DATA PRIVACY REGULATION'S IMPACT ON THE GLOBAL DIGITAL INNOVATION ECONOMY: AN ANALYSIS OF INTERNATIONAL REGULATORY EFFECTS ON THE TECHNOLOGY INDUSTRY

Lucas V. Di Lena[†]

ABSTRACT

This work aims to discuss the genesis of data privacy regulation and how it has impacted the overall international digital economy. Namely, how the regulatory framework present in today's society has developed, sparking action by nations including the European Union, United States, and the United Kingdom to police the use of their citizens' data. As each individual country developed their own national laws regarding data privacy, various impacts were felt by companies operating internationally, as well as domestically in their efforts to grow.

A discussion on the disparate impacts across the technology sector as a whole will review how both large and small technology companies have been and continue to be subject to regulation which brings positive and negative results. Particularly, the regulatory framework has grown increasingly complex with each individual nation proffering its own regulations which depart at various junctures. Small and midsized enterprises have experienced harmful impacts from these regulatory frameworks, with larger enterprises notably better equipped to handle these changes.

As the landscape for data privacy protections and the protection of an individual's right to privacy has become a key point at the core of these regulations, an important balancing test must be struck between liberty and the stifling of innovation. Overly complex regulation has impacted the mergers and acquisition space, a strong tool utilized in the technology sector to foster innovation and the further development of novel technology. With an ever-growing market in the technology sector based on artificial intelligence, some countries stand at a disadvantage from an investment and innovation perspective given their approach to regulation.

[†]*J.D. Candidate, Syracuse University College of Law, Class of 2024.* *A special thank you to the professors who contributed their time in helping to develop this note, namely, Professor Emily Brown and Professor Shuba Ghosh. An additional thank you to my Syracuse University colleagues and the members of the Syracuse University Journal of International Law and Commerce for their tireless efforts, insight, and encouragement.*

INTRODUCTION

How data privacy is regulated and what laws will govern how individuals' personal data is used, processed, and ultimately monetized is one of the most hotly debated topics this century across the globe.[1] Companies face heightened levels of scrutiny and corporate challenges specific to their profitability and ability to provide services to their customers, including Citymapper.[2] Citymapper, a UK startup with a goal of providing users with a new means to city navigation, amassed close to fifty million users before facing revenue generation issues and a clear route to profitability.[3] The route usually taken, that of amassing millions of data points on customers and ultimately selling or monetizing that data, is one that the startup could not achieve in light of the infamously wide-reaching European Union ("EU") data privacy regulation, the General Data

1. Astrid Gobardhan, *Data Privacy Trends to Follow for 2023*, INFORMATIONWEEK (Jan. 26, 2023), *available at* https://www.informationweek.com/big-data/data-privacy-trends-to-follow-for-2023 (last visited Mar. 18, 2024).

2. Margaret Taylor, *How to Save Citymapper*, WIRED (May 26, 2021), *available at* https://www.wired.co.uk/article/how-save-citymapper (last visited Mar. 18, 2024).

3. *Id.*

Privacy Regulation ("GDPR").[4] Facing issues to monetize, Citymapper eventually failed, accumulating millions in losses and frustrating investors keen on pulling back their investments after seeing poor routes to profitability.[5] Here lies a large problem when approaching wide-reaching legislative movements toward regulating large industries–disparate impacts. The highly complex global regulatory framework on data privacy and artificial intelligence ("AI") has stifled innovation by adding ineffective, burdensome complexities to the mergers and acquisitions process, most of which disproportionately impact smaller and midsize organizations.

I. THE GENESIS OF DATA PRIVACY REGULATION

Privacy, a concept once defined as the "right to be left alone" by two American lawyers at the turn of the century, has now come to permeate all facets of everyday life in the modern age.[6] In 1948, the Universal Declaration of Human Rights was adopted, which formalized a framework of universal human rights that the global community believed were fundamental to human life, including the right to privacy.

Over the last 100 years, this fundamental right began to shift and take a more modern shape as technology and innovation infused the lives of citizens across the world.[7] Governments and companies amassed information and data on individual citizens, all of which could be considered intrusive as private citizens lacked control of and visibility into this information. Granted, in the mid-20th century, technology was far from the level of sophistication it has achieved today, and the stakes were lower, with respect to the value of transmission and control of personal information. However, in 1967, the United States ("U.S.") led the charge on access to and protection of information by passing the Freedom of Information Act ("FOIA").[8]

FOIA provided everyone the right to request access to documents from state and federal agencies that were related to, concerning, or

---

4. *Id.*

5. *Id.*

6. International Network of Privacy Law Professionals, *A Brief History of Data Protection: How Did It All Start?*, INPLP (July 10, 2020), *available at* https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/ (last visited Mar. 18, 2024).

7. The Economist, *The Roaring 20s?: Why a Dawn of Technological Optimism Is Breaking*, THE ECONOMIST (Jan. 16, 2021), *available at* https://www.economist.com/leaders/2021/01/16/why-a-dawn-of-technological-optimism-is-breaking (last visited Mar. 18, 2024).

8. International Network of Privacy Law Professionals, *supra* note 6.

encompassing their own personal information.[9] Following FOIA's adoption, other countries began to follow suit by providing similar frameworks to allow citizens to access data as the flow of data between various entities; both public and private, became more common across society.[10]

During the 1980s, the Organization for Economic Cooperation and Development ("OECD"), an intergovernmental organization with thirty-eight member countries, focused on stimulating economic progress and world trade, issuing guidelines on data protection as a reaction to the increasing use of computers to process business transactions.[11] The OECD set forth guidelines on the Protection of Privacy and Transborder Flows of Personal Data, acknowledging the importance of transborder data flows.[12] With the rise of computer-reliant banking and insurance industries, it became necessary to ensure the free flow of data across international borders but presented the challenge of balancing privacy interests with economic influences.[13]

The EU realized that despite the guidelines issued under OECD, they were merely guidelines and therefore inherently non-binding.[14] As technology continued to advance, becoming more entrenched in everyday life, the first major European privacy and human rights directive, European Data Protection Directive ("DPD"), took effect on December 13, 1995.[15] As a policy directive, the DPD was aimed at protecting individuals concerning the processing of personal data and the free movement of such data. As a directive, and not a regulation, EU member states were encouraged to follow this directive and implement the corresponding provisions outlined therein as national laws by October 24, 1998.[16]

---

9. *Id.*

10. *Id.*

11. *Ratification of the OECD Convention, Organisation for Economic Co-operation and Development*, OECD, *available at* https://www.oecd.org/about/document/ratification-oecd-convention.htm (last visited Mar. 18, 2024).

12. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development* ORG. FOR ECON. COOP. AND DEV., *available at* https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum (last visited Mar. 18, 2024).

13. *Id.*

14. Nate Lord, *What Was the Data Protection Directive? The Predecessor to the GDPR*, DIGIT. GUARDIAN (July 12, 2018), *available at* https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr (last visited Feb. 19, 2024).

15. Ernst-Oliver Wilhelm, *A Brief History of the General Data Protection Regulation,* INT'L ASSOC. OF PRIV. PRO. (Feb. 2016), *available at* https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/ (last visited Mar. 18, 2024).

16. Directive 94/46/EC, 1995 O.J. (L 281) 31.

Following the DPD, EU member states began to define what personal data encompassed and enacted regulatory structures within each member state to create a compliance framework to protect all EU citizens and their data.[17] Under Article 2(a) of the Data Protection Directive, EU member states were to define personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified directly, or indirectly, in particular by reference to an identification number or to one or more factors special to his physical, mental, economic, cultural or social identity."[18] Put simply, the DPD established protections for data where if any information, taken in the aggregate, could be linked back to any particular person.

Some of these changes directly affected categories of data, including names, government-issued identification numbers, credit card numbers, bank statements, and addresses traceable to any private citizen.[19] The DPD defined personal data and established a requirement for companies and actors who leverage personal data to have "data controllers." These data controllers are responsible for notifying governing bodies of the purpose of their data processing, providing contact information, listing categories of data subjects, identifying types of data collected, specifying who can view the data, indicating whether or not the data will be transferred to other countries, and outlining what protective measures have been put in place to ensure the security of the processed data.[20]

Despite the implementation of the DPD across EU member states, international considerations necessitated other protections in moving toward a framework that balanced protection of EU citizen data with the need to ensuring free flows of data from the EU to other countries.[21] On July 26, 2000, the United States and the EU achieved this goal and agreed upon a mechanism that would provide for "adequate level[s] of protection" required by the DPD.[22] This agreement was codified by the United States Department of Commerce and arrived on the heels of the DPD.

---

17. Lord, *supra* note 14.

18. *Id.*

19. *Id.*

20. *Id.*

21. Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, BROOKINGS (October 1, 2015) *available at* https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf *(*last visited Mar. 18, 2024).

22. Martin A. Weiss & Kristin Archick, CONG. RSCH SERV., R44257, U.S. EU DATA PRIV.: FROM SAFE HARBOR TO PRIV. SHIELD, (2018), *available at* https://sgp.fas.org/crs/misc/R44257.pdf (last visited Mar. 18, 2024).

Named the "Safe Harbor Privacy Principles Agreement" ("Safe Harbor Agreement"), it was implemented and subsequently recognized by the European Commission.[23]

The Safe Harbor Agreement established the mechanism that balanced the privacy of EU citizens with the need to ensure free flows of data across transatlantic borders. To achieve this, the Safe Harbor Agreement provided a method for companies based in the United States to self-certify annually to the Department of Commerce that the seven principles (required by the DPD) and other related requirements conformed with the data privacy adequacy standards.[24] These seven principles of the DPD included notice, onward transfer, security, data integrity, access, enforcement, choice (opt-out or opt-in for sensitive information.)[25] The Safe Harbor Agreement protected United States companies and the growth of the digital economy for roughly two decades as the cornerstone of companies' compliance with international data privacy regulations.[26]

However, this cornerstone may not have been as strong a foundation as envisioned. The Safe Harbor Agreement faced harsh criticism from European privacy advocates who believed it facilitated significant data protection loopholes, poor implementation, and a lack of oversight.[27] These complaints were paired with issues of false compliance claims by U.S. corporations and non-mandatory annual compliance checks.[28] These claims evidenced hundreds of companies that fraudulently claimed they had properly registered and adhered to the Safe Harbor Agreement framework.[29] In addition to issues with compliance, oversight was also thought to be inadequate. The Federal Trade Commission ("FTC") only brought enforcement actions against thirty-nine companies over the course of the first thirteen years of the Safe Harbor Agreement.[30] This paradigm of prioritizing the flows of data at the cost of potential inadequacies in the protection of personal data laid the foundation for a shift

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. Weiss & Archick, *supra* note 22.

28. *Id.*

29. Nikolaj Nielsen, *Hundreds of U.S. Companies Make False Data Protection Claims*, EUOBSERVER (Oct. 8, 2013) *available at* https://euobserver.com/rule-of-law/121695 (last visited Mar. 18, 2024).

30. *FTC Privacy and Security Report*, FED. TRADE COMM'N (2020), *available at* https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf (last visited Mar. 18, 2024).

in the European Union's approach to data privacy. As a result, the General Data Protection Regulation brought sweeping changes to global data flows and privacy regulation across global markets.[31]

Following years of debate, on April 27, 2016, the European Commission adopted the GDPR, with enforcement beginning on May 25, 2018.[32] The DPD was implemented at a time where the internet was in its infancy and OECD member states agreed to prioritize functional data flows and prioritize economic growth and development. Therefore, regulatory changes would likely be inevitable. With the adoption of GDPR came the most expansive changes to any privacy policy to date, and with it, a threat to innovation in the technology sector. [33]

Primarily, the GDPR changed the definition of personal data, expanding the DPD definition to include: any information that could be used, on its own, or in conjunction with other data, to identify any individual.[34] This new definition reflected the changes in more modern technology such as IP addresses, mobile device identifiers, geolocation, and biometric data, as well as any data related to an individual's physical psychological, genetic, mental, economic, cultural, or social identity.[35] As technology matured and allowed for companies based in countries outside of the EU to harness and capitalize on user data across international borders, it became imperative to establish more stringent data controller or processor requirements. These requirements were enforced regardless of the company's location.[36] Further, with the bark of the GDPR came the bite of the EU, which created high financial penalties for failure to comply with the GDPR. In the event a company was found to be in breach of the GDPR, that fine could reach up to €20 million, or four percent of the total global annual turnover a company earned in the preceding fiscal year.[37]

---

31. Samantha Beaumont, *The Data Protection Directive versus the GDPR: Understanding key changes,* SYNOPSYS (Jan. 18, 2018), available at https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/ (last visited Mar. 18, 2024).

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. He Li et al., *The Impact of GDPR on Global Technology Development*, J. OF GLOB. INFO. TECH. MGMT. (2019), *available at* https://www.tandfonline.com/doi/pdf/10.1080/1097198X.2019.1569186?cookieSet=1 (last visited Mar. 18, 2024).

37. *Id.*; Ben Wolford, *What are the GDPR Fines?*, PROTON AG, *available at* https://gdpr.eu/fines/ (last visited Mar. 18, 2024).

Outside of the direct financial penalties for noncompliance, it also established new mechanisms to empower EU citizens. Under the GDPR, companies were required to offer EU citizens robust privacy rights such as, the right to be forgotten, the right to access data, the right to data portability, and the right to explanation of automated decision-making.[38]

II. DATA PRIVACY REGULATION CROSSES INTERNATIONAL BORDERS BRINGING ADDITIONAL COMPLEXITY

Following the implementation of the GDPR, countries outside of the EU began to model data privacy regulations on the GDPR and make strides towards protecting citizens digital privacy rights.[39] Shortly after the GDPR was passed and implemented, other countries followed suit in implementing data privacy regulation; namely, individual states in the United States.[40] In the U.S., California pioneered the effort to create state-level legislation to provide residents of California rights similar to those created for EU citizens under the GDPR.[41] Both regulations take similar steps to ensure companies take appropriate measures to safeguard data they collect and use, however, they differ slightly in their approaches.[42] The GDPR takes a much more detailed approach on implementation of data protection standards, as well as the efforts companies must take to achieve compliance with the GDPR.[43] Where the GDPR, as its namesake, acted as the pioneer in the global data privacy regulation forum, other regions followed suit.[44] California went a step further in passing the California Privacy Rights Act ("CPRA") which transferred rulemaking authority from the California Attorney General to the

38. Li, *supra* note 36.

39. *California Consumer Privacy Act (CCPA)- an overview* USERCENTRICS (Aug. 5, 2021), *available at* https://usercentrics.com/knowledge-hub/california-consumer-privacy-act/#:~:text=The%20California%20Consumer%20Privacy%20Act%20(CCPA)%20was%20the%20first%20data,effect%20from%20January%201st%2C%202023 (last visited Mar. 18, 2024).

40. *Id.*

41. *Id.*

42. *Id.*

43. Danielle Kucera, *CCPA vs. GDPR: Similarities and Differences Explained*, OKTA (Apr. 13, 2021), *available at* https://www.okta.com/blog/2021/04/ccpa-vs-gdpr/ (last visited Feb. 15, 2024).

44. *How GDPR Changed the World, and Privacy Regulation's Future*, KASPERSKY (Dec. 15, 2021), *available at* https://kfp.kaspersky.com/news/how-gdpr-changed-the-world-and-privacy-regulations-future/ (last visited Mar. 18, 2024).

California Privacy Protection Agency.[45] Acting in effect as the United States' first formally codified expansive data privacy protection law, other states began to follow in California's footsteps, including Virginia, Connecticut, and Colorado which presently are in effect.[46] However, in addition to those four states, an additional nine states have also passed data privacy laws which will take effect during the second half of 2024, and some in early 2025.[47] As thirteen states have passed comprehensive privacy legislation, as of February 9, 2024, an additional seventeen states have active bills of varying scope regarding privacy and data protection presently working their way through respective state legislatures.[48]

It is important to note the differences in how each of these governmental bodies have approached data privacy regulation in their own respects. Despite taking cues from the EU and their passage of the GDPR, California defined the scope of its privacy laws in a slightly different manner, protecting "consumers," i.e., natural persons who are California residents, rather than "data subjects" or any identifiable person who resides in the EU.[49] Taking this a step further, the CCPA was drafted to direct the regulation of businesses, specifically, any for-profit organization in California, processing the personal information of California-based consumers.[50]

With a seemingly larger scope targeting businesses directly, and not that of data controllers and data processors, like the GDPR, the CCPA

---

45. *CCPA vs. CPRA: What's the Difference?*, BL (Jan. 23, 2023), *available at* https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ (last visited Mar. 25, 2024).

46. Mark Smith, *Analysis: Five Subtle Ambiguities in Virginia's New Privacy Law*, BL (June 9, 2021), *available at* https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-five-subtle-ambiguities-in-virginias-new-privacy-law (last visited Mar. 25, 2024); *What is the Virginia Consumer Data Protection Act (VCDPA)?*, BL (Dec. 28, 2022), *available at* https://pro.bloomberglaw.com/brief/what-is-the-vcdpa/ (last visited Mar. 25, 2024); *See* F. Paul Pittman, *US Datq Privacy Guide*, WHITE & CASE (March 22, 2024), *available at* https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide#:~:text=Currently%2C%20a%20total%20of%20thirteen,Montana%2C%20Oregon%2C%20and%20Delaware (last visited Mar. 25, 2024).

47. States such as Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, and Delaware have also passed laws but will not take effect until mid-2024 and early 2025. *See* F. Paul Pittman, *US Data Privacy Guide*, WHITE & CASE (March 22, 2024), *available at* https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide#:~:text=Currently%2C%20a%20total%20of%20thirteen,Montana%2C%20Oregon%2C%20and%20Delaware (last visited March 25, 2024).

48. *See* Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (March 22, 2024), *available at* https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited March 25, 2024).

49. Kucera, *supra* note 43.

50. *Id.*

established three thresholds where one of which must apply to be subject to the CCPA.[51] These thresholds include: $25 million dollars or more in gross annual revenues; the purchase, sale, sharing or receipt of personal information of 50,000 or more consumers, households or devices; or the company derives at least 50% of gross revenue from the sale of consumers' personal information.[52] The ability for a business to use and process personal data is automatic under the CCPA, as long as there is a clear option provided for consumers to opt out of the sharing of their personal information.[53] In contrast, under the GDPR, to process personal data, an organization must meet at least one of the six legal principles of consent, contract, legal obligation, vital interests, public task, or the more flexible lawful basis, a legitimate interest.[54]

When discussing these two wide-reaching data privacy regulations, enforcement is governed by various bodies and varies country by country. In California, the CCPA was recently bolstered by the passage and enactment of a subsequent data privacy regulation, the California Privacy Rights Act, which provides Californians with a formalized separate state regulatory body with data privacy enforcement powers that may pursue enforcement.[55] The CPRA became operative on January 1, 2023, at which point it vested and transferred power in the California Privacy Protection Agency granting "full administrative power, authority, and jurisdiction to implement and enforce" the CCPA.[56]

The state-level privacy regulations enacted across the U.S. have sparked a movement at the federal level prompting members of Congress to begin the arduous process of crafting federal regulation on data privacy.[57] Enter the American Data Privacy and Protection Act ("ADPPA"), an omnibus federal privacy bill that garnered significant bipartisan support, but faced objection from state level actors who believed it may not

51. *Id.*

52. *Comparing privacy laws: GDPR v. CCPA,* DATA GUIDANCE & FUTURE PRIV. F. (2018), *available at* https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (last visited Mar. 25, 2024).

53. *Id.*

54. Kucera, *supra* note 43.

55. Bloomberg Law, *supra* note 45.

56. *Id.*

57. Niketa K. Patel et al., *The American Data Privacy and Protection Act: Is Federal Regulation of AI finally on the Horizon?*, MAYER BROWN (Oct. 21, 2022), *available at* https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/the-american-data-privacy-and-protection-act-is-federal-regulation-of-ai-finally-on-the-horizon (last visited Mar. 25, 2024).

go far enough as a federal regulation.[58] This backlash comes primarily from California advocates, lobbyists, and government officials who believe that the ADPPA does not go far enough to protect Californians.[59] A federal law will usually govern a conflict involving state and federal disputes.[60] Preemption is at the core of this data privacy regulation dispute in the U.S. today, as the members of Congress seek to enact sweeping legislation at the federal level which would drive the U.S. closer to a level playing field across the global data privacy regulatory framework.[61] The ADPPA would act as a much larger scale piece of legislation that goes much further than the CCPA by shifting the burden of information protection to those who process data, rather than who generates it.[62] Further, the ADPPA also extends a much broader individual right to sue under the ADPPA whereas the CCPA currently provides this right to only Californians.[63]

Notably, the CCPA in its current form "only requires that businesses notify individuals of the information they collect and the purposes for which they use it, and to use it in ways 'reasonably necessary and proportionate to achieve the operational purpose for which it was collected or processed.'"[64] On the other hand, the ADPPA goes further to limit data collection to only what is "reasonably necessary and proportionate." This may impose limits on the information that companies can collect from individuals, bolstering the inherent right to privacy these regulations seek to protect in the first instance.[65] With a battle set to begin among lobbyists, non-profit organizations rooted in the data privacy space, and Congress as a whole, there is a long road ahead before the U.S. is able to firmly add a layer of complexity to the global data privacy regulatory framework. This ultimately will lead corporations to make some assumptions regarding their data privacy practices when navigating their path to profitability.

---

58. Cameron F. Kerry, *Will California be the Death of National Privacy Legislation?*, BROOKINGS (Nov. 18, 2022), *available at* https://www.brookings.edu/blog/techtank/2022/11/18/will-california-be-the-death-of-national-privacy-legislation/ (last visited Mar. 25, 2024).

59. *Id.*

60. *Preemption*, CORNELL LAW SCH. LEGAL INFO. INST., *available at* https://www.law.cornell.edu/wex/preemption (last visited Mar. 25, 2024).

61. Kerry, *supra* note 58.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

Global data privacy regulation still saw further degrees of complication where large geopolitical changes like the United Kingdom's ("UK") exit from the EU resulted in a need for the UK to bring their own regulatory shade to international data transfers.[66] Following the complex geopolitical move of the UK leaving the EU, or "Brexit," this necessitated a large scale shift in many regulations and laws governing the UK, and for the purposes of this endeavor, the UK's adopted their own General Data Privacy Regulation..[67] Initially taking a similar approach to that of the EU GDPR, the UK modeled much of their version upon the pioneering nations of the EU.[68] After the UK widely adopted the EU's GDPR, the UK went further to pass the Data Protection Act of 2018 ("DPA") which bolstered the UK GDPR to ensure that all rules under the original EU GDPR would be followed in other sectors where it did not originally apply.[69] For example, the UK DPA established requirements for data protection officers, as well as an Information Commissioner who enforces, supervises, and regulates the UK GDPR.[70]

With all these privacy acts in force today, there is a complex regulatory system that companies must be aware of, and in compliance with, to avoid harsh penalties.[71] Companies interested in operating within the United States or globally have been forced to comply with all these privacy acts across international borders, which creates a complicated web of data privacy regulations and potential penalties. Though these privacy acts differ in their breadth and scope, a trend has emerged across the global stage that has thrust policing and safeguarding of customer and user data to the forefront of the technology sector.[72]

---

66. Itgovernance, *Data Protection and Brexit: How the UK's Withdrawal from the EU Affects Data Protection in the UK: the EU GDPR, UK DPA 2018, and UK GDPR*, ITGOVERNANCE (2023), *available at* https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr (last visited Mar. 25, 2024).

67. *See The Data Protection Act*, GOV. UK, *available at* https://www.gov.uk/data-protection (last visited Mar. 25, 2024).

68. Itgovernance, *supra* note 66.

69. GDPR EU, *How Do the UK's GDPR and EU's GDPR Regulation Compare?*, GDPR EU, *available at* https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/ (last visited Mar. 25, 2024).

70. *Id.*

71. Laura Jehl & Alan Friel, *Comparison Chart: GDPR, CCPA, and Other State Privacy Laws*, BAKER & HOSTETLER LLP, (July 2019), *available at* https://perma.cc/7LZW-FR6J, (last visited Mar. 25, 2024).

72. Kaspersky, *supra* note 44.

III. MERGERS AND ACQUISITIONS IN THE TECHNOLOGY SECTOR UNDER GDPR

The array of international data privacy regulations present and applicable to the technology industry subjects both large and small organizations, operating globally, to varying regulatory schemes from many different countries. What originated under the EU's approach with the GDPR, eventually blossomed into a bouquet of data privacy regulations from EU member states, the UK, and individual states in the U.S. including California, Virginia, and Colorado, to what may ultimately be a formalized federal law in the coming years.[73]

As companies need to comply with these varying data privacy regulations to remain competitive in the marketplace, ensuring compliance and creating stringent internal policies across an organization is of paramount importance in light of the regulatory frameworks. The failure to do so could result in a large financial penalty that may be catastrophic to a smaller organization or result in an unexpected, high-priced expenditure for a larger organization.[74]

The overlapping international regulations have created potentially burdensome issues for the technology industry and impacted how technology companies approach the mergers and acquisitions space.[75] Particularly, when smaller companies bring new innovative products or services to the international market, be it through an acquisition by a larger entity or simply by natural growth of their product offering, cumbersome regulations can be an impediment to these efforts.[76]

Considering the web of regulation woven over the years since the EU enacted the GDPR, it is important to note the impacts that the technology sector as a whole has experienced and understand if this approach may be misguided.[77] Regulation of any industry can lead to issues with

---

73. Anne Godlasky, *Data Privacy Act Has Bipartisan Support. But…,* NAT'L PRESS FOUND. (Dec. 28, 2022), *available at* https://nationalpress.org/topic/data-privacy-act-adppa-us-lacks-law-eu-standard
(last visited Mar. 25, 2024).

74. Jennifer Huddleston, *The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More*, AM. ACTION F. (June 3, 2021), *available at* https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more (last visited Mar. 25, 2024).

75. Laurent Belsie, *Impacts of the European Union's Data Protection Regulations*, NAT'L BUREAU ECON. RSCH. (July 2022), *available at* https://www.nber.org/digest/202207/impacts-european-unions-data-protection-regulations (last visited Mar. 25, 2024).

76. *Id.*

77. Garrett A. Johnson et al., *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR*, FED. TRADE COMM'N 1, 2 (Mar. 20, 2020), *available at*

development and innovation, and overregulation may have harmful effects on global economies and important technological advancements. Namely, areas like AI, which rely heavily on the free flow of data to develop these novel inventions, can be hindered where technology companies face overly complex regulatory mechanisms.[78]

Companies can take multiple approaches to growth, one of which can be inorganic growth, a term used in the corporate sector to define the process where a company grows in size by a merger, an acquisition, or the takeover of another company.[79] When companies merge, this process typically involves one company acquiring or purchasing another company[80] Traditionally, the acquirer will purchase all of the stock or assets of another company, thus adding them to their existing organization.[81] Organic growth, on the other hand, refers to the natural growth a company experiences through their own internal primary product strings or services, for example, growth over time from the merits of a successful business.[82]

Both of these processes have their respective benefits and drawbacks, some of which include concepts like economies of scope and scale, competitive market edge, talent and resource access, access to new markets, and risk diversification through portfolio expansion.[83] In the technology sector, inorganic growth is often seen where a large technology company is seeking to corner the market in a particular product or service area or expand into a new market.[84] This trend of inorganic growth by merger or acquisition continues to foster digital innovation where

---

https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-garrett_johnson.pdf (last visited Mar. 25, 2024).

78. Ryan Ayers, *Big data and Artificial Intelligence: How They Work Together*, INDATA LABS (Mar. 29, 2022), *available at* https://indatalabs.com/blog/big-data-tech-and-ai (last visited Mar. 25, 2024).

79. Saikiran Chandha, *Understanding the Crux of Organic and Inorganic Growth,* FORBES (Apr. 1, 2022, 7:45 AM), *available at* https://www.forbes.com/sites/forbesbusinesscouncil/2022/04/01/understanding-the-crux-of-organic-and-inorganic-growth (last visited Mar. 25, 2024).

80. Tom Addleston-Towney, *The Basics of an M&A Deal*, FLEXIMIZE, *available at* https://fleximize.com/articles/001039/the-basics-of-an-m-a-deal (last visited Mar. 25, 2024).

81. Chandha, *supra* note 79.

82. *Id.*

83. *The Top Mergers and Acquisitions Benefits You Should Know*, WINDES (Apr. 28, 2021), *available at* https://windes.com/the-top-mergers-and-acquisitions-benefits-you-should-know (last visited Mar. 25, 2024).

84. *See generally, Id.*

companies seek to acquire market competitors to drive disruptive growth opportunities.[85]

Companies across various sectors, including consumer businesses, telecommunications, and financial services, have pushed boundaries of how technology companies have been defined.[86] In doing so, they are targeting disruptive technologies including financial technology, AI, and robotics as they become active deal-makers.[87] These trends have permitted companies to bridge gaps between product and market offerings across many sectors, thus leveraging inorganic growth to innovate, attract talent, and increase customer loyalty through private capital infusions in new ventures.[88] Ultimately, strategic acquisitions in the digital space have allowed companies to converge across market sectors and pursue long-term strategic goals that can allow large companies to collaborate and co-invest in emerging technologies aimed at pushing digital innovation further.[89]

For example, Oracle Corporation, one of the largest technology companies by market cap, has long operated across the technology sector.[90] In July of 2016, Oracle acquired the very first cloud company, NetSuite, in a transaction valued at approximately $9.3 billion.[91] During this acquisition process, companies like Oracle and NetSuite engage in due diligence processes to understand the value and potential costs of the acquisition target. [92] Often, the company seeking to acquire another will consider various benefits of purchasing technology through an acquisition, rather than developing similar technology in-house by an investment in the research and development of that technology.[93] Regardless of the decision to build or buy, ultimately the end result drives benefits for the

85. Iain Macmillan & Sriram Prakash, *Fueling Growth Through Innovation*, DELOITTE 1, 1, 4 (2017), *available at* https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/corporate-finance/deloitte-uk-ma-innovation.pdf (last visited Mar. 25, 2024).

86. *Id.*

87. *Id.*

88. *Id.* at 1.

89. *See id.*

90. *See Market Capitalization of Oracle*, COMPANIESMARKETCAP , *available at* https://companiesmarketcap.com/oracle/marketcap (last visited Mar. 25, 2024).

91. *See Oracle Buys NetSuite*, ORACLE (July 28, 2016), *available at* https://www.oracle.com/corporate/pressrelease/oracle-buys-netsuite-072816.html (last visited Mar. 25, 2024).

92. *See generally id.*

93. Saikat Chaudhuri & Behnam Tabrizi, *Capturing the Real Value in High-Tech Acquisitions*, HARV. BUS. REV. (Sept. 1, 1999), *available at* https://hbr.org/1999/09/capturing-the-real-value-in-high-tech-acquisitions (last visited Mar. 25, 2024).

average consumer who could see new products entering the marketplace or higher quality product and service offerings to corporate customers.[94]

All these considerations are facets of the mergers and acquisition space within the technology sector, and the GDPR complicates them significantly. This added layer of complication comes directly from the new data processing requirements following the adoption and enforcement of the GDPR.[95] Now, not only do companies need to go through traditional due-diligence procedures, which may entail costs like hiring outside advisory firms, accounting firms, or lawyers to advise on a transaction, but in the GDPR era, data security has now become a top priority.[96] With extremely high penalties in place for failure to comply with the GDPR, a company seeking to acquire a smaller organization must consider whether the acquisition target is compliant with the GDPR. Smaller organizations may believe they are in compliance, but this may not always be the case and the potential acquirer will likely need to review various areas like supplier contracts, customers, and employees of the acquisition target. [97]

Occasionally, where an acquisition target is too small to be subject to GDPR regulation, this could necessitate a costly investment on the acquiring party to ensure that all the assets and underlying third-party contracts present are in compliance with the GDPR.[98] Under these circumstances, it may be necessary to invest significant sums of money to bring the target company into compliance, which may result in a scenario where the cost becomes too high to acquire the targeted company despite it potentially owning valuable technology necessary to the acquirer's business model.[99]

Existing agreements or contracts that a target company may have in place may also require certain amendments where there are third parties processing data on its behalf, which adds further complexities to a

94. *See id.*

95. *GDPR and the Effects on the M&A Process*, M&A WORLDWIDE (2022), *available at* https://m-a-worldwide.com/gdpr-and-the-effects-on-the-ma-process (last visited Mar. 25, 2024).

96. *See id.*

97. *See generally* Kevin Stout, *GDPR Becomes Major Factor in M&A Transactions,* LOCKTON, (Jan. 23, 2020), *available at* https://global.lockton.com/gb/en/news-insights/gdpr-becomes-major-factor-in-m-and-a-transactions (last visited Mar. 25, 2024).

98. *Id.*

99. *See generally id.*

successful acquisition.[100] Not only does data privacy regulation pose potential hurdles in the acquisition process, but it can also present companies with issues that may arise after a transaction has closed.

When an acquisition closes, some of the assets that may accompany this transaction often include the data held by the acquired company, which may bring with it unforeseen issues.[101] For example, consider the large hotel group Marriott, which faced a fine of roughly £18.4 million from the UK's Information Commissioner's Office because one of Marriott's customer databases was compromised in 2014.[102] That customer database came under Marriott's ownership following the completion of the Starwood acquisition, another major hotel company, in 2016, evidencing the incredible importance of conducting thorough due diligence of GDPR compliance factors when evaluating an acquisition.[103] Despite the fact that these systems came under Marriott's ownership following the 2016 acquisition, whose breach of those databases occurred in 2014, Marriott was ultimately held liable for the breaches of their customer's personal data.[104] Marriott was forced to pay the financial penalty due to insufficient technical and organizational measures to ensure information security for systems they came to own by an acquisition.[105] This directly evidences the important implications that data privacy regulation has placed on corporations not only in their everyday operations but also in their business-to-business transactions as corporate entities.

---

100. Mikaela Dealissia et al., *Private M&A: Data Privacy and Cyber Security in Global Dealmaking*, LEXOLOGY, (Oct. 3, 2022), *available at* https://www.lexology.com/library/detail.aspx?g=0e3896f6-55f8-40b5-a8e0-0682266a0ce9 (last visited Mar. 25, 2024).

101. Suzy Bibko, *Data with Destiny: How GDPR is Changing M&A*, DATASITE, (July 2, 2021), *available at*
https://www.datasite.com/us/en/resources/insights/blog/how-gdpr-is-changing-m-and-a.html (last visited Mar. 12, 2023).

102. *Id.*

103. Jena Tesse Fox, *Marriott Completes Starwood Merger*, HOTEL MGMT., (Sept. 23, 2016), *available at*
https://www.hotelmanagement.net/transactions/marriott-completes-starwood-merger#:~:text=Long%20live%20the%20new%20Marriott,hotel%20brands%20to%20its%20portfolio (last visited Mar. 25, 2024).

104. *Marriott International Inc, Penalty Notice*, INFO. COMM'R OFF. (Oct. 30, 2020), *available at*
https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf (last visited Mar. 25, 2024).

105. *Id.*

IV. DATA BREACHES BRING NEW COMPLEXITIES UNDER THE GDPR

Society has continued to trend more toward an ever-increasing dependence on technology and connected systems, and this movement has brought with it many benefits but also some varying degrees of risk. As technology becomes more and more complex, there are now more risks and threats of cybercrime, particularly over the past decade, for businesses operating across the internet.[106] With so many companies reliant upon their systems and connectivity, it is of the utmost importance to secure these systems and the data contained within them. Over the past three decades, cybercrime has permeated nearly all industries across the globe, targeting financial institutions, healthcare centers as well as municipal and state governments.[107] Most cybercrimes involve some form of data theft or breach of personally identifiable information ("PII") often achieved by deploying ransomware or other more sophisticated malware.[108]

Throughout the 1990s, society as a whole achieved some of the greatest communication technologies of the last 100 years which connected the globe across networks that lacked the levels of security present today.[109] Given these technological advancements were novel at the time, trust and safety controls did not develop until the rates of cybercrime began to increase. For example, in 1994, one of the first known hackings of a financial institution occurred.[110] This involved the compromise of Citibank's network where a hacker received more than $10 million in fraudulent transactions.[111] As these cyber-attacks continued to increase into the 2010s and to the present day, nations saw more sophisticated approaches to cybercrime, including targeted attacks by nation-states and criminal groups.[112] Widespread breaches of large companies housing the personal data of their users, employees, and customers have become more common. This data, referred to as PII became a large focus of the modern GDPR.

---

106. *A Brief History of Cybercrime*, ARCTIC WOLF (Nov. 16, 2022), *available at* https://arcticwolf.com/resources/blog/decade-of-cybercrime/ (last visited Mar. 25, 2024).

107. *Id.*

108. *Id.*

109. *Id.*

110. Amy Harmon, *Hacking Theft of $10 Million from Citibank Revealed*, L.A. TIMES (Aug. 19, 1995), *available at* https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html (last visited Mar. 25, 2024).

111. *Id.*

112. Arctic Wolf, *supra* note 106.

After a security breach, or more specifically, a breach which implicates PII, the GDPR requires that companies notify all appropriate supervisory authorities within seventy-two hours upon discovery of a breach.[113] In the event of a breach that triggers the notice requirement, data controllers of the company must report to their supervisory authority the nature of the personal data compromised, approximations of the number of data subjects, number of records impacted, describe the likely consequences of the breach, and outline any measures taken or proposed to be taken to mitigate any possible adverse effects.[114] Following this reporting requirement is essential under the GDPR.[115] For example, any shortcomings can leave a company already suffering from the results of a breach subject to administrative fines such as €20,000,000 or 4% of total worldwide annual turnover under article 83(4)(a) of the GDPR.[116]

GDPR fines imposed for mishandling EU-citizen data can also be imposed upon any company that operates outside of the EU, as evidenced by the varying degree of financial penalties levied against companies like the hotel group Marriott in 2020.[117] These companies operate on a global scale, progressively amassing large amounts of PII of EU citizens and other nations.[118] There is a high level of scrutiny on large financial institutions, technology companies, and governmental organizations alike to secure their internal data not only from the likes of cybercriminals, but also to prevent any reprimand or financial penalty levied against them.[119]

Companies had to adopt structured internal cybersecurity policies, often making large investments to bolster their protection from cybercriminals and to avoid internal data leaks or the misuse of PII.[120] Data privacy protective measures have also seen rapid growth over the past two decades in the cybersecurity industry as a whole, where companies

113. *Guidelines 01/2022 on Personal Data Breach Notification*, EUR. DATA PROT. BD. (Oct. 2022), *available at* https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf (last visited Mar. 25, 2024).

114. *Id.*

115. *Id.*

116. *Art. 83 GDPR – General conditions for imposing administrative fines*, GDPR INFO. (May 27, 2018), *available at* https://gdpr-info.eu/art-83-gdpr/ (last visited Mar. 25, 2024).

117. Information Commissioner's Office, *supra* note 104.

118. *Id.*

119. *See* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY, (Feb. 21, 2023), *available at* https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last visited Mar. 25, 2024).

120. *See A Privacy Reset from Compliance to Trust-Building*, PWC *available at* https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html (last visited Mar. 25, 2024).

have begun to offer entire suites of software with a main goal of protecting a company's internal data.[121] As GDPR penalties and industries have grown and we as a society move toward the modern age of data privacy regulations, it is important that a balance is struck between privacy protection controls and penalties in order to avoid stifling any form of innovation. In the world of technology startups, the levels of sophistication often required by the GDPR in terms of data privacy protections, data control officers, internal cybersecurity software services, can impose large financial costs for smaller organizations.[122] This can quickly pose problems to smaller companies that do not have adequate safety measures in place.[123] One of the more common issues that comes up in modern merger and acquisition discussions within the technology sector in particular is whether a target company has adequate information security measures and protocols in place at the time of the due-diligence process.[124] The GDPR and other international privacy regulations are trending toward more stringent measures and continue to change year after year, but these trends may inadvertently stifle innovation in the technology sector.

V. GLOBAL DATA PRIVACY REGULATION AND THE IMPACT ON DIGITAL INNOVATION

Since the GDPR's inception, it and global regulatory enforcement mechanisms similar to it have changed the manner in which new technology companies and long-standing companies approach and interact with global markets.[125] A key factor at play in the relationship between companies, global markets, and governmental bodies is that of regulation. An important balance must be struck as to not over-regulate. Overregulation often presents where a high bar for compliance costs ultimately slow innovation by disincentivizing new investments.[126]

---

121. *Id.*

122. *Id.*

123. *Id.*

124. Huddleston, *supra* note 74.

125. Benjamin Mueller, *A New Study Lays Bare the Cost of the GDPR to Europe's Economy: Will the AI Act Repeat History?*, CTR. FOR DATA INNOVATION (Apr. 9, 2022), *available at* https://datainnovation.org/2022/04/a-new-study-lays-bare-the-cost-of-the-gdpr-to-europes-economy-will-the-ai-act-repeat-history/ (last visited Mar. 25, 2024).

126. Michael Pisa et al., *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity*, CTR. FOR GLOB. DEV. (Dec. 2021), *available at* https://www.cgdev.org/sites/default/files/why-data-protection-matters-for-development.pdf (last visited Mar. 25, 2024).

The EU in particular has seen negative impacts to their digital economy and the rates of new application development since the enforcement of the GDPR.[127] In a recent study reporting on the GDPR's impact on mobile app development, at the start of GDPR enforcement the EU saw the exit of a third of all mobile apps available in the marketplace.[128] In addition, there was a drop of roughly 47.2 percent in new entry of mobile applications in the EU market and the same study shows there is likely a 30.6 percent reduction in aggregate usage and revenue for EU based mobile apps.[129] Further, the GDPR has also negatively impacted companies that target European consumers where firms who were subject to regulation saw an eight percent decline in profits and a two percent reduction in overall sales.[130]

Not only has the EU's economy overall seen harmful impacts, but these harmful impacts have been laid disproportionately across small and midsize enterprises ("SME") in the EU.[131] Large tech giants are notoriously better equipped to handle the impact of GDPR regulation than that of their small and midsized counterparts simply from a resource standpoint.[132] Following the adoption and later enforcement of the GDPR, tech giants like Facebook, Google, and Apple were able to rapidly adapt to GDPR enforcement by employing means such as increased investment in lobbying, and hiring new engineers, lawyers, and managers to ensure compliance and offset costs.[133] In leveraging their stature as tech giants, those same companies increased their lobbying efforts, ranking among

127. Benjamin Mueller, *More Evidence Emerges That the GDPR Has Inflicted Lasting Damage to the EU's Digital Economy*, CTR. FOR DATA INNOVATION (May 11, 2022), *available at* https://datainnovation.org/2022/05/more-evidence-emerges-that-the-gdpr-has-inflicted-lasting-damage-to-the-eus-digital-economy/ (last visited Mar. 25, 2024).

128. Rebecca Janßen et al., *GDPR and The Lost Generation of Innovative Apps,* NAT'L BUREAU OF ECON. RSCH. (May 2022), *available at* https://www.nber.org/system/files/working_papers/w30028/w30028.pdf?utm_campaign=PANTHEON_STRIPPED&amp%3Butm_medium=PANTHEON_STRIPPED&amp%3Butm_source=PANTHEON_STRIPPED (last visited Mar. 25, 2024).

129. *Id.*

130. Chinchih Chen et al., *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*, UNIV. OF OXFORD, OXFORD MARTIN SCHOOL (Jan. 6, 2022), *available at* https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf (last visited Mar. 25, 2024).

131. Giorgio Presidente & Carl Benedikt Frey, *The GDPR effect: How Data Privacy Regulation Shaped firm Performance Globally*, VOXEU (Mar. 10, 2022), *available at* https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally (last visited Mar. 25, 2024).

132. *Id.*

133. *Id.*

the top five corporate spenders for lobbying the EU with annual budgets that exceed €3.5 million.[134]

Whereas in the SME space, SMEs have seen a decrease in their market share, as a result of their inability to adjust as quickly and effectively to the GDPR as the large technology enterprises were able to.[135] A key consideration in the studies that show disproportionate impacts on SMEs involves the consent to share data requirement of the GDPR.[136] Given that under the GDPR companies must maintain affirmative consent to share customer data, larger information technology companies can more easily allocate resources to structured data consent management divisions than their SME counterparts.[137]

The disadvantage that SMEs face is evidenced plainly by Citymapper, a city navigation mobile application launched in the UK that despite securing £6.7m of new cash in just 24 hours, suffered GDPR specific growing pains.[138] Similar to many SMEs operating in the technology sector, most SMEs approach early-stage revenue generation by selling data.[139] Citymapper amassed large amounts of user and public data, developed a strong model to provide it's users with a useful service for travel, yet failed to turn a profit and ultimately burned capital.[140] Typically the datasets on nearly 50 million users would be packaged and sold to interested parties seeking to harness the underlying data on those 50 million users, but this is an expensive undertaking to seek the affirmative consent from those same users to comply with GDPR requirements.[141] As a result, Citymapper found itself in an exceedingly difficult position like other similar SMEs to turn a profit and continue to provide a service to its users.[142]

Turning to more novel forms of technology and innovation, the GDPR has broadly hurt the EU's position as a haven for private-sector investment in technologies like AI.[143] The EU failed to secure a foothold

134. *Id.*

135. Muller, *supra* note 125.

136. Chen, *supra* note 130.

137. *Id.*

138. Taylor, *supra* note 2.

139. *Id.*

140. *Id.*

141. *Id.*

142. Janßen, *supra* note 128.

143. Benjamin Mueller, *Is the EU Doing Enough to Address Europe's Digital Investment Shortfall?*, CTR. FOR DATA INNOVATION (Apr. 20, 2021), *available at* https://datainnovation.org/2021/04/is-the-eu-doing-enough-to-address-europes-digital-investment-shortfall/ (last visited Mar. 25, 2024).

as the home to large technology firms, holding only two of the thirty largest technology firms by market cap.[144] As the EU has adopted the first binding regulation to regulate AI, this could potentially impose even more of a burden on the EU's position as a center for novel technology development harnessing AI.[145]

In 2020, private-sector AI funding for startups in Europe sat at roughly around $4B, far from the levels of the United States and China, at $36B and $25B respectively.[146] Further, beyond AI alone, Europe's entire digital economy has seen a decline in private investment following the GDPR's enforcement.[147] Global markets have seen stark differences in venture capital investment with the EU securing only $40B in venture capital investment, a "small" amount when compared to the $150B of private investment in the United States.[148] Despite the EU's laggard position in the race to develop AI technology from a private investment standpoint, it has solidified itself as the first major body to propose and pass a legal regulatory framework for AI.[149]

However, the European Commission's goals to "facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation," will require companies in the EU to collect large amounts of data.[150] AI development generally requires large amounts of data, typically data on individual persons, in order to process,

144. CompaniesMarketCap, *supra* note 90.

145. Shiona McCallum, et al., *MEPs Approve World's First Comprehensive AI Law*, BBC (Mar. 12, 2024), *available at https://www.bbc.com/news/technology-68546450* (last visited Apr. 12, 2024).

146. Kevin Körner, *How will the EU become an AI Superstar?,* DEUTSCHE BANK (Mar. 18, 2020), *available at* https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000505746/%28How%29_will_the_EU_become_an_AI_superstar%3F.pdf?undefined&realload=njg/hwUiq~NzVtY1gqBJw-TeZefzEboXVM3~bNnAogi0htyygawyhQr13CTgAcC/l (last visited Mar. 25, 2024).

147. *Id.*

148. Gené Teare, *European VC Report 2020: Strong Fourth Quarter Closes Out 2020*, CRUNCHBASE, (Jan. 21, 2021) *available at* https://news.crunchbase.com/startups/european-vc-report-2020-strong-fourth-quarter-closes-out-2020/ (last visited Jan. 8, 2024); Pitchbook et al., *Venture Monitor Q4 2020*, PITCHBOOK (2020), available *at* https://files.pitchbook.com/website/files/pdf/Q4_2020_PitchBook_NVCA_Venture_Monitor.pdf (last visited Mar. 25, 2024).

149. Future of Life Institute, *The Artificial Intelligence Act*, FUTURE OF LIFE INS. (Feb. 27, 2024), *available at* https://artificialintelligenceact.eu/ (last visited Mar. 25, 2024); McCallum, *supra* note 145.

150. *Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, EUR. COMM'N (Jan. 4, 2021), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (last visited Mar. 25, 2024).

train, and develop their algorithms.[151] This data is already increasingly held by many companies based in the United States or China which have already amassed large data profiles on their users, with adequate GDPR compliance measures readily in place.[152] Herein lies the dilemma that the EU faces, balancing the interests in protecting the rights of EU citizens and their privacy, with that of preventing the creation of barriers to digital innovation.[153]

VI. REGULATORY FRAMEWORK IS CUMBERSOME IN ITS CURRENT FORM

The GDPR itself offers guidance to those who fall under its jurisdiction, ideally providing that any enforcement actions or investigations will be decided "without delay" under article 60(3) of the GDPR.[154] This may be the goal across the vast-reaching privacy regulation, however, in practice, it does not always occur without delay.[155] The current regulatory framework allows for a per-member state approach, in practice, a "one-stop shop" system which allows corporations to subject themselves to enforcement on cross-border data processing issues in the state where their European headquarters is located.[156] This framework has been met with much pushback as some nations have been slow to pursue enforcement, and others have been slow to provide decisions "without delay."[157] Ireland's Data Protection Commission, in particular, has struggled to issue fines and provide draft decisions regarding enforcement on questionable data processing practices by certain big tech players.[158]

---

151. James E. Bessen, et al., *GDPR and the Importance of Data to AI Startups*, N.Y.U. STERN SCH. OF BUS. (Sept. 10, 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576714 (last visited Mar. 25, 2024).

152. Körner, *supra* note 146.

153. Axel Voss, *How to Bring GDPR into the Digital Age*, POLITICO (Mar. 25, 2021), *available at* https://www.politico.eu/article/gdpr-reform-digital-innovation/ (last visited Jan. 8, 2024).

154. *Irish DPC Burns Taxpayer Money over Delay Cases*, NONE OF YOUR BUS.–EUR. CTR. FOR DIGIT. RIGHTS, (Apr. 28, 2022), *available at* https://noyb.eu/en/irish-dpc-burns-taxpayer-money-over-delay-cases (last visited Mar. 25, 2024).

155. *Id.*

156. Data Protection Commission, *One-Stop Shop (OSS) Cross-Border Processing and the One Stop Shop*, DATA PROTECTION COMM'N, *available at* https://www.dataprotection.ie/en/organisations/international-transfers/one-stop-shop-oss#:~:text=The%20GDPR%20provides%20a%20new,it%20applies%20to%20your%20organisation (last visited Mar. 25, 2024).

157. Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STUDIES (Sept. 13, 2021), *available at* https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement (last visited Mar. 25, 2024).

158. None of Your Business–European Center for Digital Rights, *supra* note 154.

These problems have brought up more significant questions for the Irish Data Protection Commission, which has taken the lead on enforcement for some larger technology companies under the "one-stop shop" framework and may be suffering from understaffing and resource issues.[159] Ireland holds the responsibility for overseeing the regulation of roughly half a billion EU citizen's data.[160] Ireland's High Court has struggled in its enforcement of larger technology companies, notably only releasing a draft decision of its enforcement action against WhatsApp and Instagram on April 1, 2022—a striking forty-six months after complaints were initially filed.[161] This led activist groups to petition for answers and further information as to the status of enforcement actions like those against WhatsApp and Instagram.[162] Underfunded GDPR enforcement vehicles will continue to complicate not only the process by which companies are able to process data in pursuit of their corporate missions, but also hinder EU citizens ability to understand if their regulators are in fact adequately policing big tech.

VII. AS TECHNOLOGY CONTINUES TO INNOVATE, NEW REGULATORY CONCERNS ARISE

As the Commission moves forward in its effort to supplement the GDPR with a new regulatory mechanism explicitly catered to the use of AI, the European Commission should carefully consider the importance of developing these technologies.[163] AI has the potential to serve as a "key element" in areas such as addressing climate change, track the spread of diseases, and even aid in developing vaccines and medical therapies.[164] Though a highly speculative assessment, with so many potential uses, AI has the potential to impact the world economy "at a staggering $13-16 trillion by 2030."[165] The EU has served as the pioneer for data privacy regulation frameworks since its first effort with the enforcement

159. Marie O'Halloran, *"Serious Shortage" of Data Protection Staff a Huge Risk to Ireland's Reputation*, IRISH TIMES (Sept. 23, 2020), *available at* https://www.irishtimes.com/news/politics/serious-shortage-of-data-protection-staff-a-huge-risk-to-ireland-s-reputation-ff-senator-1.4362865 (last visited Mar. 25, 2024).

160. *Id.*

161. None of Your Business–European Center for Digital Rights, *supra* note 153.

162. *Id.*

163. Mueller, *supra* note 143.

164. Körner, *supra* note 146.

165. *Id.*

of the GDPR.[166] Now, it has the opportunity to take another market-making step in the AI space. Considering the issues that are currently present across global markets, where nations have begun to adopt their own data privacy standards, a complex web of regulations has formed.[167] This web of regulation has resulted in disparate effects on SMEs, large tech giants, and companies across all industries that leverage any form of personal data.[168]

As the EU attempts to step forward yet again in setting the tone for regulating AI, it is imperative that a common approach to the implementation and enforcement of data protection rules occurs on a global scale.[169] With the U.S. keen on adding to the global regulatory framework that is currently in place across the EU and the UK, albeit an effort that will likely take years to formalize, collective action is imperative to reduce complexity.[170] The EU has long provided for each of its twenty-seven member states, the authority to leverage their own data protection authorities and enforcement arms, but this may have fallen short of its goal. With AI regulation rapidly approaching as the next frontier ripe for regulatory intervention, the global community of nations must come together to strike a balance. This balance must focus on balancing the protection of individuals' fundamental right to privacy while not creating oppressive barriers to the development of digital innovations, including AI.[171]

The UK has already taken steps toward untangling some of the more cumbersome regulations currently in force under the EU GDPR, potentially driving more complexity.[172] The UK has published a revision to the existing UK GDPR which is designed with feedback from various businesses and data experts to create less stringent requirements on record

166. European Comm'n, *A European Approach to Artificial Intelligence*, EUR. COMM'N (2022), *available at* https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (last visited Mar. 25, 2024).

167. Körner, *supra* note 146.

168. *See* Prof. Thomas B. . .ck, et. al., *Digital SME Position Paper on the EU AI Act*, EUR. DIGIT. SME ALL. (Sept. 2021), *available at* https://www.digitalsme.eu/digital/uploads/DIGITAL-SME-Position-Paper-AI-Act-FINAL-DRAFT-1.pdf (last visited Mar. 25, 2024).

169. Voss*, supra* note 153.

170. Godlasky, *supra* note 73.

171. *See* Vincent Manancourt, *Top EU Official Warns Privacy Rules May Need to Change*, POLITICO (Dec. 2, 2021), *available at* https://www.politico.eu/article/eu-privacy-regulators-clash-gdpr-enforcement/ (last visited Mar. 25, 2024).

172. John Georgievski & Gregory Szewczyk, *The UK Publishes Bill to Update UK GDPR,* BALLARD SPAHR LLP (Mar. 9, 2023), *available at* https://www.jdsupra.com/legalnews/the-uk-publishes-bill-to-update-uk-gdpr-4040942/ (last visited Mar. 25, 2024).

keeping and cookies consent, among other specific changes under the revised UK GDPR standards.[173] This step is presumably an effort toward reducing the degree of complexity and ensuing costs that UK businesses face, with estimates projected at a reduction of four billion pounds to the UK economy over the next ten years.[174]

As the lighthouse of data privacy regulation, the EU comes again with the opportunity to fall back on its original aspirations to create a unified data privacy regulation that may serve as a beacon to other nations.[175] Rather than the U.S. approaching the ADPPA in a vacuum, a referendum, among all major nations, to create a unified approach to data privacy and AI regulation could provide for much clearer guidelines as companies do business in the digital age.[176] As opposed to siloed regulation coming from various nation-states including, among others, the UK, EU, and the U.S., an international data privacy regulatory body could be formed akin to the International Court of Justice which could handle the regulation of international corporations.

Should a company primarily do business within one nation's borders, regulation could continue to be centralized within that nation but with an overarching international regulatory body to provide oversight and collaboration on enforcement. Today, where large corporations ultimately face the prospect of being subject to financial penalties from more than one regulatory body, this can pose an overarching threat to the technology sector's ability to operate and develop groundbreaking technological advancements freely.

CONCLUSION

Recalling the same sentiment that led to the cornerstone principle of all individuals' right to privacy that the Universal Declaration of Human Rights codified, a modern, common approach to regulation may help to untangle the web that companies face today.[177] The GDPR in its current form, has negatively impacted digital economies, small and midsize enterprises alike, and shown slow judicial progress on adequately delivering

---

173. *Id.*

174. Natasha Lomas, *UK Takes Another Bite at post-Brexit Data Protection Reform–with 'New GDPR,'* TECHCRUNCH (Mar. 8, 2023), *available at* https://techcrunch.com/2023/03/08/uk-data-reform-bill-no-2/ (last visited Mar. 25, 2024).

175. *See* Manancourt, *supra* note 171.

176. *See* Mark MacCarthy, *What U.S. Policymakers Can Learn from the European Decision on Personalized Ads,* BROOKINGS (Mar. 1, 2023), *available at* https://www.brookings.edu/blog/techtank/2023/03/01/what-u-s-policymakers-can-learn-from-the-european-decision-on-personalized-ads/ (last visited Mar. 25, 2024).

177. *See id.;* Heine, *supra* note 157.

enforcement decisions. This process will only become increasingly complex as more regulatory frameworks emerge. Without a global concerted effort to create new fundamental guidelines regarding AI and data privacy laws generally, the progressive privacy rights that the EU pioneered under the GDPR may continue to create inequitable and disjointed global regulatory frameworks in the decades to come.