More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance

Transnational data governance has been a field of growing legislative development, emblematic of the increasing regulation of the digital economy. However, there are substantial challenges in governing cross-border data flows and activities while ensuring uniformity across borders and between jurisdictions. The General Data Protection Regulation (GDPR), a European Union (EU) regulation put into effect in 2018, is a transnational data governance regime that aims to create a golden data privacy standard with an extraterritorial reach. The GDPR is an emerging global standard that digital companies and nations will likely ultimately adhere to due to the significance of the European economy and to the EU's regulatory power. However, the GDPR's intra-EU implementation in the past five years has brought to light the inconsistencies in its application.

This Note analyzes the obstacles confronted by the GDPR as a transnational data governance regime and the degree of legal fragmentation that has surfaced within its regional roll-out. The lack of consistency in implementing the GDPR will not only undermine the credibility and reliability of European regulatory power, but also create uncertainty for users and regulators across the world. To better understand the gap between the intended global reach of the GDPR and the current state of its uneven implementation, this Note discusses various factors that have contributed to the intra-EU divergence within national enforcement and corporate compliance. It then evaluates the strengths and deficiencies of suggested solutions to enhance the effective enforcement of the GDPR. By doing so, it links the GDPR's intra-EU legal fragmentation to the

broader tension between Europe's right-based approach to data privacy, the United States' market-based approach, and China's state-based approach. Lastly, the Note sheds light on the importance of aligning these fundamental models in order to create a uniform and sustainable solution to transnational data governance and envision the future for global data privacy.

INTRODUCTION

Transnational data governance is a field of rapid legislative development as increasing numbers of digital platforms and data flows have transformed the global economy. Between 2010 and 2019, cross-border data flows increased by 45 percent annually, growing from 45 to 1,500 terabits per second.[1] Between 2020 and 2022, data flows were projected to continue to reach unprecedented heights in the face of the new demands for remote work and global communication.[2] As data becomes increasingly important to the international economy, there has been a growing recognition of the need for data privacy and protection. This need is slowly being met. According to statistics released by the United Nations (U.N.) Conference on Trade and Development, 137 out of 194 countries had put forth legislation to secure the protection of data and privacy as of 2021.[3] From February 2021 to March 2023, 17 new countries enacted data privacy laws, bringing the global total to 162.[4] Yet these regulations lack uniformity. The expanding global landscape of data privacy regulations has ushered in an emerging concern that the disparities in national laws could hamper cross-border data flows and disrupt the digital economy.[5] Devising general principles and policies to govern data across borders is thus a growing priority for legislative bodies and international organizations.[6] However, there are substantial challenges in implementing a transnational data governance regime while ensuring its consistency across borders.[7]

---

1. JEONGMIN SEONG ET AL., GLOBAL FLOWS: THE TIES THAT BIND IN AN INTERCONNECTED WORLD 4 (Janet Bush ed., McKinsey Global Institute 2022).

2. *See, e.g.*, WORLD BANK GROUP, WORLD DEVELOPMENT REPORT 2021: DATA FOR BETTER LIVES 102–06, 237 (2021).

3. U.N. Conference on Trade and Development (UNCTAD), Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/AVW3-WPCT].

4. Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills*, 181 PRIVACY L. & BUS. INT'L. REP. 1, 1–2 (2023).

5. Organisation for Economic Co-operation and Development (OECD), OCED GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 47–53 (1981).

6. *See, e.g.*, OECD, *Recommendation of the Council on Enhancing Access to and Sharing of Data*, OECD/LEGAL/0463 (May 10, 2021), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463 [https://perma.cc/5K32-RPUU].

7. *See generally* Douglas W. Arner, Giuliano G. Castellano & Eriks Selga, *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L. J. 623 (2022).

The General Data Protection Regulation (GDPR), put into effect by the European Union (EU) in May 2018, aims to create a comprehensive data privacy regulation regime within Europe and across the globe.[8] Under the legislation's mandate, "data controllers" and "processors" located outside of the EU must also comply with the GDPR when they monitor or process data from individuals within the EU.[9] Under the theory of the "Brussels Effect," Professor Anu Bradford describes the GDPR as an emerging global standard that digital companies as well as nations will adhere to because of the significance of the European economy and the EU's regulatory power.[10] European regulators have articulated this aspiration to set an international data privacy standard. Věra Jourová, the vice-president of the European Commission, remarked that the GDPR seeks to advance a common EU approach and culture of data privacy that will play a key role in leading global data governance.[11] She recognized the EU's "window of opportunity" to "promote the golden standard [it has] established and inspire others."[12]

Despite the standard-setting ambition of the GDPR, the legislation has faltered in achieving uniform results even within the EU. Under the consistency mechanism of the regulation, coined the one-stop-shop (OSS),[13] enforcement responsibilities are delegated to the national supervisory authorities (SAs) of each EU Member State.[14] For an organization conducting cross-border data processing, the

8. Deloitte, *GDPR Top Ten: #3 Extraterritorial applicability of the GPDR*, DELOITTE: GDPR (Apr. 3, 2017), https://www2.deloitte.com/lt/en/pages/legal/articles/gdpr-top-ten-extraterritorial-applicability.html [https://perma.cc/KU9T-H5QQ].

9. Commission Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32–33 (EU) [hereinafter GDPR]. A data controller is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. *Id.* art. 4. A data processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.*

10. ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 142 (2020).

11. Věra Jourová, Commissioner for Values and Transparency, Eur. Comm'n, Speech at the Computers, Privacy and Data Protection Conference: General Data Protection Regulation (Jan. 30, 2019).

12. *Id.*

13. EUROPEAN DATA PROTECTION BOARD (EDPB), THE EDPB: GUARANTEEING THE SAME RIGHTS FOR ALL (2020) [hereinafter EDPB: GUARANTEEING THE SAME RIGHTS FOR ALL].

14. *Id.*

GDPR requires the organization to work with the SA based in the same Member State as its "main establishment."[15]

While the one-stop-shop was designed as a consistency mechanism, the implementation of the legislation has been uneven. Issues including insufficient resources, disagreements among national data protection authorities (DPAs), and troubled application of the OSS have made it difficult to implement the law effectively within the region.[16] Companies and consumers are left uncertain by the inconsistent application.[17]

Five years after the GDPR came into effect, European users and regulators still hope to establish a data privacy standard and lead by example in the protection of digital rights.[18] There have been tightening measures of enforcement,[19] including various landmark cases in

---

15. Annika Sponselee & Rodney Mhungu, *GDPR Top Ten #10: One Stop Shop*, DELOITTE: GDPR, https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html [https://perma.cc/3376-QFH4]; see GDPR, *supra* note 9, art. 4 for the definition of "main establishment:"

> a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

16. ESTELLE MASSÉ, ACCESS NOW, THREE YEARS UNDER THE EU GDPR: AN IMPLEMENTATION PROGRESS REPORT 15, (2021).

17. *See* ERNST & YOUNG, GLOBAL FORENSIC DATA ANALYTICS SURVEY 2018, 24 (2018) https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-global-fda-survay.pdf [https://perma.cc/7MSJ-3NSN] (According to this survey, as of 2018, only 33% of the respondents indicated that they had a plan for GDPR compliance, while the remaining majority said that they were either not familiar with the GPDR, or had yet to take any action); *see also* Matthew Newman et al., *GDPR and CCPA Start to Bare Teeth as Privacy Protection Goes Global*, 21 BUS. L. INT'L 283–84 (2020).

18. Wojciech Wiewiórowski, European Data Protections Supervisor (EDPS), Speech at the EDPS "Future of Data Protection: Effective Enforcement in the Digital World" Conference (June 17, 2022).

19. SEBASTIÃO BARROS VALE ET AL., FUTURE OF PRIVACY FORUM, INSIGHTS INTO THE FUTURE OF DATA PROTECTION ENFORCEMENT: REGULATORY STRATEGIES OF EUROPEAN DATA

2021 and 2022 with sizeable fines on tech giants Amazon ($ 888 million)[20] and Meta ($ 400 million).[21] Nevertheless, there is a continuing demand for more effective, stringent, and consistent enforcement.[22] Regulators have begun calling for reforms to show that the GDPR can be implemented uniformly, or alternatively, to institute a bigger role for a pan-European regulator.[23] It has become increasingly apparent that before fulfilling its global ambition for the regulation, the EU must first ensure effective protection of data privacy for its own citizens.

This paper delves into the obstacles confronted by the GDPR as a transnational data governance legislation and the degree of legal fragmentation that has surfaced within its intra-EU implementation. To better understand the gap between the intended global reach of the GDPR and the reality of its inconsistent regional implementation, this Note discusses various factors that have contributed to the national divergences within enforcement efforts and the mirrored problem of uneven corporate compliance. Without establishing intra-EU consistency and robustness of GDPR enforcement, the GDPR will fail to achieve its aspiration of setting a global standard since the failure will damage the credibility of European regulatory power and create uncertainty among users and regulators. This Note links the intra-EU legal fragmentation to the broader obstacle of striving for standardization while wrestling with national specificity, a problem confronted by transnational data governance regimes at large.

The paper proceeds in three parts. First, it examines the development of the GDPR as the EU's leading legislation on data privacy

---

PROTECTION AUTHORITIES FOR 2021-2022, at 3 (2021), https://iapp.org/media/pdf/resource_center/fpf_report_insights_future_data_protection_enforcement_european_dpas_2021_2022.pdf [https://perma.cc/G39C-VG3H].

20. Stephanie Bodoni, *Amazon Gets Record $888 Million EU Fine Over Data Violations*, BLOOMBERG LAW (July 30, 2021, 7:03 AM), https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach (last accessed Dec. 1, 2023).

21. Adam Satariano, *Meta Fined $400 Million for Treatment of Children's Data on Instagram*, N.Y.TIMES (Sept. 5, 2022), https://www.nytimes.com/2022/09/05/business/meta-children-data-protection-europe.html [https://perma.cc/3CUC-MYXQ].

22. Vincent Manancourt, *EU Privacy Chief Bashes Lack of GDPR Enforcement Against Big Tech*, POLITICO (June 17, 2022, 12:07 PM), https://www.politico.eu/article/gdpr-europe-wojciech-wiewiorowski-privacy-chief-lack-enforcement-big-tech/ [https://perma.cc/CK4F-3CAY].

23. Luca Bertuzzi, *10 Years After: The EU's 'Crunch Time' on GDPR Enforcement*, INT'L ASSOC. OF PRIVACY PROFESSIONALS (June 28, 2022), https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement/ [https://perma.cc/JL7A-F599]; *see also* Manancourt, *supra* note 22.

and explains its anticipated global effect. Part I lays out the regulation's structure and enforcement mechanisms, before discussing the obstacles it has confronted in achieving effectiveness and consistency. Part II examines the intra-EU divergence and fragmentation that have surfaced in enforcing the GDPR. This section also addresses the status of Big Tech's evasive compliance as a mirrored issue that has been exposed and exacerbated by the GPDR's enforcement problem. Building from this descriptive context, Part III proceeds to assess the strengths and weaknesses of various proposals raised by EU regulators. It suggests that the legal fragmentation that has surfaced under the GDPR goes beyond the insufficiency of its design or enforcement; rather, it has exposed the inherent challenge within transnational data governance regimes in attempting to reconcile the aim of global uniformity and the reality of tensions and rifts between nations. Lastly, Part III draws attention to the broader tension between Europe's right-based approach to data privacy, the United States' market-based approach, and China's state-based approach, and urges the alignment of these fundamental models in order to create a uniform solution to data governance across the globe.

I. UNDERSTANDING THE GDPR: A REGIONAL AND GLOBAL ENDEAVOUR

A. The GDPR's Extraterritorial Reach and the Brussels Effect

The GDPR arose against the backdrop of a globalized economy that is increasingly dependent on digital technologies and data,[24] and is populated by technology companies that have amassed immense power by controlling personal data and cross-border data flows.[25] The GDPR firmly stipulates that the "protection of natural persons in relation to the processing of personal data is a fundamental right."[26] It calls for "lawfulness, fairness and transparency" as central principles in the processing of personal data,[27] and limits the purposes for which data can be used and the quantity of data that can be collected and processed.[28]

24. *Digital Development*, THE WORLD BANK, https://www.worldbank.org/en/topic/digitaldevelopment/overview [https://perma.cc/T6QR-57CV].

25. BRADFORD, *supra* note 10, at 131.

26. GDPR, *supra* note 9, at 1.

27. *Id.* art. 5(1)(a).

28. *Id.* arts. 5(1)(b), 5(1)(c).

The binding GDPR replaced the EU's voluntary 1995 Data Protection Directive, which was adopted in the infancy of the Internet.[29] From the conception of GDPR, it was viewed as more than just a European law due to its extraterritorial scope.[30] It applies to all companies processing the personal data of individuals residing in the EU, regardless of the company's location or where the processing activities take place.[31] Even if a company is not established in the EU, the GDPR can still apply if the company targets individuals in the EU by offering products or monitoring their behavior.[32] Additionally, the regulation bars cross-border transfer of data from the EU to non-EU countries, also called third countries, unless the European Commission has determined that the third country, or the international organization in question, "ensures an adequate level of protection."[33] This practice of territorial extension allows the EU to govern activities beyond its physical territory and "shape the focus and content of third country and international law."[34] By way of the GDPR's expansive coverage, the EU's global regulatory power in data privacy is "hard-wired into the design" of the legislation.[35]

The Brussels Effects, coined by Professor Anu Bradford, provides insight into the intended global impact of the GDPR. She theorizes that the EU has been vested with global regulatory power, consisting of a de facto effect and a de jure effect, that allows the jurisdiction to become a source of global standards.[36] The GDPR imparts a de facto effect because global businesses generally adopt uni-

29. *The History of the General Data Protection Regulation*, EDPS, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU [perma.cc/PRG9-J6PY]; *see also* Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L 281) 31(EU) [hereinafter Data Protection Directive].

30. *See* Deloitte, *supra* note 8; *see also* Wim Nauwelaerts, *The Extra-Territorial Reach of EU Data Protection Law,* SIDLEY AUSTIN LLP (July 2019), https://www.sidley.com/en/insights/publications/2019/07/the-extra-territorial-reach-of-eu-data-protection-law [https://perma.cc/P7F7-LCGY].

31. BRADFORD, *supra* note 10, at 133.

32. *See* Nauwelaerts, *supra* note 30.

33. GDPR, *supra* note 9, art. 45.

34. Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 AM. J. COMP. L. 87, 89 (2014).

35. *Id.*

36. BRADFORD, *supra* note 10, at 132.

form policies to streamline their internal corporate processes in accordance with the regulation.[37] Indeed, neither abandoning the EU, which occupies a significant market share for data-driven technology companies, nor circumventing the GDPR, which would entail moving their data processing activities outside the EU, is a commercially viable option for large tech companies, such as Google and Facebook.[38] Following this theory, the convergence of transnational data privacy protections would emerge as a result of the compliance of global businesses.[39]

Bradford also suggests that there is a de jure Brussels Effect, where nations will look toward the GDPR as a model for devising their own data privacy and protection legislations.[40] More than 120 countries have already adopted privacy laws based on the EU's data regulations in recent decades.[41] For instance, Japan set up an independent agency to handle privacy complaints to conform to the EU's privacy standards;[42] Brazil put in place a data protection bill months following the GDPR;[43] and most recently in 2021, China adopted its first data privacy law, the Personal Information Protection Law (PIPL), which closely resembles the GDPR.[44]

The ambition of the EU to "forge a common EU approach and a European culture of data privacy" is apparent.[45] At the "Computers, Privacy and Data Protection" EU Conference eight months after the GDPR went into effect, then-European Commissioner and now European Commission Vice-President, Věra Jourová, expressed the desire

37. *Id.* at 142.

38. *Id.*

39. *Id.* at 144.

40. *Id.* at 148.

41. Daniel Michaels, *Hot U.S. Import*: *European Regulations*, WALL ST. J. (May 7, 2018), https://www.wsj.com/articles/techs-pickup-of-new-data-privacy-rules-reflects-eus-growing-influence-1525685400 [https://perma.cc/NV2C-FWC7].

42. Mark Scott and Laurens Cerulus, *Europe's new data protection rules export privacy standards worldwide*, POLITICO (Jan. 25, 2018), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ [https://perma.cc/KEN9-XAMN].

43. Angelica Mari, *Brazilian president signs data protection bill*, ZDNET (Aug. 15, 2018), https://www.zdnet.com/article/brazilian-president-signs-data-protection-bill/ [https://perma.cc/7QYY-K5TK].

44. Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J. (Aug. 20, 2021, 4:55 AM), https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138 [https://perma.cc/2WPL-82F3].

45. Jourová, *supra* note 11.

"to promote this gold standard [the EU] ha[s] established and inspire others."[46]

B. Implementation of the GDPR

To ensure a "consistent level of protection . . . and to prevent divergences" throughout the EU, the GDPR must provide legal certainty, fairness, and transparency.[47] Specifically, it identifies the need for "consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States."[48]

One of the GDPR's main objectives is to ensure the homogenous protection of data privacy throughout the EU and prevent legal fragmentation or uncertainty.[49] Under the GDPR's predecessor, each country was free to adopt its own data privacy laws, which resulted in a patchwork of divergent privacy standards.[50] France and Germany, in particular, became champions of data privacy regulation due to historical concerns over terrorism and cybersecurity.[51] Unlike the prior Directive, the GDPR is binding on all Member States, and sets out

46. *Id.*

47. GDPR, *supra* note 9, at 3.

48. *Id.*

49. *Id.* at 2.

50. Kurt Wimmer, *The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?*, COMMUNICATIONS LAWYER (ABA) (Sept. 2017) at 16, https://www.cov.com/-/media/files/corporate/publications/2017/09/the_long_arm_of_the_european_privacy_regulator_does_the_new_eu_gdpr_reach_us_media_companies.pdf [https://perma.cc/FX3G-XN7Z].

51. *See* Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, TIME (May 24, 2018, 7:12 PM), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ [https://perma.cc/R638-5WAB]; Winston Maxwell, *French Surveillance Law Permits Data Mining, Drawing Criticism from Privacy Advocates*, HOGAN LOVELLS: CHRONICLE OF DATA PROTECTION (Aug. 6, 2015), https://www.engage.hoganlovells.com/knowledgeservices/news/french-surveillance-law-permits-data-mining-drawing-criticism-from-privacy-advocates_1 [https://perma.cc/7HC2-MFRN].

comprehensive data privacy mandates[52] to achieve greater harmonization across the region.[53]

1. Enforcement Structure and Mechanisms of the GDPR

To give effect to its transnational regulatory power, the GDPR is designed with robust enforcement mechanisms. The enforcement structure of the GPDR is multi-tiered, ranging from regional to the EU member-state level.[54] Under the one-stop-shop, the GDPR's enforcement obligations principally fall to the data protection authorities (DPAs) of each Member State.[55] The GDPR requires each Member State to establish one or more public "supervisory authority" (SA) via national legislation,[56] which are responsible for enforcing and implementing the regulation at a countrywide level.[57] These independent authorities are also referred to as national data protection authorities. They have investigative, corrective, authorization, and advisory powers to oversee GDPR enforcement, investigate breaches of the GPDR, and bring legal proceedings.[58] Their respective jurisdictions and enforcement powers are primarily limited to the territory of the Member State that appointed them.[59]

The one-stop-shop is developed to reconcile the two goals of simultaneously ensuring a level playing field across the EU and pro-

52. Andrew Rossow, *The Birth of GDPR: What Is It and What You Need To Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=73cf1c2255e5 [https://perma.cc/56HA-2YMZ].

53. Peter Hustinx, EU DATA PROTECTION LAW: THE REVIEW OF DIRECTIVE 95/46/EC AND THE PROPOSED GENERAL DATA PROTECTION REGULATION, STATEWATCH 29 (2014), https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf [https://perma.cc/TZY7-P27Y].

54. *See* Brian Daigle & Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*, 2020 J. OF INT'L COM. & ECON. 1, 5.

55. *See id*.

56. *See* GDPR, *supra* note 9, art. 51 & art. 54.

57. *See id.* art. 51(1); *see also* Detlev Gabel & Tim Hickman, *Chapter 14: Data Protection Authorities—Unlocking the EU General Data Protection Regulation* (Apr. 5, 2019), https://www.whitecase.com/insight-our-thinking/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection [https://perma.cc/VV5R-LN2L].

58. *See* Gabel & Hickman, *supra* note 57; *see also* GDPR, *supra* note 9, art. 58.

59. Gabel & Hickman, *supra* note 57.

moting the proximity of citizens and companies to national authorities.[60] Individuals may lodge a complaint with a SA in the Member State of their habitual residence, place of work, or place of the alleged infringement.[61] Organizations are also able to deal with just one SA for their cross-border processing activities. By its design, the mechanism streamlines the administrative processes, both for companies and individuals, to exercise their rights under the GDPR from their home base.[62]

The enforcement mechanism is also designed to ensure that competent national authorities work in cooperation with each other to oversee cross-border cases and reach consensus.[63] The GDPR provides that the regional SAs over a company's main establishment are competent to act as the lead SA (LSA) for the cross-border processing carried out by the company's controllers or processors.[64] The data controller or processor has the discretion to designate a main establishment where its decisions regarding data processing are taking place, subject to the supervision of the SAs.[65] When the controller or processor is established in more than one Member State, or where the processing activity substantially affects—or is likely to substantially affect—data subjects in more than one Member State, the LSA will need to cooperate with other SAs where the complaints may be lodged initially.[66]

To further ensure consistent application of the GDPR and effective cooperation between the SAs, the EU formed the European Data Protection Board (EDPB), an independent body that brings together the head of each national authority, as well as the data protection

60. *See Breakout 1 - Enforcement: The Key to a Golden Standard?*, EDPS CONFERENCE 2022 (June 16, 2022), https://www.edpsconference2022.eu/en/press-media/media [https://perma.cc/27NS-KLRS].

61. GDPR, *supra* note 9, art. 77.

62. EDPB: GUARANTEEING THE SAME RIGHTS FOR ALL, *supra* note 13.

63. *See* GDPR, *supra* note 9, art. 60(1).

64. CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL), *GDPR ENFORCEMENT COOPERATION AND THE ONE-STOP-SHOP: LEARNING FROM THE FIRST THREE YEARS*, 3 (Sept. 24, 2021), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_discussion_paper_-_gdpr_enforcement_cooperation_and_the_one-stop-shop__23_sept_2021_.pdf [https://perma.cc/8DBX-PPCB]. For the definition of "main establishment," see *supra* note 15. For the definition of "data controller" and "data processor," see *supra* note 9.

65. *See* Gabel and Hickman, *supra* note 57.

66. GDPR, *supra* note 9, art. 124; *see also id.* arts. 55, 60; MASSÉ, *supra* note 16, at 13.

supervisor of the EU institutions (EDPS).[67] The EDPB's responsibilities include "issu[ing] guidelines on the interpretation of core concepts of the GDPR," and "rul[ing] by binding decisions on disputes regarding cross-border processing."[68] The EDPB advises that while the LSAs shall assume a leading role in managing and steering the cases forward, they do not have exclusive competence, meaning that their decisions are subject to the views of other SAs.[69] Relevant SAs should provide each other with information and mutual assistance in order to apply the legislation consistently and effectively.[70] The GDPR also authorizes joint operations between SAs to conduct collaborative investigations and issue joint enforcement measures.[71] When a consensus cannot be reached, the EDPB has the authority to step in and issue binding decisions.[72]

Additionally, the GDPR equips each Member State with authority to issue sanctions and remedial relief, including warnings, a ban on processing, and monetary fines.[73] The monetary fines are the most high-profile and punitive enforcement measures.[74] They are administered by the SAs in each Member State,[75] and such penalties must be "effective, proportionate and dissuasive."[76] The GDPR lays out two tiers of fines: Less severe infringements can result in a fine up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever is higher. More serious infringements can trigger maximum fines of up to €20 million, or 4% of the business's total annual worldwide turnover, whichever is higher.[77]

---

67. EUR. COMM'N, *What is the European Data Protection Board (EDPB)?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en [https://perma.cc/8HCK-Q4KN].

68. *Id.*; *see also* GDPR, *supra* note 9, art. 65.

69. EDPB, GUIDELINES 02/2022 ON THE APPLICATION OF ARTICLE 60 GDPR 9 (2022) [hereinafter EDPB, GUIDELINES].

70. GDPR, *supra* note 9, art. 61.

71. *Id.* art. 62.

72. *Id.* art. 65.

73. EUR. COMM'N, *What if my Company/Organisation Fails to Comply with the Data Protection Rules?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en [https://perma.cc/6DBM-P633].

74. *See generally, Three Years of GDPR: The Biggest Fines So Far*, BBC (May 24, 2021), https://www.bbc.com/news/technology-57011639 [https://perma.cc/5K3V-NSJN].

75. *Id.*

76. GDPR, *supra* note 9, art. 83–84.

77. *Id.*

The €20 million ceiling on fines marks a pivotal change from the former Directive, under which the maximum fine for a single infringement was less than €1 million in most cases.[78] As of August 2023, there had been 1,801 GDPR fines, amounting to over €4.05 billion.[79] The largest fine to date under the GDPR was a penalty of €1.2 billion imposed on Meta by the Irish Data Protection Commission (DPC).[80]

2. Burdens and Challenges

The Court of Justice of the European Union (CJEU), in June 2021, confirmed that "[the one-stop-shop model] is essential for the proper and effective operation of the GDPR."[81] In the updated guidelines released by the EDPB in March 2022, the EDPB remarked that the OSS model allows SAs of all Member States to "be involved in a type of co-decision procedure."[82] Yet the model has garnered growing scrutiny. First, there has been uncertainty in cross-border cases as to which Member State and its respective DPA are responsible for investigating and monitoring firms whose business affects subjects across the EU.[83] Companies are allowed to designate their main establishment subject to certain criteria. However, it is unclear how the DPAs apply these criteria and determine the legitimacy of the companies' designation.[84] Consequently, there is concern over whether companies are able to forum shop and choose main establishments in countries that best serve their commercial and regulatory interests.[85]

78. Detlev Gabel & Tim Hickman, *Chapter 16: Remedies and Sanctions—Unlocking the EU General Data Protection Regulation*, WHITE & CASE LLP (Apr. 5, 2019), https://www.whitecase.com/insight-our-thinking/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection [https://perma.cc/M9AC-Z4S7]; *see also* Data Protection Directive, *supra* note 29.

79. *See* CMS, *GDPR Enforcement Tracker* (last visited Aug. 7, 2023), https://www.enforcementtracker.com/?insights [https://perma.cc/AJ9P-6PES].

80. Arthur Beesley, *Meta Fined Record €1.2bn by Irish Regulator for Violating European Privacy Rules*, IRISH TIMES (May 22, 2023), https://www.irishtimes.com/technology/big-tech/2023/05/22/facebook-owner-meta-fined-record-12bn-by-irish-regulator-for-violating-european-privacy-rules/ [https://perma.cc/S4CL-XQHB].

81. CIPL, *supra* note 64, at 4; *see also* Case C-645/19, Facebook v. Gegevensbeschermingsautoriteit, ECLI:EU:C:2021:483, ¶ 88 (June 15, 2021).

82. EDPB, GUIDELINES, *supra* note 69, at 6.

83. Daigle & Khan, *supra* note 54, at 6.

84. MASSÉ, *supra* note 16, at 17–18.

85. *Id.* at 18.

This issue of determining who the LSA is, though purportedly resolved by the establishment of the EDPB and one-stop-shop,[86] reveals the larger issue of lack of communication and clarity amongst DPAs on how to apply the law.[87] In 2020, a number of DPAs expressed reservation over the adequacy of the current communication system, the Internal Market Information System (IMI).[88] Further, local authorities do not have a harmonized approach in interpreting and applying the GDPR. Member States follow different approaches when adopting various levels of specification and safeguards.[89] The EDPB has identified diverging interpretations of concepts relating to the cooperation mechanism, such as what "relevant information" or "without delay" entails in practice.[90] The lack of clear guidelines, compounded by the insufficiency of intra-regional communication, poses additional roadblocks in ensuring the GDPR's consistent application.[91]

The divergence amongst nations is further sharpened by the differences in national laws and administrative procedures.[92] The GDPR requires Member States to legislate in some areas and provides them with the flexibility to further specify the GDPR in others.[93] As of January 2023, all Member States have adopted new legislation or adapted their national data protection law.[94] The application of the

86. *See* Daigle & Khan, *supra* note 54, at 23.

87. MASSÉ, *supra* note 16, at 15.

88. *Id.*; EDPB, *Individual Replies from the Data Protection Supervisory Authorities*, https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en [https://perma.cc/R94V-PFL4].

89. *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation*, at 6, COM (2020) 264 final (June 24, 2020).

90. EDPB, *Contribution of the EDPB to the Evaluation of the GDPR Under Article 97*, 10 (Feb. 18, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf [https://perma.cc/Y56E-X8AL] [hereinafter EDPB, *Contribution of the EDPB*].

91. *Id.* at 10–11.

92. *See id*. at 10; *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 5.

93. *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 7.

94. *Id.* The new Slovenian Data Protection Act ("ZVOP-2"), which seeks to implement certain aspects of the GDPR systematically, was formally adopted in December 2022 after a four-year delay and officially "transposes" the EU regulation onto Slovenian law. *See Slovenia Passes Personal Data Protection Act*, INT'L ASSOC. OF PRIV. PROS.: DAILY DASHBOARD (Dec. 16, 2022), https://iapp.org/news/a/slovenia-passes-personal-data-protection-act/ [https://perma.cc/7BKB-8VUA].

GDPR in conjunction with local laws has led to "a degree of fragmentation and diverging approaches,"[95] both substantively and procedurally. One example of a substantive difference among Member States is the age of consent for children to access certain kinds of sensitive information.[96] There are procedural differences as well. The EDPB identified notable differences among national procedures concerning complaint-handling procedures, admissibility criteria, duration of proceedings, and consultation of other concerned SAs on draft measures.[97] Such differences, both substantive and procedural, have resulted in gaps among national practices and introduced confusion within the one-stop-shop.

These issues stem in part from the fact that the DPAs have not made sufficient use of the tools provided by the GDPR to facilitate co-decision and cooperation.[98] As of February 2020, the European Commission noted that no joint operation procedure had been triggered.[99] Two years later, the EDPB identified the lack of utilization of cooperation instruments as a persistent issue.[100] Cultural and strategic differences between DPAs regarding data privacy, and the lack of experience of lead authorities in handling cross-border matters, are also responsible for the divergence in implementation practices.[101] These issues have made the development of a common EU data privacy standard, and harmonization between DPAs, challenging.[102]

95. *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 6.

96. *Id.* at 7.

97. EDPB, *Contribution of the EDPB*, *supra* note 90, at 3.

98. *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 5.

99. EDPB, *Contribution of the EDPB*, *supra* note 90, at 14. Subject to Article 97 of the GDPR, the Commission shall submit a public report on the evaluation and review of the GDPR to the European Parliament and to the Council by May 25, 2020 and every four years thereafter. *See* GDPR, *supra* note 9, art. 97.

100. EDPB, *Statement on Enforcement Cooperation*, 1 (Apr. 28, 2022), https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf [hereinafter EDPB, *Statement on Enforcement*].

101. CIPL, *supra* note 64, at 5–6.

102. *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 5.

II. LEGAL FRAGMENTATION AND DIVISIBILITY WITHIN THE GDPR

Jourová, vice-president of the European Commission, remarked at the EDPS Conference held in Brussels in June 2022 that this is indeed "crunch time" for EU legislators and agencies to act.[103] She expressed the urgency for the EU to "collectively [show that] the GDPR and its enforcement [are] effective."[104] The lack of a uniform data privacy standard within the EU has cast doubt on the credibility of European regulatory power and the feasibility of regulating cross-border data privacy. It will also discourage users and countries from regulating and protecting digital rights. The need to resolve the GDPR's intra-EU inconsistency is therefore a crucial step in preventing the GDPR from becoming a "paper tiger" law. Without establishing a unified regional data privacy standard, the Brussels Effect envisioned by EU legislators and scholars will be undermined, confidence among nations to follow suit will waver, and incentives for companies to comply will be diminished.[105]

A. Identifying Fragmentation and Inconsistency in GDPR Enforcement

1. Unequal Burden Sharing

One of the fundamental structural obstacles within GDPR enforcement is the issue of "unequal burden sharing" between Member States and their respective DPAs.[106] As the one-stop-shop requires the SAs in the country where a company has declared its main establishment to take the lead in enforcing the regulation, the costs of enforcement have fallen unevenly on various Member States, which has led to fragmentation and bottlenecks in implementation.

Major tech giants, notably Meta, Google, WhatsApp, and Microsoft, have all made Ireland their main establishment, partly due to Ireland's favorable tax regime.[107] The DPC has thus assumed the role

103. Bertuzzi, *supra* note 23.

104. EDPS, THE FUTURE OF DATA PROTECTION: EFFECTIVE ENFORCEMENT IN THE DIGITAL WORLD 37 (2022), https://www.edpsconference2022.eu/sites/default/files/2022-11/22-11-10-EDPS-Conference-Report-2022_EN.pdf [https://perma.cc/U7Y7-2X8V].

105. *Id.* at 17.

106. Wiewiórowski, *supra* note 18.

107. Ryan Browne, *How Ireland Lost its Chance to Become Big Tech's 'super regulator'*, CNBC (May 4, 2022, 1:15 AM), https://www.cnbc.com/2022/05/04/how-ireland-lost-its-chance-to-become-big-techs-super-regulator.html [https://perma.cc/F7HD-7YAL].

of lead authority in regulating these companies. Between May 2018 and September 2022, the DPC received 1,278 cross-border complaints, for 85% of which it acted as the LSA.[108] Sixty-two percent of cross-border complaints handled by the DPC as the LSA were originally filed elsewhere.[109] Out of all cross-border complaints received by the DPC, 87% relate to just ten data controllers, including Meta, Google, and WhatsApp.[110] One-fifth of all complaints referred among the DPAs are referred to the Irish DPC.[111] The data poignantly illustrates the disproportionate regulatory and oversight burden falling on Irish regulators.

The Irish DPC has come under attack for its failure to effectively regulate the tech giants.[112] It has drawn criticisms from a number of individuals and organizations, including the Members of the European Parliament (MEPs), a group that called for an independent review of the DPC in 2021.[113] The Irish Council for Civil Liberties (ICCL) identified the DPC as the main bottleneck preventing the effective implementation of the GDPR. It reported that 98% of the cross-border cases handled by the DPC were unresolved as of May 2021.[114] The alleged delays in reaching decisions have been attributed to insufficient resources and staffing.[115] The DPC rebutted such criticism[116] and reported on the contrary that since May 2018, 73% of all cross-

108. DATA PROTECTION COMMISSION (DPC), ONE-STOP-SHOP CROSS-BORDER COMPLAINT STATISTICS: 25 MAY 2018 – 19 SEPT 2022, at 4 (Oct. 4, 2022), https://www.dataprotection.ie/sites/default/files/uploads/2022-10/04.10.22%20Cross%20border%20complaint%20stats%202018%20to%20Sept%202022.pdf [https://perma.cc/9SWX-CDHL].

109. *Id.*

110. *Id.* at 15.

111. IRISH COUNCIL FOR CIVIL LIBERTIES (ICCL), EUROPE'S ENFORCEMENT PARALYSIS: ICCL'S 2021 REPORT ON THE ENFORCEMENT CAPACITY OF DATA PROTECTION AUTHORITIES 4 (2021) https://www.iccl.ie/digital-data/2021-gdpr-report/ [https://perma.cc/EC5Q-5QBL].

112. Charlie Taylor, *DPC Rejects Criticism of its Regulation of Big Tech Companies*, IRISH TIMES (Apr. 27, 2021, 10:07 PM), https://www.irishtimes.com/business/technology/dpc-rejects-criticism-of-its-regulation-of-big-tech-companies-1.4549370 [https://perma.cc/D27Q-HHDB].

113. Luca Bertuzzi, *MEPs Call For Infringement Procedure Against Ireland*, EURACTIV (May 20, 2021), https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/ [https://perma.cc/A26X-QWGF].

114. ICCL, *supra* note 111, at 5.

115. Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES: STRATEGIC TECHNOLOGIES BLOG (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement [https://perma.cc/MGC3-DB2W].

116. Taylor, *supra* note 112.

border complaints it handled as the LSA have been concluded.[117] The agency, however, did not dispute the issue of staffing and financing and stated that the current management framework of the agency was "unsustainable and unfit for the purpose."[118]

In the meantime, there has been a committed effort to ameliorate the capacity problem confronted by the national authority. Between May 2018 and December 2022, the DPC grew from a staff of 90 to 258.[119] Two additional senior commissioners were appointed in 2022.[120] Its budget has also expanded annually, increasing by 22% from €19.1 million in 2021 to €23.2 million in 2022.[121] The DPC has requested an additional €1.25 million in its legal budget for 2023, a 50% increase from that of the previous year, and has vocalized an urgent need to appoint new senior staff.[122] The expanded resource allocation has correlated to a 53% reduction in the authority's average response time to conclude a case or complaint over the first twenty-four months following the implementation of the GDPR.[123] However, despite the significant increase in the DPC's staff and budget, there nevertheless remains a substantial gap in resources between the agency and the corporations it oversees. While the DPC announced final decisions to fine Meta Ireland €210 million and €180 million respectively for breaches of the GDPR in relation to its Facebook and Instagram

117. DPC, *supra* note 108.

118. Charlie Taylor, *DPC Warns Government of Need for Major Staffing Changes*, IRISH TIMES (Dec. 6, 2021), https://www.irishtimes.com/business/technology/dpc-warns-government-of-need-for-major-staffing-changes-1.4747874 [https://perma.cc/LCC7-QHHB].

119. Marie Daly, *Irish DPC Reports on Cross-Border Activity and Resources*, COVINGTON: INSIDE PRIVACY (Apr. 1, 2022), https://www.insideprivacy.com/uncategorized/irish-dpc-reports-on-cross-border-activity-and-resources/ [https://perma.cc/F6LB-6Q6M].

120. Laura Slattery, *Two Additional Data Protection Commissioners to be Appointed, McEntee Confirms*, IRISH TIMES (July 27, 2022), https://www.irishtimes.com/business/2022/07/27/two-additional-data-protection-commissioners-to-be-appointed-helen-mcentee-confirms/ [https://perma.cc/5HYR-9AU7].

121. *Id.*; Press Release, DPC, Statement on Budget 2022 (Oct. 12, 2021), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-budget-2022 [https://perma.cc/SF8M-SLF8].

122. Ken Foxe, *Data Protection Commission Warns of Urgent Need for New Senior Staff*, IRISH TIMES (Nov. 10, 2022), https://www.irishtimes.com/business/2022/11/10/data-protection-commission-warns-of-urgent-need-for-new-senior-staff/ [https://perma.cc/3B2K-9WN8].

123. *Id.*; *see also* DPC, RESOURCE ALLOCATION AUDIT 11 (2022), https://www.dataprotection.ie/sites/default/files/uploads/2022-03/Data%20Protection%20Commission%20-%20Resource%20Allocation%20Audit%20Final%20250122.pdf [https://perma.cc/CUP9-URBW].

services,[124] Meta had a total revenue of $32.17 billion for just its fourth quarter in 2022.[125] Its expected total expense for 2022 was $87.66 billion,[126] a figure almost 200 times greater than the fines imposed. Considering the drastic gap between the resources of the regulating authority and those of Big Tech companies, under-enforcement is a continuous concern impeding the regulation's ambition to standardize cross-border data privacy even within the EU.

The problem of insufficient resources is not unique to the Irish DPC. Between 2016 and 2019, there was a 42% increase in staff and a 49% increase in budget for DPAs across the board.[127] Yet despite the substantial expansion in resource allocation to national authorities, as of September 2022, 77% of the DPAs stated that they did not have enough resources, and 87% expressed a shortage in human resources.[128] The EDPB and the EDPS have also requested additional budget and staff to fulfill their duties, especially the enforcement of the regulation vis-à-vis Big Tech.[129] The EDPB claims an enhanced budget will strengthen the credibility, robustness, and legal predictability of enforcement under the GDPR.[130] Part III will assess whether an expansion in budget and staff would be a sufficient fix to the problem confronted by the GDPR, though the issue of under-capacity is not confined to jurisdictions with disproportionate responsibility and is instead reflected within the entire EU's enforcement of the GDPR.

2. Divergent Local Practices and Inadequate Intra-EU Cooperation

---

124. DPC, *Data Protection Commission Announces Conclusion of Two Inquiries Into Meta Ireland* (Jan. 4, 2023), https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland [https://perma.cc/K7E8-5TDU].

125. Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2022 Results (Feb. 1, 2023), https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx [https://perma.cc/6UH4-NKBT].

126. *Id.*

127. *Communication from the Commission to the European Parliament and the Council*, *supra* note 89, at 6 n.34.

128. EDPB, *Overview on Resources Made Available by Member States to the Data Protection Supervisory Authorities*, 5, 8 (Sept. 5, 2022), https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf [https://perma.cc/9MTB-VRZV] [hereinafter EDPB, OVERVIEW ON RESOURCES, Sept. 5, 2022].

129. Open letter from Andrea Jelinek and Wojciech Wiewiórowski on the EDPB Budget Proposal for 2023 (Sept. 15, 2022), https://edpb.europa.eu/our-work-tools/our-documents/letters/open-letter-edpb-budget-proposal-2023_en [https://perma.cc/HE5F-J22J].

130. *Id.*

Mechanisms

The differences in procedural rules, data protection cultures, and market situations among countries pose another legal and political hurdle to the GDPR's implementation. The absence of a robust intra-EU cooperation and communication system further prevents the reconciliation of these differences. [131]

The lack of uniformity between local authorities' practices and attitudes towards data privacy is reflected in the gap in the regulation's regional enforcement. There have been instances where national regulators have adopted divergent and even isolated views from the rest of the EU.[132] The newly-concluded case against Meta in 2021 provides such an example. In the Irish DPC's initial draft decision published in October 2021, the agency demonstrated an alarming willingness to side with the tech giant and allow it to bypass the GDPR. It claimed that Meta did not have an obligation to gather consent from its users as a legal basis for processing their data for targeted ads because it was offering a contract to its users that primarily concerned the processing of personal data. [133] This stance departs from the EDPB's long-standing guideline that a contract cannot "artificially expand the categories of personal data or types of processing operation."[134] The draft decision also proposed a penalty of $36 million—an amount that Meta earns in just over two and a half hours.[135] Ten out of the forty-seven DPAs, including those of Germany and France, which are historically more aggressive in data privacy regulation,

131. Letter from Ventsislav Karadjov replying to the EDRi, EPDB 2 (June 14, 2022), https://edpb.europa.eu/system/files/2022-06/20220614_edpb_reply_to_edri_letter.pdf [https://perma.cc/TC4R-VHBB].

132. ACCESS NOW, FOUR YEARS UNDER THE EU GDPR: HOW TO FIX ITS ENFORCEMENT 4 (July 2022), https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf [https://perma.cc/QEN5-9P9H].

133. Natasha Thomas, *Ireland's draft GDPR decision against Facebook branded a joke*, TECHCRUNCH (Oct. 13, 2021, 3:25 PM), https://techcrunch.com/2021/10/13/irelands-draft-gdpr-decision-against-facebook-branded-a-joke/ [https://perma.cc/MHK6-FGM6]; *see also* LB (through NOYB) v. Facebook Ireland Limited, IN-18-5-5, Draft Decision 68 DPC (Oct. 6, 2021), https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf [https://perma.cc/5CNW-ZAY6].

134. EDPB, GUIDELINES 2/2019 ON THE PROCESSING OF PERSONAL DATA UNDER ARTICLE 6(1)(B) GDPR IN THE CONTEXT OF THE PROVISION OF ONLINE SERVICES TO DATA SUBJECTS 10 (2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf [https://perma.cc/GMC4-W635].

135. Thomas, *supra* note 133.

raised objections.[136] Consultation between the DPC and concerned authorities failed to resolve their disagreement.[137] This dispute was subsequently referred to the EDPB, which issued a binding decision in December 2022 and stated that Meta Ireland inappropriately relied on a contract as a legal basis to process personal data for the purpose of behavioral advertising.[138] It also instructed the DPC to order Meta to bring its data processing into compliance within three months and issue significantly higher fines.[139] Accordingly, on January 4, 2023, the DPC issued a final decision against Meta Ireland following the EDPB's recommendations. It issued two fines of €210 million for breaching the GDPR relating to its Facebook service and a €180 million fine for breaches in relation to its Instagram service.[140] The conclusion of these two inquiries arrived over four years after the complaints were initially lodged on May 25, 2018, the day the GDPR went into operation.[141] However, in its press release, the DPC expressed its frustration over the EDPB's determinations and noted that the EDPB's direction to conduct a new investigation into Meta's activities was an overreach beyond the EDPB's designated role.[142] It further stated that it would bring an action for annulment before the CJEU to dismiss the EDPB's directions.[143] While this decision showcases the one-stop-

136. Isabella Roccia, *What the DPC-Meta Decision Tells us About the EU GDPR Dispute Resolution Mechanism*, INT'L ASSOC. OF PRIVACY PROFESSIONALS (Jan. 10, 2023), https://iapp.org/news/a/what-the-dpc-meta-decision-tells-us-about-the-gdprs-dispute-resolution-mechanism/ [https://perma.cc/N6YM-ZSTN].

137. Gareth Kristensen et al., *Irish Data Protection Commission's Decisions Regarding Facebook and Instagram*, CLEARY GOTTLIEB: CLEARY CYBERSECURITY AND PRIVACY WATCH (Jan. 17, 2023), https://www.clearycyberwatch.com/2023/01/irish-data-protection-commissions-decisions-regarding-facebook-and-instagram/ [https://perma.cc/YSZ4-6ZHH].

138. EDPB, *Facebook and Instagram decisions: "Important impact on use of personal data for behavioural advertising"* (Jan. 12, 2023), https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_en [https://perma.cc/RH87-R6XS] [hereinafter EDPB, *Facebook and Instagram decisions*]; *see also* EDPB, BINDING DECISION 4/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS INSTAGRAM SERVICE (ART. 65 GDPR) 113 (2022), https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf [https://perma.cc/HFZ9-5WQG].

139. *See* EDPB, *Facebook and Instagram decisions*, *supra* note 138.

140. DPC, *supra* note 124.

141. *Id.* Meta has also stated that it intends to appeal the substance of the decision and the fines. *See* Meta, *How Meta Uses Legal Bases for Processing Ads in the EU* (Jan. 4, 2023), https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/ [https://perma.cc/582W-R6JX].

142. DPC, *supra* note 124.

143. *Id.*

shop at work in resolving disputes between national authorities, it plainly reveals the growing tension between the DPAs and the difficulty for the EDPB and the European courts to adjudicate and reconcile these differences. As both Meta and the DPC are appealing the EDPB decision, this case also illustrates the stark reality that the interests of various DPAs are not always aligned, and that in some instances, the lead regulator may take a position favorable to the regulated company.

The discrepancies between national practices in enforcing the GDPR are also manifested in inconsistent procedures and efficiency in addressing complaints. The DPAs often employ different technical approaches for the submission of complaints and have various requirements for supporting evidence or prior actions related to a complaint.[144] For instance, while the Belgian and Italian DPAs allow submission of complaints via mail or website, others rely on national public portals that are used for general government submissions, not tailored for GDPR purposes.[145] The Hamburg DPA allows the attachment of files to clarify the complaints as an option rather than an obligation, while the Dutch DPA only allows for submissions that contain proof of communication about the complaint's subject matter with the organization against which the complaint is lodged.[146] These procedural differences, in effect, mean that individuals in different Member States do not enjoy a uniform level of procedural access to lodge complaints to their respective authorities.

The frequencies with which DPAs impose penalties and the severity of those penalties also vary. Local authorities are granted discretion in imposing sanctions, and they have published divergent criteria for determining fines. The Danish DPA, for example, requires the consideration of whether the processing purpose is profit-seeking or benevolent, while the Latvian DPA instead places an emphasis on the duration of the breach, the number of data subjects affected, and the financial benefits attained by the controller or processor.[147] In contrast to the delay of the Irish DPC, the Spanish Data Protection Agency (AEPD) produced over ten times more draft decisions than its Irish

144. ACCESS NOW, DATA PROTECTION LAW SCHOLARS NETWORK (DPSN), THE RIGHT TO LODGE A DATA PROTECTION COMPLAINT: OK, BUT THEN WHAT?: AN EMPIRICAL STUDY OF CURRENT PRACTICES UNDER THE GDPR 42–43 (2022), https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf [https://perma.cc/XR3M-WARY].

145. *Id.* at 42.

146. *Id.* at 44–45.

147. Sebastião Barros Vale, *Diverging Fining Policies of European DPAs: Is There Room for Coherent Enforcement of the GDPR?,* FUTURE OF PRIVACY FORUM (May 13, 2022), https://fpf.org/blog/diverging-fining-policies-of-european-dpas-is-there-room-for-coherent-enforcement-of-the-gdpr/ [https://perma.cc/C4UF-MFAE].

counterpart despite a smaller budget.[148] However, the penalties imposed by the AEPD have generally been less severe. Their highest fine to date is the €10 million imposed on Google in May 2022, which is a distance apart from the hundred-million-Euro fines imposed by other DPAs.[149]

The problem of inadequate cooperation and communication and the problem of insufficient budget are not divorced from one another, but are interrelated. In the 2022 EDPB survey, a number of SAs attributed the need for resource expansion partially to the costs of participating in and handling joint cooperation and communication.[150] The inadequacy of intra-EU cooperation procedures therefore impose additional costs, both financial and personnel-related, to resolve cross-border cases, and further accentuates the problem of inadequate resource allocation faced by national authorities.

The culture of data protection and the individual concerns of consumers in each jurisdiction are also partially responsible for the divergent national practices.[151] EU residents demonstrate varying levels of awareness of the GDPR, data protection laws, and DPAs. For example, most respondents in Czechia have heard about their DPA (90%), while in Belgium, less than half have heard about their DPA (44%).[152] They also have various practices and experiences sharing personal data online. In Belgium and Cyprus, 47% of respondents say that they do not read terms and conditions, whereas in Estonia, only 22% do not.[153] Therefore, the challenge of harmonization can find its source in consumer demands and interests.

148. ICCL, *supra* note 111, at 6.

149. Manel Santilari, *Spanish Data Protection Agency Imposes 10 Million Euro Fine on Google*: *Highest Fine to Date*, CLIFFORD CHANCE: TALKING TECH (May 27, 2022), https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/05/spanish-data-protection-agency-imposes-10-million-euro-fine-on-g.html [https://perma.cc/6AWS-G7MC].

150. EDPB, OVERVIEW ON RESOURCES, Sept. 5, 2022, *supra* note 128, at 5.

151. *See* Lawson Mansell, *GDPR Fines Increasing, but Big Tech Companies Avoid Maximum Fines*, MILKEN INSTITUTE: TECH REGULATION DIGEST (Oct. 5, 2022), https://milkeninstitute.org/article/tech-regulation-digest-october-2022-gdpr [https://perma.cc/8FUQ-TPDQ].

152. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, YOUR RIGHTS MATTER: DATA PROTECTION AND PRIVACY: FUNDAMENTAL RIGHTS SURVEY 14 (2020), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf [https://perma.cc/T3EQ-XJRG].

153. *Id.* at 9.

3. Lack of Clarity from Judicial Intervention

The CJEU has sought to address disputes between DPAs. In the 2015 lawsuit against Facebook initiated by the Belgian DPA, the local authority sought to maintain its jurisdiction, despite the GDPR's one-stop-shop, in the face of the DPC's reluctance to take action.[154] The CJEU, in its landmark judgment in 2021, upheld the general rule of one-stop-shop, but stated that the supervisory authority (which is not the LSA) is not per se precluded from acting before domestic courts against a data controller or processor when the processing is cross-border in nature.[155] It further ruled that the LSA is obliged to take into account the views of other SAs, and that "any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority."[156] The result of this ruling is two-fold. First, it permits the Belgian DPA to continue in part its proceedings against Facebook. Second, it does not change the mandate that one-stop-shop applies to direct enforcement: The LSA is responsible for initiating investigations, launching court proceedings, and generally overseeing enforcement. Under this ruling, the LSA here, which is Ireland's DPC, is still afforded broad competence.[157] Otherwise, the court noted that the "objective[ness], and the effectiveness" of the mechanism may be "jeopardised."[158]

Commentators suggest that this decision may unleash a flood of investigations by various national DPAs against tech companies.[159]

---

154. Paraskevi Theofanous, *Facebook/Belgian DPA: the One-Stop-Shop Mechanism Questioned*, DPORGANIZER (Oct. 26, 2021), https://www.dporganizer.com/blog/facebook-belgian-dpa/ [https://perma.cc/ACR9-W64R].

155. Case C-645/19, Facebook v. Gegevensbeschermingsautoriteit, ECLI:EU:C:2021:483, ¶¶ 63–65 (June 15, 2021) [hereinafter Case C-645/19].

156. *Id*.

157. Heidi Waem and Simon Verschaeve, *EU: What's Left of the GDPR One-stop-shop? CJEU Clarifies the Competences of Non-lead Data Protection Authorities*, DLA PIPER: PRIVACY MATTERS (July 5, 2021), https://www.lexology.com/library/detail.aspx?g=60dea241-1b84-4c9f-b5ed-9012f29643ea [https://perma.cc/7EBX-XWAD].

158. Case C-645/19, ¶ 65 (June 15, 2021); *see also* Lokke Moerel and Ronan Tigner, *The CJEU did not rescind the one-stop shop. Quite the Opposite.*, INT'L. ASSOC. OF PRIVACY PROS. (July 1, 2021), https://iapp.org/news/a/the-cjeu-did-not-rescind-the-one-stop-shop-quite-the-opposite/ [https://perma.cc/R8WR-E295].

159. Foo Yun Chee, *EU data watchdogs ruling sharpens focus on Facebook, big tech*, REUTERS (June 15, 2021), https://www.reuters.com/world/europe/top-eu-court-says-national-watchdogs-may-act-against-violations-blow-facebook-2021-06-15/ [https://perma.cc/8DE9-QENN].

It also does not clarify how national authorities should assist and cooperate with each other in order to address the complaints effectively.[160] In response to the concern of under-enforcement raised by the Belgian DPA, the CJEU suggests existing mechanisms such as mutual assistance and urgency procedures may be undertaken when necessary.[161] However, considering that these mechanisms have rarely been invoked,[162] it is doubtful that they would be adequate to ensure robust enforcement or actually foster intra-regional communication. Therefore, the decision may in turn result in more fragmentation and uncertainty in the GDPR's enforcement and also substantially increase the costs of regulating multinational companies.[163]

Judicial developments aside, the task of enforcing the GDPR largely remains within the framework of one-stop-shop. By putting national authorities in charge of overseeing tech companies, the one-stop-shop has created a highly fragmented enforcement structure within the GDPR.

B. Identifying Divergence and Divisibility in Corporate Compliance

The fragmentation within GDPR enforcement has raised concerns over a mirrored compliance problem where affected companies are given the incentives and opportunities to circumvent the GDPR. Despite the upward trend in fines on Big Tech, none of the fines have yet to hit the maximum penalty permitted under law, which is 4% of the company's global revenue.[164] Compliance costs and fines are readily internalized by Big Tech as collateral damages and sunken costs of doing business. However, the damage to the companies' reputation and consumer confidence nevertheless creates an incentive to minimize exposure to the regulation and risk of legal liability. Furthermore, the commercial consequences of exiting Europe would entail

160. Theofanous, *supra* note 154.

161. Case C-645/19, ¶¶ 67–70 (June 15, 2021); *see also CJEU Advocate General Reinforces the GDPR's One Stop Shop,* HOGAN LOVELLS (Jan. 17, 2021), https://www.engage.hoganlovells.com/knowledgeservices/news/advocate-general-reinforces-the-gdprs-one-stop-shop [https://perma.cc/HR5J-V2LT].

162. *See* EDPB, *Contribution of the EDPB*, *supra* note 90, at 14.

163. Foo Yun Chee, *supra* note 159.

164. Mansell, *supra* note 151.

losing not only the regional market, but also EU-US data transfers, which even the largest tech companies could not afford.[165]

One of the criticisms of the one-stop-shop was the potential threat of forum shopping, where companies could flock toward friendly regulators.[166] However, in reality, tech companies have not engaged in this kind of forum shopping for the purposes of avoiding GDPR enforcement. These companies have chosen Ireland as their main establishment for tax considerations, rather than to evade the GDPR, so the lenient data privacy regulation they enjoy by virtue of establishing in Ireland is merely an ancillary benefit.[167] The unevenness and bottleneck in GDPR enforcement has thus, as a byproduct, allowed Big Tech companies to take advantage of the forum and avoid, or at least delay, liabilities without engaging in active forum-shopping.

Big Tech companies have also adopted strategies to bypass the GDPR by removing their user bases from the EU. In response to the announcement of the GDPR, Facebook—now Meta Platforms—moved 1.5 billion of its users in Africa, Asia, Australia, and Latin America outside the coverage of the regulation. [168] The affected users, whose data are now processed in the United States and other jurisdictions, are instead governed by more lenient privacy laws.[169] While Facebook pledges to apply the same privacy protections globally,[170] this move restricts the global reach of the GDPR and limits its impact to European users, who make up less than 20% of the platform's users

165. *See* Markus Reinisch, *Meta Is Absolutely Not Threatening to Leave Europe*, META (Feb. 8, 2022), https://about.fb.com/news/2022/02/meta-is-absolutely-not-threatening-to-leave-europe/ [https://perma.cc/3NAM-CYYG].

166. Natasha Lomas, *Europe's Top Court Unblocks More GDPR Litigation Against Big Tech*, TECHCRUNCH (Apr. 28, 2022, 11:14 AM), https://techcrunch.com/2022/04/28/cjeu-gdpr-consumer-litigation/ [https://perma.cc/P8VM-QDDQ].

167. *See* Ari Shapiro, *U.S. Tech Firms See Green As They Set Up Shop In Low-Tax Ireland*, NPR (Dec. 8, 2014, 4:16 AM), https://www.npr.org/sections/parallels/2014/12/08/368770530/u-s-tech-firms-see-green-as-they-set-up-shop-in-low-tax-ireland [https://perma.cc/GAV5-VA38].

168. David Ingram, *Exclusive: Facebook to Put 1.5 Billion Users Out of Reach of New EU Privacy Law*, REUTERS (Apr. 18, 2018, 8:13 PM), https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-change-user-terms-limiting-effect-of-eu-privacy-law-idUSKBN1HQ00P [https://perma.cc/C2HS-73FK].

169. *Id.*

170. *See What is the General Data Protection Regulation (GDPR)?*, META, https://www.facebook.com/business/gdpr [https://perma.cc/JWU8-M3FE] (last visited Nov. 28, 2023).

worldwide.[171] Other multinational tech companies have followed suit, including LinkedIn, which similarly moved its non-EU users from Ireland to the United States.[172]

The Brussels Effect may still be achieved, independent of enforcement from EU regulators, if companies opt to adopt uniform data privacy policies across jurisdictions. However, the strategy of reducing exposure to the GDPR adopted by tech companies highlights their ability to take advantage of the regulation's legal fragmentation. By "introducing divisibility through changes in its corporate structures,"[173] tech companies are able to maneuver around the GDPR and adopt jurisdictionally-tailored privacy policies despite the facial uniformity of their corporate policies in compliance with the GDPR. [174] Therefore, to make the Brussels Effect possible, the GDPR needs to be enforced consistently within the EU in order to provide incentives for companies to align their corporate policies with these mandates across the board.

III. ASSESSING SOLUTIONS TOWARDS A GLOBAL DATA PRIVACY STANDARD

The failure to implement the GDPR consistently within the EU has repercussions beyond Europe. It displays to the world the difficulty in pushing forth a uniform data privacy standard even within the EU, despite the fact that the region enjoys a relative degree of commonality from the Member States' historical, political, and economic alignment. It also puts into question the strength and credibility of the EU's regulatory power to govern beyond its territory. Lastly, it makes

171. Ingram, *supra* note 168. Ingram states that the change affects more than 70% of Facebook's 2 billion-plus members. As of December 2022, Facebook had 239 million users in the United States and Canada, 370 million users in Europe, and 1.52 billion users elsewhere. The 20% value provided in the accompanying text is estimated using this information.

172. Alex Hern, *Facebook moves 1.5bn users out of reach of new European privacy law*, THE GUARDIAN (Apr. 19, 2018, 7:03 PM), https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [https://perma.cc/Z2E3-HND2].

173. BRADFORD, *supra* note 10, at 145.

174. *See, e.g.*, *What is the General Data Protection Regulation (GPDR)?*, *supra* note 170; Chad Woolf, *All AWS Services GDPR Ready*, AWS SECURITY BLOG (Mar. 26, 2018), https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/ [https://perma.cc/2WRT-EMST]; *Google Cloud & the General Data Protection Regulation (GDPR)*, GOOGLE CLOUD, https://cloud.google.com/privacy/gdpr [https://perma.cc/H5EZ-3YGX].

uncertain the viability of data privacy standardization and the feasibility of governing data privacy across borders. Thus, the GDPR's intra-EU legal fragmentation reveals the broader challenge confronted by transnational data governance regimes that should be acknowledged as more than just a local or regional enforcement problem.

The current state of inconsistent application has put forward a central question: Is consistent regional enforcement a sufficient key to achieving a data privacy standard within and beyond the EU, and if so, is it attainable? It has certainly become clearer after five years that resolving the intra-EU enforcement problem serves as the necessary foundation for a global data privacy standard. This part explores the merits and drawbacks of proposed solutions to the current state of legal fragmentation under the GDPR, and concludes by drawing attention to the rifts between data privacy models of two other leading nations, the United States and China, that underlie the larger conundrum of regulating data privacy globally.

A. Evaluating Proposed Solutions

At the EDPS conference held in June 2022, Vera Jourová suggested three potential paths for the future of data protection. First, maintaining the status quo. Second, re-opening the GDPR for reform in a targeted manner with the aim to fix structural issues, including its centralization. And third, a targeted intervention, focusing in particular on the harmonization of laws amongst Member States.[175] She expressed preference for the third option, calling on the DPAs to generate solutions to improve cooperation and accelerate the processing of cross-border cases.[176] While European regulators and scholars have dismissed a complete reform of the GDPR or a replacement of the one-stop-shop, they have echoed the urgency of unifying data privacy practices within the EU.[177] Didier Reynders, the EU Justice Commissioner, delivered a similar sentiment, centering the discussion on improving the GDPR and rejecting the notion of a "crisis of enforcement" or an overhaul of the system altogether.[178] Three proposed initiatives

175. EDPS, THE FUTURE OF DATA PROTECTION, *supra* note 104, at 37.

176. NEIL HODGE, HOW EUROPE MOVES FORWARD WITH GDPR 4, (Compliance Week 2022), https://d6jxgaftxvagq.cloudfront.net/Uploads/q/m/s/exterrogdpr2022_814710.pdf [https://perma.cc/6EQ6-874F].

177. EDPS, THE FUTURE OF DATA PROTECTION, *supra* note 104, at 17.

178. Didier Reynders, Commissioner Reynders' speech on the "Future of Data Protection: Effective Enforcement in the Digital World" at the EDPS Conference (June 16, 2022), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_3796 [https://perma.cc/UQX2-TKGV].

have surfaced as potential solutions to guide future directions of data privacy regulation under the GDPR.

1. Expansion of Resource Allocation

Increasing the budget and staff of the DPAs will partially ameliorate the problem of under-enforcement and uneven enforcement of the GDPR[179] and will likely be one of the more feasible and easily implementable solutions. The resources necessary to regulate tech giants require not only the expansion of monetary investment in the national authorities and the governing institutions, but also a body of staff with sufficient technical expertise to enforce the legislation.[180] The increase in capacity will allow DPAs to more efficiently address complaints, conduct investigations, and use cooperation and communication tools on cross-border cases.[181] Past improvements in budget and staffing have been found to correlate to more robust enforcement efforts.[182]

The gap between the fines imposed by the DPAs and the resources of the companies penalized, however, will remain substantial. For instance, the market cap of Apple is $2.067 trillion as of December 30, 2022, despite losing $846.34 billion in value in the same year.[183] This dwarfs the second largest GDPR fine of €746 million (~$802 million) levied by the Luxembourg DPA. While ensuring that enforcement authorities are equipped with sufficient financial and technical resources is an important first step in addressing the burden-sharing problem between national authorities, the effective regulation of tech giants will likely continue to be challenging to regulators considering the companies' sheer sizes.

The initial allocation of budgets and human resources was determined based on the "differences in the scope of competencies, activities, and financial responsibilities at [a] national level" among

179. HODGE, *supra* note 176, at 3.

180. *Id.*

181. EDPB, OVERVIEW ON RESOURCES, Sept. 5, 2022, *supra* note 128.

182. DPC, *supra* note 123, at 11.

183. Alex Harring, *Apple and Amazon lost a 'staggering' $800 billion in market cap in 2022. Here's what that looks like*, CNBC (Jan. 3, 2023, 5:35 PM), https://www.cnbc.com/2023/01/03/apple-and-amazon-lost-a-staggering-800-billion-in-market-cap-in-2022.html [https://perma.cc/YC6F-BS2D].

Member States.[184] Despite the disproportionate regulatory responsibility on the Irish DPC, other nations including Germany, Italy, and Austria have larger allocations.[185]

To resolve this, the EDPB should monitor complaint levels within each jurisdiction in order to match the allocated resources to the enforcement demands. Expanded resources for local authorities will require a similar expansion in the EDPS's and EDPB's own budgets, which are determined by the European Parliament and Council's respective courts. The expansion in regulatory capacity therefore demands a concerted effort on the regional level—from both legislative and judicial branches—to dedicate more resources to data privacy protection.

2. Harmonization of DPAs and National Procedural Laws

The EDPB identified the development of a more robust and cohesive cooperation system between the DPAs and their national procedural laws as crucial to future enforcement collaboration.[186] The EU also included DPA harmonization as one of the key initiatives for its 2023 work program.[187] The DPAs have committed to further enhance cooperation on cross-border and strategic cases.[188] Increased transparency and collaboration between national authorities could be pivotal in partially mending the fragmentation of GDPR enforcement along jurisdictional lines. Similarly, the harmonization of national procedural laws will help minimize the friction between national practices and prevent local laws from hindering the enforcement of the GDPR. In the formal request sent to the EU Commission by the EDPB in Oc-

184. EDPB, *Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities*, 4–5 (Aug. 5, 2021), https://www.statewatch.org/media/3516/eu-edpb-overview-national-data-protection-resources-9-22.pdf [https://perma.cc/7TVA-RYR7].

185. *See id.*

186. *See* EDPB, *Statement on Enforcement*, *supra* note 100.

187. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2023: A Union Standing Firm and United*, at 13, COM (2022) 548 final (Oct. 18, 2022).

188. EDPB, *DPAs Decide on Closer Cooperation for Strategic Files* (Apr. 29, 2022), https://edpb.europa.eu/news/news/2022/dpas-decide-closer-cooperation-strategic-files_en [https://perma.cc/YEK7-XPYB].

tober 2022, the EDPB also identified the need to unify and align divergent national laws, including administrative procedures and cooperation procedures.[189]

Harmonization between national laws and authorities will require more than legislative efforts, as national divergences in current practices are rooted in cultural attitudes or political hurdles that are difficult to overcome in the short term. Additionally, any harmonizing measure is likely to come into conflict with the other important objective of the GDPR, which is to ensure the accessibility of national authorities to citizens and companies in their jurisdictions.[190] Legislators will need to write cohesive procedural rules that apply evenly across the region without eliminating jurisdictional flexibility. New directions urging the unification of national rules would inevitably demand compromises from the DPAs and local legislatures. It would require voluntary coordination between each Member State and their respective legislatures, as well as continuous monitoring from the European Commission and the EDPB to ensure national alignment. In order to preserve the local accessibility of GDPR implementation, regulators should retain the initial intake processes on the national level so that citizens may lodge their complaints locally. However, the procedures for such processes should be standardized amongst the DPAs. After the intake stage, regulators could consider a more centralized approach to resolving complaints when they are cross-border in nature.

3. A Pan-European Regulator?

Wojciech Wiewiórowski, the European data protection supervisor, in his keynote speech at the EDPS conference in June 2022, called for a "pan-European data protection enforcement model" as a necessary step to ensure data privacy across the EU.[191] Wiewiórowski vocalized his view that cross-border privacy cases at such a scale should be handled by EU watchdogs rather than national agencies.[192] Indeed, there have been demands for more centralization by "putting

189. *See EDPB*, *EDPB Letter to the EU Commission on Procedural Aspects That Could be Harmonized at EU Level* (Oct. 10, 2022), https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf [https://perma.cc/6L5D-XR6D].

190. *See* Reynders, *supra* note 178.

191. Wiewiórowski, *supra* note 18.

192. Foo Yun Chee, *Regulator Calls for Big Tech Privacy Cases to be Handled by EU Watchdog*, REUTERS (June 17, 2022, 4:24 PM), https://www.reuters.com/technology/regulator-calls-big-tech-privacy-cases-be-handled-by-eu-watchdog-2022-06-17/ [https://perma.cc/32UC-YTYS].

more enforcement power in the hands of one authority at the EU level."[193]

More centralized enforcement under a pan-European regulatory agency, in theory, would unquestionably alleviate the problem of uneven burden allocation to national authorities and improve intra-EU consistency. Regulating on the EU level would also resolve the differences between national procedural laws and allow uniformity in addressing complaints, conducting investigations, and issuing penalties. The EDPS already exists as the EU-level supervisor on data protection, and it could take on a larger leadership role in spearheading the regulation of Big Tech. Alternatively, scholars and legislators have pondered the possibility of an independent oversight agency at the EU level to regulate digital platforms and policies.[194]

However, as Reynders, the EU justice commissioner, wondered: "[W]ould centralisation bring concrete benefits to the citizens?"[195] National priorities and attitudes may not always be in alignment with those of the EDPB or other regulators, as the Irish DPC demonstrated in the Meta case. A shift of enforcement power from DPAs to a pan-European regulator is likely to be accompanied by diminishing levels of accessibility of local authorities and a lack of tailoring to the customs and needs of various jurisdictions. It would call for a new evaluation of the relationships between the national DPAs and an adjustment of their roles and responsibilities. The Member States may also be reluctant to cede their independent authority to a centralized regulator. Essentially, creating an EU-level regulator would be a "top-down exercise" of enforcing the GDPR's consistency within the region rather than one created by cooperation between national authorities from the bottom up.[196] It would demand a reform, or at the very least a drastic transformation, of the one-stop-shop and the enforcement structure of the GDPR. A pan-European approach would bring forth a united front to the rest of the world, but it would need to be consistently maintained. These new challenges under a pan-European model may outweigh its benefits and even backtrack the progress already made in the past five years by regulators on how to govern data privacy nationally and regionally under the GDPR.

193. Reynders, *supra* note 178.

194. EUROPEAN UNION, EDPS CONFERENCE REPORT: THE FUTURE OF DATA PROTECTION – EFFECTIVE ENFORCEMENT IN THE DIGITAL WORLD at 21 (2022), https://www.edpsconference2022.eu/sites/default/files/2022-11/22-11-10-EDPS-Conference-Report-2022_EN.pdf [https://perma.cc/P6AV-NT77].

195. Reynders, *supra* note 178.

196. *See id.*

B. Is Effective Enforcement Even Sufficient?

The proposed solutions assume that effective enforcement of the GDPR within the EU will fix the current deficiencies in the regulation and set the example of transnational data governance it was intended to create. This section argues that achieving global uniformity in data governance will require more than just uniform enforcement of the GDPR, though it is certainly an important step. Instead, a global data privacy standard will demand a more fundamental alignment between nations and jurisdictions financially, geopolitically, and ideologically.

The underlying forces that have led to the divergence and fragmentation in the GDPR's implementation are not unique to the European regulation. Arner and co-authors theorized about the "wicked" transnational data governance problem. They note that the governance styles of the three major and standard-setting economies—the United States, the European Union, and China—are fractured, and this results in a fractured global digital economy.[197] While the one-stop-shop's emphasis on the national dimension in GDPR enforcement has undoubtedly contributed to the lack of a European data privacy standard, the obstacles confronted by the GDPR should not be attributed merely to the fault of its designs or the problem of enforcement. Rather, they are emblematic of the larger problem that faces transnational data governance in wrestling with the tensions between global uniformity and jurisdictional specificity.[198]

Extending the analysis of the legal fragmentation confronted by the intra-EU application of the GDPR to a global scale reveals that the problem is rooted in issues beyond deficient legislative design or enforcement. The challenge of unequal burden sharing between national authorities is further magnified when applying the GDPR beyond the region. While the extraterritorial reach of the regulation has resulted in widespread GDPR-compliant corporate policies by multinational tech companies and non-EU legislations, data privacy and

197. *See generally* Arner et al., *supra* note 7.

198. *Compare* Giulia Gentile & Orla Lynskey, *Deficient by Design? The Transnational Enforcement of the GDPR*, 71 INT'L. & COMPAR. L. Q. 799, 800 (2022) (agreeing that the design and implementation of GDPR's decision-making procedures and consistency mechanisms have resulted in the shortcomings observed within the transnational enforcement of the GDPR) *with supra* Section I.A. (situating the regulation within the larger context of transnational data governance, connecting these causes of deficiency to beyond just the letter of the law and its enforcement, and suggesting that overhauling or reforming the OSS may not lead to consistency and will likely entail its own set of issues in ensuring the GDPR's national, regional, and cross-border implementation).

protection under the law is far from uniform in action. Local authorities, and in particular, those in low- and middle-income countries, have faced constraints in funding and technical expertise.[199] The Office of the Data Protection Commissioner (ODPC) of Kenya, for example, was allocated Ksh 50,000,000 (around $400,000) between 2021 and 2022, and was estimated to have expenditures of a similar amount over the two following years.[200] In contrast, the Irish DPC received a budget of €19.1 million (~$21 million) in 2021,[201] a figure that has been continuously expanded in the past years. Though the European authorities complain of insufficient resources, the under-capacity problem of non-EU enforcement authorities is significantly more dire when considering the substantial limitation in resources, both financial and technical, and the disparity between various economies in regulating the digital economy.

The divergence between national laws and cultures is similarly heightened between regions and countries beyond the EU, mirroring and enlarging discrepancies between national procedural laws and practices amongst EU Member States that have contributed to the GDPR's inconsistent regional implementation. While the European model has established data privacy as a fundamental human right, this is not a value that is historically or culturally familiar to other parts of the world.[202] The Beijing Effect,[203] as a competing force to the Brussels Effect, has sought to propel a state-based governance model that

199. *See* Michael Pisa & Ugonma Nwankwo, *Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development*, CENTER FOR GLOB. DEV., 2 (Aug. 9, 2021), https://www.cgdev.org/publication/are-current-models-data-protection-fit-purpose-understanding-consequences-economic [https://perma.cc/7R42-BTSA]; *see also* EDPS CONFERENCE, *supra* note 60.

200. THE REPUBLIC OF KENYA NATIONAL TREASURY, 2021/2022 ESTIMATES OF RECURRENT EXPENDITURE OF THE GOVERNMENT OF KENYA FOR THE YEAR ENDING 30TH JUNE, 2022, at 614 (2021), https://www.treasury.go.ke/wp-content/uploads/2021/05/FY2021-22-Recurrent-Expenditure-Vol-I-Votes-1011-1162.pdf [https://perma.cc/HE82-HVCV]; *see also* Bridget Andere, *Data Protection in Kenya: How is this right protected?*, ACCESS NOW (Oct. 2021), https://www.accessnow.org/cms/assets/uploads/2021/10/Data-Protection-in-Kenya.pdf [https://perma.cc/TH9C-BUB6].

201. Press Release, Data Protection Commission Statement on Funding in 2021 Budget, DPC, (Oct. 13, 2020), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget [https://perma.cc/BD2G-KJCC].

202. *See* EDPS CONFERENCE, *supra* note 60.

203. Professor Bradford has argued that China is unlikely to bring about a Beijing Effect in the near term despite its market size, due to its limited regulatory influence over other jurisdictions and digital economy companies alike. *See* BRADFORD, *supra* note 10, at 266. However, the China Personal Information Protection Law (PIPL), put into effect in November 2021, suggests the country's ambition in emulating the EU and the GDPR in setting standards

approaches data privacy as a tool of data sovereignty.[204] In contrast, the United States has largely followed a market-based approach.[205] The differences between global conceptions of data privacy informed by distinct national cultures, histories, and political systems consequently create larger pushbacks against standardization in the implementation of transnational data governance legislations.[206] Furthermore, the difficulty of communication and cooperation between jurisdictions and setting up a system of robust judicial review is compounded when envisioning transnational data governance beyond the EU.

The twin aims of the GDPR of ensuring regional consistency while allowing national specificity are thus similarly reflected in considering transnational data governance at large, beyond the scope of the European regulation. Data governance on a global scale requires the parallel considerations of standardizing data privacy and protection across jurisdictions while leaving room for adaptability to national capacities and customs. It also raises implications of national security and digital sovereignty.[207] While the one-stop-shop has been faulted

in data privacy. *See* Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [PRC Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) http://www.xinhuanet.com/politics/2021-08/20/c_1127781552.htm [https://perma.cc/72J7-9X6G]; *see also* Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance,* 54 N.Y.U. J. INT'L L. & POL. 1, 21–23 (2021) (hypothesizing other mechanisms through which China may exert influence on foreign data governance regimes and arguing that China already imparts a Beijing Effect, one that is distinct from the Brussels Effect and likely to grow, and will therefore expand its regulatory effect on transnational data governance).

204. *See generally* Erie & Streinz, *supra* note 203.

205. *See* Arner et al., *supra* note 7, at 658.

206. *See id.* at 623–33 ("As idiosyncrasies solidify, the extraterritorial application of domestic rules reinforces the incompatibility of governance styles… As data governance styles harden into conflicting, competing, non-interoperable transnational data governance regimes, national interests clash, and international coordination becomes even more difficult. Instead of aiming to work within a global internet-based data system, jurisdictions strive to change its parameters, with material consequences for the global data economy and globalization more broadly. This includes, for example, increasing transaction costs through additional compliance requirements within supply and value chains, or the total breakdown of data transmission that can disconnect commercial, financial, or other markets.").

207. *See, e.g.*, UNITED NATIONS SYSTEM CHIEF EXECUTIVES BOARD FOR COORDINATION, *INTERNATIONAL DATA GOVERNANCE: PATHWAYS TO PROGRESS* 4 (2023) ("Data governance have evolved in a fragmented and uncoordinated manner resulting in different approaches to governing data, with some regions focusing on protecting individual data, others on maximizing profit from data or using data to control societies in the name of national security."); *see also*

as a design within the GDPR that has partially led to its inconsistent enforcement, it has also served as a microcosm of the inherent challenge of governing global data privacy and coordinating between fragmented jurisdictions, economies, and legislations. Therefore, effective enforcement will only serve as a necessary but not sufficient fix to the problem confronted by the GDPR.[208] Without aligning the fundamental approaches of data privacy governance in various countries and regions, or at least finding a middle ground, any attempt to regulate transnational data flows will only further expose the geopolitical tensions, economic disparities, and ideological rifts among nations, just as the GDPR has done within the EU.

C. Recognizing the Lack of a Data Privacy Consensus

By targeting effective enforcement within the region, the proposed solutions by the EU regulators may ameliorate the legal fragmentation within the EU. However, they expose the magnified problem of digital and legal fragmentation confronted by transnational data governance schemes that have thus far been unable to attain global compliance. While a sweeping European data protection regulation has been enacted due to the regulation-intense history of the EU, is global data governance unity possible absent the historical and political alignment that the EU as a region has enjoyed?[209] As the leading world powers, notably the EU, United States, and China, continue to develop and expand their efforts in regulating technology companies

---

Erie & Streinz, *supra* note 203, at 4 (arguing that the theme of data sovereignty has been invoked often in the context of China and its internal regulatory scheme in order to justify the exertion of governmental control over data flows); BERTRAND DE LA CHAPELLE & LORRAYNE PORCIUNCULA, INTERNET & JURISDICTION POL'Y NETWORK, WE NEED TO TALK ABOUT DATA: FRAMING THE DEBATE AROUND FREE FLOW OF DATA AND DATA SOVEREIGNTY 1, 3 (2021) (arguing that while free flow of data has been championed by many as enabling digital transformation and innovation as well as social and economic benefits, notions of data sovereignty have raised concerns related to privacy, taxation, competition, security, and even the democratic process).

208. *See* Arner et al., *supra* note 7, at 680 ("To ensure cross-border digital connectivity, allowing data flows to move outside domestic borders, there must be a minimum level of harmonization of infrastructures and technical standards. Yet, current trends include the decoupling and the duplication of technological infrastructures, the definition of different technical standards, and the compartmentalization of contents within domestic borders as a result of the emergence of competing, non-interoperable, and increasingly conflicting data governance regimes across major economies, combined with their external export, resulting in fragmentation of transnational data governance.").

209. *See also* EDPS CONFERENCE, *supra* note 60.

and the digital spaces they occupy, the tension and potential incompatibility between each nation's approaches and legislations have surfaced.[210] The mismatch between their philosophies, resources, and models will continue to magnify and trifurcate the landscape of global data privacy.

The World Bank has long discussed the phenomenon of uneven distribution of digital dividends, i.e., the broader developmental benefits from using digital technologies in many parts of the world.[211] A similar analysis can be extended to the realm of data privacy. For countries to equally reap the benefits of transnational data governance, they will need to be equipped with adequate resources, expertise, laws, and institutions. Much like the lessons observed from the GDPR, efforts of data privacy capacity-building within national authorities will only falter and fail to impart a uniform privacy standard absent a consensus on cultural and political attitudes amongst jurisdictions. Governing cross-border data privacy requires an urgent recognition of the rifts between national philosophies and regulatory models that have in turn resulted in increasingly divisive digital empires. It demands a willingness, especially by the leading nations, to adapt and accommodate these differences to prevent the further fragmentation of the global digital economy and to regulate technology and data effectively and uniformly.

CONCLUSION

Five years after the GDPR went into effect, its promise of propagating a European culture of data protection and setting a global data privacy standard remains unfulfilled. While regulators have narrowed their focus to effective regional enforcement, the obstacles confronted by the GDPR can find their roots in the problem within transnational data governance at large—that of reconciling the ideological, economic, and geopolitical differences between jurisdictions and economies.[212]

The tension and competition between the leading powers to regulate global technologies and data networks have become a reality

210. *See* Arner et al., *supra* note 7, at 660–676 (discussing various aspects of differences between the United States, EU, and China with regards to digital sovereignty, extraterritorialization and internalization, and data securitization).

211. *See generally* WORLD BANK GROUP, WORLD DEVELOPMENT REPORT 2016: DIGITAL DIVIDENDS (2016), https://www.worldbank.org/en/publication/wdr2016 [https://perma.cc/V63T-VNMD].

212. *See generally* Arner et al., *supra* note 7.

that nations, companies, and citizens will have to confront. The new EU-U.S. Data Privacy Framework, launched in July 2023, allows businesses to transfer data from the EU to the United States in a secure and GDPR-compliant way[213] and suggests the possibility of a reconciliation between the two nations in their data governance schemes. However, the agreement has already drawn criticism for the potential under-protection of non-U.S. citizens.[214] While scholars have debated whether China has sufficient regulatory power or mechanisms to exert such an influence over foreign data governance regimes,[215] the nation has put forth its own regulatory model for data privacy and displayed its standard-setting ambition with the publication of the PIPL in 2021.

Establishing a global data governance regime would require significant infrastructural and institutional support and face substantial economic and political hurdles. It would demand the support of collaboration between jurisdictions involved in order to adequately and equitably resolve cross-border cases. In practice, the question of how to reconcile the Brussels Effect with the Washington Effect or the Beijing Effect remains murky in an age of geopolitical divisiveness. To answer such a question goes beyond the singular capacities of EU regulators, or their American and Chinese counterparts.

Yiran Lin[*]

213. *See* European Commission, *Questions & Answers: EU-US Data Privacy Framework*, (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752 [https://perma.cc/EHR3-NCFJ].

214. *See* Ryan Browne, *Europe and the U.S. finally agree a landmark data-sharing pact—and it's already under threat*, CNBC, (July 12, 2023, 5:53 AM), https://www.cnbc.com/2023/07/12/eu-and-us-agree-new-data-sharing-deal-what-is-it-and-why-it-matters.html [https://perma.cc/EQ68-YSY8].

215. *See* discussion *supra* note 203.

[*] J.D. Candidate, Columbia Law School, 2024. Thank you to Professor Anu Bradford for her immensely illuminating guidance and insights on this Note; and to the editors and staff of CJTL for their diligent and meticulous editorial work.