiency and privacy standards in the US? For many years now, the US has raised the question of whether federal privacy law is needed in order to balance the interests of business freedom and privacy protection.[62] The support for the lack of unified federal data protection law mainly relies on the freedom of business and the possibility of using personal data almost unrestrictedly. In the current market model, processing personal data means more profit for technology-based organisations. More personal data – more possibilities to provide personalised advertisements, create customer profiles, and use other methods to increase sales or benefit otherwise. Besides, broad data protection regulation creates more limitations for technological developments.[63] For example, despite the intention of the technologically neutral text, GDPR is considered incompatible with many technological solutions, such as based on artificial intelligence or automated decision-making. For example, the GDPR emphasizes transparency, purpose limitation, and data minimization, which can conflict with how AI systems operate. AI often requires large datasets for training and improving accuracy, making it difficult to align with GDPR's restrictions on data collection and processing. As provided in the European Parliament study "a number of AI-related data protections issues are not explicitly answered in the GDPR, which may lead to uncertainties and costs, and may needlessly hamper the development of AI applications".[64] Following this, companies might choose to innovate less or pursue their ideas in less restrictive jurisdictions, such as the US.[65]

55 Despite clear advantages for business activity and advanced technological development, the US data protection framework faces severe criticism: among others are (i) the application, scope, enforcement, and sanctions of distinct sectora legislations and state-level rules vary greatly[66]; (ii) the regulation is often considered as not providing individuals with the necessary level of protection.[67]

corporation, but they are a significant burden for small and medium enterprises in the EU. It is even argued that users are less willing to experiment with new platforms and tools, preferring to remain with the "devil they know" regarding privacy compliance (see Layton R, 'The 10 Problems of the GDPR. The US Can Learn from the EU's Mistakes and Leapfrog Its Policy' (Statement before the Senate Judiciary Committee on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation, American Enterprise Institute, 2019).

59 it is argued that with the GDPR, consumer notices have become even more frequent and complicated, making it less possible for users to properly read the content and make informed decisions. See CMA (n 56) 16.

60 Martina F. Ferracane, 'The Costs of Data Protectionism.' In *Big Data and Global Trade Law*, ed. Mira Burri [2021] Cambridge: Cambridge University Press. chapter, 63–82.

61 Pascal D. König, 'Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept' <https://onlinelibrary.wiley.com/doi/10.1002/epa2.1160> accessed 22 December 2023.

62 Kessler, J. 'Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource"', (2019) 93/1 Southern California Law Review 99-128.

63 Ibid. p. 105.

64 European Parliament, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Study, 2020) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530 accessed 10 October 2024.

65 CMA (n 56).

66 For example, the fact that the FTC *de facto* acts as the federal Supervisory Authority creates uncertainty for companies operating in the US. In many cases, the FTC has charged organisations with violation of Section 5 of the FTC Act, which prohibits unfair and deceptive actions and practices in or affecting commerce.

67 In 2016, Pew Research Centre (PRC) published a report stating that many Americans believe that tracking their online behaviour is in their best interests or that it is a price to pay for free or discounted products (Lee Rainie L and Maeve Duggan, 'Privacy and Information Sharing' (*Pew*

56 In the EU, the GDPR, while pioneering, imposes high compliance costs and extensive regulatory obligations that disproportionately burden smaller entities, creating what Shavell would view as an inefficient allocation of resources. The abstract nature of the GDPR's requirements, combined with its strict data protection mandates, supports Shavell's critique of regulatory error: the high risk of overregulation where harm potential is low, especially for smaller enterprises with limited data processing scopes. By failing to directly address new technological advances the GDPR inadvertently disincentivises technological growth within the EU, reinforcing Shavell's view that *ex-ante* regulations must evolve continually to reflect practical contexts.

57 In the US, the sectoral, fragmented regulatory approach offers flexibility and low compliance costs, arguably fostering innovation. However, this comes at the expense of consistent privacy protections, and the patchwork nature of US data laws results in regulatory gaps that may lead to public mistrust. Shavell's determinants suggest that this model risks underestimating the social cost of privacy harm due to its *ex-post* liability reliance, which may fail to deter data misuse effectively. Furthermore, the absence of a federal standard aligns with Shavell's notion that *ex-post* liability does not guarantee adequate preventative measures. The lack of uniformity across sectors and states means that while companies enjoy greater freedom, this freedom may result in less accountability and variable privacy standards.

Research Center: Internet, Science & Tech, 14 January 2016) <https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/> accessed 22 December 2023.). Four years later, another PRC research found that about half of adults in the US (52 per cent) indicated they recently opted not to use a product or service because they were concerned about how much personal data would be gathered (see Andrew Perrin, 'Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns' (*Pew Research Center*, 14 April 2020) <https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/> accessed 22 December 2023).

II. How Do the EU and the US Jurisdictions Attempt to Consider Economic Efficienty?

58 The developments in recent years in the EU and the US suggest that, with or without intentional economic analysis of law, rule-makers in both jurisdictions understand the flaws of data protection frameworks. Therefore, recent legislative steps presuppose that jurisdictions have already taken steps to rebalance their data protection regulation approaches that encompass efficiency arguments.

59 A good example of the flawed European data protection framework and the possibilities to balance the interests of data subjects and organisations is the approach taken by the United Kingdom's authorities after Brexit. In the post-Brexit era, the regulator started consulting the stakeholders on implementing a more pro-growth and pro-innovation data regulation framework instead of the adopted UK GDPR.[68] According to the UK Information Commissioner, "(...) there are ways in which the legislation can be changed to make it simpler for companies to do the right thing when it comes to our data. Perhaps most notably, it is vital that the inevitable regulatory and administrative obligations of legal compliance are proportionate to the risk an organisation's data processing activities represent."[69] Currently, the UK Parliament is still in negotiations as to the chosen approach to balance the rights of individuals and regulatory certainty for organisations in order to boost the UK economy.[70]

68 *See* 'UK: ICO Welcomes DCMS Consultation Reviewing UK Data Regime' (*DataGuidance*, 7 October 2021) <https://www.dataguidance.com/news/uk-ico-welcomes-dcms-consultation-reviewing-uk-data> accessed 28 December 2023.

69 *See* ICO 'Ico Response to DCMS Consultation "Data: A New Direction"' <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/10/response-to-dcms-consultation-foreword/> accessed 28 December 2023.

70 The UK Parliament is currently in legislative stage of the new Data Protection and Digital Information Bill. *See* Data Protection and Digital Information Bill HL Bill (2023–24) 67 <https://bills.parliament.uk/bills/3430> accessed 31 October 2024.

60 Although data protection is now considered one of the main paradigms in the EU regarding the protection guaranteed to its citizens, the EU still significantly focuses on the economic side of regulation, maintaining its primary idea as an economic union (even though it had already shifted from these roots). Therefore, the approach to economic efficiency cannot be completely abandoned in the EU. The GDPR itself reflects that data protection is necessary for the proper functioning of the internal market[71] and that the activities of Supervisory Authorities in terms of enforcement of the GDPR shall also facilitate the free flow of personal data within the internal market.[72] Irrespective of the fact that GDPR applies directly in all the EU member states, as mentioned above, each national Supervisory Authority still has its own leeway towards the enforcement actions of the GDPR.

61 The recently adopted Digital Markets Act[73] (DMA) exemplifies the EU's effort to balance economic efficiency with data protection. Although the DMA does not function as a data protection law Baschenhof explains that the DMA aims to recalibrate data interactions in the EU by emphasising market objectives more strongly, particularly for reasons connected to fair competition.[74] For data collected by gatekeepers (core platform service providers), the DMA aligns partially with data protection goals by mandating fair practices.

62 While not a dedicated data protection law, the DMA contains several provisions[75] reflecting a "data as a resource", framing data as a market resource to promote competition. This approach may inadvertently lower privacy standards, despite requiring gatekeepers to comply with GDPR. Thus, the DMA reflects the EU's evolving approach, influenced by economic analysis, to balance business growth with data protection.

63 On the other side of the Atlantic, taking into account public opinion and changes in the international arena, the US returns to discussions on whether one federal law to rule all sectoral laws shall be adopted. There are many federal bill initiatives that deal with one or another aspect of federal privacy legislation in the US Congress.[76] The scholarship is divided into two camps – the one is for and the other is against the need to enact federal data protection legislation.

64 Kessler suggests that the US should adopt a federal standard that would grant consumers protection as strong as the GDPR or the California Consumer Privacy Act (CCPA).[77] Large technology businesses are concerned about having to comply with a patchwork system of regulations, which will likely be more expensive and burdensome than complying with a single state's law because other states are expected to follow California's lead and implement rules similar to the CCPA. Most businesses would reject legislation as harsh as the GDPR. Privacy activists claim that these businesses are just trying to pre-empt laws like the CCPA by establishing a diluted standard that is considerably less stringent than California's.[78] Privacy activists reject this strategy and have stated that they would fight attempts to pass a watered-down federal law that pre-empts state laws.[79] The disruption – pandemic-related issues like vaccine certificates, digital contact tracing, and mobile health apps – have helped put privacy and data security at the forefront of public debate, changing the public demand for federal privacy law.

65 There are certain advantages if the federal law is

71 GDPR (n 24) recital §21.

72 GDPR (n 24) recital §123.

73 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1.

74 Phillip Baschenhof, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?'[2022] Journal of Law, Technology and Policy, Volume 2022, Issue 1, 101.

75 For example, DMA (n 72) Article 6(10).

76 International Association of Privacy Professionals, 'US Federal Privacy Legislation Tracker' (IAPP, 15 August 2023) https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ accessed 23 August 2024.

77 California Consumer Privacy Act of 2018 (CCPA), California Civil Code Section 1798.100.

78 Kessler (n 62), p. 123.

79 Joanna Kessler (n 62), 99.

enacted, including the ones related to economic efficiency. Rather than requiring consumers to parse through privacy policies and understand the nuances of various state laws, federal privacy legislation would clarify which baseline rights consumers are entitled to when it comes to safeguarding their data and ensure there are appropriate enforcement mechanisms in place. Comprehensive legislation at the federal level would benefit businesses. Rather than monitoring fifty different state laws and sectoral federal legislation and attempting to assess, interpret, and design frameworks that comply with each, federal legislation would provide a simplified framework for company compliance and help the companies to understand better privacy requirements and follow them. The latest developments in state-level enforcement also prove that federal law could provide more clearance for organisations. For example, in August 2022, Sephora Inc. reached a settlement of 1.2 million dollars with the California Attorney General for CCPA violations.[80] With one federal legislation, the enforcement actions would be more coordinated without the possibility for organisations to be fined for the same privacy practices in different states. Enforcement actions before organisations at a state level and rising possibilities to fine organisations by FTC may push the federal government to fasten the federal privacy legislation discussions.

66 The federal privacy legislation in the US could also benefit the economy. In the current global privacy scenery, compliance with privacy standards also makes brands more attractive to customers. Organisations tend to set at least minimal standards if no regulatory framework is in force. Therefore, adopting federal privacy legislation would promote data sharing with organisations subject to privacy standards, such as the GDPR, because data processed by US organisations would be more compatible with these standards. The fact that the EU has already created the data protection framework could benefit the US if it adopts a GDPR-style privacy law. Many American companies do business in the EU. Therefore, they are legally required to follow the GDPR. If the US privacy rules and regulations followed the GDPR's model closely, it would eliminate the necessity for organisations to develop a separate set of data protection measures for US customers.

67 While the US continues to negotiate federal legislation, some companies tend to keep aware and be proactive. Any legislation approved in the US will probably include elements of the GDPR, CCPA, other state laws. Rules on the use of AI-driven technologies, and other privacy and consumer protection areas will be included into regulation accordingly. Compliance with such standards will ensure a smoother transition when a general legislation is adopted in the US. The bottom line of the provided analysis is that irrespective of the chosen current regulatory approach - both jurisdictions aim to search for a long-term balance where economic efficiency plays a significant role.

E. Conclusion

68 Our analysis, grounded on the seminal work of Shavell, utilised efficiency-based arguments to evaluate whether an *ex ante* or *ex post* legal framework is more appropriate in specific regulatory contexts. We discovered that Shavell's classic model is instrumental in analysing current data protection regulations. While comprehensively accounting for all aspects of data protection regulation is challenging, our analysis suggests that the US data protection model more effectively enables data processing organisations to assess risks associated with potential data breaches compared to the EU legal framework.

69 The study shows that while the GDPR overextends regulatory scope, leading to inefficiencies for smaller entities, the US's fragmented model creates inconsistencies in privacy protection. Both the EU and US models face difficulties in ensuring that responsible organisations are held accountable for harm caused, largely due to the challenges in identifying harm in data protection violations. The potential for entities to evade legal consequences for such harm exists in both jurisdictions. This could be attributed to the complex burden of proof in the EU and the lack

80 See 'Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act' (*State of California - Department of Justice - Office of the Attorney General*, 24 August 2022) <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement> accessed 22 December 2023.

of clear recognition of harm in data protection violations in the US. The US model appears more favorable, considering administrative costs that constant and comprehensive monitoring in the EU entails. The US model benefits from less regulation and less intrusive oversight, which potentially makes it a more efficient framework for managing data protection concerns.

70 Although our analysis was limited to economic analysis of law, in particular, the model of Shavel, we found out how difficult it is to assess data protection in merely economic analysis of law realm. However, the actual need to minise costs of data protection regulatory frameworks grounds important efforts from both jurisdictions – the EU and the US – to find out better calibrated balance between *ex ante* regulation and *ex post* liability. The most prominent examples include the discussion on whether the differential approaches of national supervisory authorities may ensure better balanced application of GDPR in the EU; the Digital Markets Act as an attempt to balance company interests and privacy of consumers even more in the digital realm and the on-going discussion in the US to adopt federal comprehensive data protection regulation.

71 Our intention was not to deliver a definitive judgment on the superiority of either the US or EU data protection models. We looked whether the purely economic analysis of law based model might contribute to the better understanding of different data protection policies. The research provided insight into how efficiency driven considerations may better support more fragmented legislation such as in the US. The costs grounded rationale of data protection supports *ex post* liability as more preferred option.

72 However, the limitations of the model itself do not allow us to speculate on better policy recommendations. This is strongly related to data protection being primarily the policy developed under different conceptual framework than economic analysis of law, i. e. human rights. The economic analysis of law provides us with more generalised view on regulation costs, disregarding possible market deficiencies such as information asymmetry. The trade-off between economic efficiency and consumer protection is at the heart of data protection. Therefore, the chosen conceptual framework implicitly prioritise one or the other. Although rapidly developing data-driven markets requires us to rethink the way individuals must be protected from intrusion to their privacy, the economic realm should also not be ignored, taking into account better informed consumers who begin to acknowledge the value of their data and the potential to trade of this high-valued asset.