The Global Fracture of Data Privacy: Sovereignty, AI, and the End of Universalism

Gaurav Banda

ABSTRACT

The notion of the "Brussels Effect" implied that the GDPR would be the sole worldwide gold standard for more than a decade. Nevertheless, by 2026, there will be a structural "Great Fracture" in the digital environment. The Great Fracture is described by a change in global interoperability to Digital Sovereignty, which implies the employment of data privacy legislation as a mechanism for trade protectionism and national security. In this paper, we examine the differences among the three main "Privacy Poles": the privacy regime based on human rights of the European Union, which is now aligned with the 2024-2026 AI Act; the Securitized Sovereignty model of China, regulated through the PIPL law; and the fragmented, sectorial-based privacy regime of the United States, known as the "Market Contract" model. The results obtained demonstrate that "the Global Fracture" has caused an escalation in the operational cost of compliance by multinational companies by 28% since 2023. Moreover, the development of Generative AI technology has made the traditional "Consent-based" approach irrelevant. The emergence of the "Privacy-Innovation Gap" phenomenon means that the jurisdictions with tough data localisation policies are witnessing a slowdown in joint AI research, whereas the "Data Havens" are experiencing a boom in algorithm training. In summary, the paper posits that the time of universal digital rights is giving way to an age of Algorithmic Realpolitik. We contend that the harmonisation of laws will not be a feasible objective going forward. The fate of the international digital economy now rests on Technical Interoperability, the formulation of interoperable privacy protocols that permit data to stay "sovereign" yet facilitate the transfer of "insights" across borders.

Keywords: *Digital Sovereignty, Splinternet, GDPR 2.0, Data Localisation, AI Ethics, Privacy-Enhancing Technologies (PETs), Data Gravity.*

I. INTRODUCTION

The concept of "World Wide Web," historically, had depended upon the free flow of information without any physical barriers, a "Global Commons" where connection was more important than location. However, to date in 2026, the concept of "World Wide Web" is no longer valid due to the concept of "Global Fracture." The issue of data privacy, historically concerned with personal liberties, has today become an integral aspect of digital sovereignty[1]. It is more than just a dispute in law between trading partners. It is a fracture of the Internet into trust zones where there are incompatible ideologies of data governance.

1 https://www.researchgate.net/publication/396975294_Digital_Sovereignty_and_Human_Rights_Balancing_Security_and_Freedom

The trigger for this rapid fragmentation is the development of Generative Artificial Intelligence (GAI) and Large Language Models (LLMs). The hunger for enormous and good data sets needed to feed these systems led to the emergence of a "Data Arms Race," forcing nations to adopt "Data Gravity" principles[2]. These principles ensure that personal data and its associated value stay confined within national territory borders. Thus, the "Brussels Effect," where the EU's GDPR imposed its regulations internationally for almost a decade, no longer holds sway. Instead, we now observe the rise of Securitised Sovereignty in Asia, Democratic Technocracies in Europe, and a Voluntarist Market approach in America[3].

In light of these developments, this paper posits that any attempt to restore harmony to data privacy globally via conventional diplomacy or law is now futile. The shift towards regulation of the logic of algorithms in processing personal data has resulted in a compliance cost threshold that cannot be sustained by global innovation[4]. Multinational corporations have become increasingly compelled to forgo universal service architectures and adopt localised stacks, wherein a person's right to privacy will be decided based on their GPS location instead of a universal human dignity standard[5].

II. TRI-POLAR WORLD OF DATA PRIVACY

The notion of "Tri-Polar World of Data Privacy" signifies the final and absolute fragmentation of international regulatory convergence, given that the online environment is divided into three separate and mutually exclusive ideological domains. The EU's "Rights-Centric" ideology is based upon the modifications to the GDPR made in 2026, where privacy has been enshrined as part of the individual's very biology, namely, "neural privacy[6]."On the other hand, the "State-Centric" Chinese approach implements Personal Information Protection Law (PIPL) and amendments to the Data Security Law by 2025 as a means of enforcing an environment where privacy is equivalent to national security; that is, where data is a state-controlled resource and personal privacy is only assured when it does not compromise social stability[7]. At the same time, the US remains an advocate of the "Market-Centric" voluntaristic framework, which is typified by the absence of national regulatory statutes, as well as a complex network of state-level legislation and industry regulations. The Market-Centric approach focuses on "the freedom to innovate" and the commoditization of data through contractual agreements between the consumer and platform[8]. This tri-polar breakup creates "geopolitical

2 https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202022/mckinsey-tech-trends-outlook-2022-full-report.pdf
3 https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/53217230/c6797.pdf
4 https://internationalaisafetyreport.org/publication/international-ai-safety-report-2025
5 https://pureadmin.qub.ac.uk/ws/files/625056928/Belluigi_2025_Being_in_Shadow_and_Light_Book.pdf
6 https://www.elon.edu/u/imagining/surveys/xv2023/the-future-of-human-agency-2035/
7 https://www.congress.gov/crs-product/R46915
8 https://research-api.cbs.dk/ws/portalfiles/portal/75601934/paul_du_gay_et_al_discretion_and_bureaucracy_publishersversion.pdf

friction" in which the data located in one pole may be legally poisonous to another, thus compelling an inherent separation between the global digital economy while mandating the creation of local "sovereign clouds"[9].

Model	Core Philosophy	Key 2026 Regulation	Enforcement Mechanism
European (Human-Centric)	Privacy as a fundamental right	GDPR 2.0 (2026 Reform)	AI Transparency Audits & "Right to Explanation"
Chinese (State-Centric)	Privacy as National Security	PIPL Amendment (Jan 2026)	CAC Security Assessments for Cross-Border Flow
American (Market-Centric)	Privacy as a Contractual Right	Patchwork (CCPA, CO, TX, etc.)	Federal Trade Commission (FTC) & State AGs

III. AI CATALYST: FROM REGULATING DATA TO REGULATING LOGIC

The development of GAI and GPAI paradigms is pushing the world towards an overhaul in terms of its data privacy framework as well, and that has moved away from being preoccupied with the data collection process to regulation of the algorithms' functioning[10]. For many years, compliance systems have been built on the premise of the old data life cycle, where information could be classified, consented to, and erased for each individual. Yet, the emergence of large language models and self-driving AI agents has made that obsolete, as the data fed into the algorithm during its training process becomes an inherent part of the algorithm's weights and parameters. It is simply impossible to erase any individual's data without changing the algorithm's structure or breaking it[11]. Thus, new legislation is emerging that can penetrate the "black box" of algorithms.

For example, the EU AI Act, along with its respective guidelines for 2025–2026, imposes heavy transparency requirements on those providing GPAI models by controlling their intake process and the logical reasoning behind them rather than merely focusing on information storage[12]. As the United States experiences new legislation in states like California, Texas, and Colorado, there is an increasing need for the developer to provide an algorithmic impact assessment showing the source of the data used in training and the minimisation of bias[13]. In essence, the emergence of these laws presents a significant legal dilemma to multinational tech companies. While compliance with the logic-based transparency laws in one country exposes the company's intellectual property in another, it shows that today's privacy wars have shifted to the neural network[14].

[9] https://medium.com/@priyangshutalukdar4/the-world-of-geopolitics-in-2025-mapping-the-digital-iron-curtain-48da2585c6e0
[10] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
[11] https://ierj.in/journal/index.php/ierj/article/view/5097
[12] https://fpf.org/blog/red-lines-under-the-eu-ai-act-understanding-prohibited-ai-practices-and-their-interplay-with-the-gdpr-dsa/
[13] https://www.rhsmith.umd.edu/programs/executive-education/learning-opportunities-individuals/genai-risk?gad_source=1&gad_campaignid=23777531738&gbraid=0AAAAAozZs1piSvpe-a59dkbpeapwKixWU&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3cfvH5LlaMvWUORtrLwRvGjb0TCxalUsf1SxppX7nOSvki8XVEdg-64aAvOaEALw_wcB
[14] https://www.gunder.com/en/news-insights?nt=1624&p=11961

IV. TECHNOLOGICAL RESPONSES: SOVEREIGNTY BY DESIGN

The increasing legal and geopolitical segmentation of the world's digital ecosystem has prompted the tech industry to shift to the paradigm of "sovereignty by design," going beyond mere data localisation and adopting a more holistic architectural approach[15]. As data privacy regulations continue to expand and measures against cross-border data flows become increasingly stringent, multinational corporations and cloud computing firms are reorganising their systems to maintain governance, portability, and resilience of their data within specific geographic territories[16]. The introduction of such projects as AWS European Sovereign Cloud at the start of 2026 is an example of this kind of change. With the establishment of physically and logically isolated regions in which data will be controlled solely by locally-based staff within a local corporate entity, with no relation to extra-territorial legal threats such as the US CLOUD Act[17], organisations can benefit from this change. To address the computational needs of modern AI training in conjunction with localisation requirements, companies are increasingly turning towards Zero Trust data sovereignty solutions, like CSE & EKM[18]. Such solutions help ensure that the information remains encrypted during transfer and is never decrypted or processed in plain text on the service providers' back-end servers, thus meeting the requirements of strict regulations such as NIS2 and DORA[19]. To train their algorithms internationally without transferring any data, companies are now opting for decentralised and federated AI models, in which the learning model is moved to the sovereign region rather than transporting data to other jurisdictions[20].

---

[15] https://www.detecon.com/en/insights/article/digital-sovereignty-after-davos-2026-how-data-cloud-and-ai-control-shape-global-resilience

[16] https://www.f5.com/glossary/cloud-load-balancing?utm_campaign=26Q2_PSE_apcj_all_security_5551-glblsem_none&utm_content=loud-balancing-glossary&gclsrc=aw.ds&gad_source=1&gad_campaignid=23664482800&gbraid=0AAAAAB-GTTSNXBKYQ0JcZV0kmdn2rbqib&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3ceB0FI7biUgeFscBFTMu_ZrCMN-YWRn98bAgmNI9IbFjJWryOD99IMaAkQ1EALw_wcB

[17] https://home.bigid.com/demo-eu-ai-act?utm_campaign=EU/UK+-+Search+-+NB+-+Data+Privacy+&+Compliance&utm_source=google&utm_medium=cpc&utm_term=eu%20artificial%20intelligence&hsa_ver=3&hsa_cam=23528018771&hsa_grp=194277481402&hsa_net=adwords&hsa_ad=799136709500&hsa_kw=eu%20artificial%20intelligence&hsa_mt=p&hsa_acc=9924524058&hsa_src=g&hsa_tgt=kwd-760244747711&gad_source=1&gad_campaignid=23528018771&gbraid=0AAAADP9WREON3RioxbrLoCj1_u1EpsFI&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3cdlISiH6t9IX-QJQgVaZsMAkuvZ53egjS_M92HBidGHIYdb_P6i1iwaAoL_EALw_wcB

[18] https://www.kyndryl.com/in/en/campaign/policy-as-code?utm_medium=paid-search&utm_source=google&utm_content=other&utm_term=policy%20as%20code&utm_campaign=KAIWW&gad_source=1&gad_campaignid=14990602944&gbraid=0AAAAArA7SN8XZpgqosPUYataRymmlyFbm&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3cchrh0Xyj4EsaTgqu4G8CqubzKLdDvUyav-hksZGxmn7UfSWMqD0NcaAt5OEALw_wcB

[19] https://www.skyflow.com/whitepapers/data-breaches-the-problem-is-pii?qgad=767409565842&qgterm=protect%20sensitive%20data&kw=protect%20sensitive%20data&cpn=22578614055&utm_agid=184282289278&creative=767409565842&extension_id=&device=c&utm_term=protect%20sensitive%20data&utm_campaign=APAC:Search:HI:DataSecurityProtection&utm_source=google&utm_medium=ppc&utm_content=PII&utm_content=PII&hsa_acc=6575335991&hsa_cam=22578614055&hsa_grp=184282289278&hsa_ad=767409565842&hsa_src=g&hsa_tgt=kwd-320057848794&hsa_kw=protect%20sensitive%20data&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gad_campaignid=22578614055&gbraid=0AAAAABzDxWqy402wKOL5K9t4OA87kudFp&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3ccrl9iinSelcOFPGOfqgaP0kTVqFI-qx8HnefCeVWSIZLSTzdTesAgaAtsZEALw_wcB

[20] https://www.nutanix.com/go/foundation-for-cloud-native-success-kit?utm_source=google_adwords&utm_medium=paid_search&utm_campaign=Nutanix_Search_APAC_T1_Generic-Applications_Google_Demand_English_India_701VO00000OPWS6YAP&utm_term=cloud%20native%20software&ut

V. THE SOCIO-ECONOMIC IMPACT OF FRAGMENTATION

Consequences for international trade, competition, and corporate governance will be felt from the global digital data privacy divide, which will be more profound than mere issues of compliance[21]. The period from now until 2026 will witness the emergence of the "compliance tax," a phenomenon that will become most intense during the period around 2026, when data localisation will be at its height[22]. The collapse of the world into a unified regulatory regime compels companies to utilise regionalised infrastructure platforms such as isolated data centres, legal departments, and regionalised AI models to preserve their presence within the marketplace. Such a fragmented system carries an economic burden, particularly affecting small tech companies without sufficient financial resources to manage the complexities of multiple jurisdictions[23].

Moreover, the division within the digital economy has resulted in the creation of another form of innovation inequality. The jurisdictions with very restrictive and inward data systems, like the European Union and some APAC countries, are now facing the challenge of an increasing “Privacy-Innovation Gap”[24]. Even though the restrictive policies work efficiently to ensure user rights protection, the process of exchanging data from other nations hinders their progress in utilising AI technologies and predictive data analytics. On the contrary, more relaxed “data havens,” where there are no stringent transparency requirements for AI and algorithmic training, as seen in the West[25], attract risky algorithmic development activities.

On the enterprise level, the socio-economic cost of this issue has brought data privacy from the IT/legal back office to board-level strategy[26]. As per the ISACA State of Privacy 2026 study, almost 47 per cent of technical privacy positions continue to be understaffed, causing severe “audit fatigue,” where routine regulatory audits cause substantial downtime. In addition to this, businesses must also reconsider their global MSAs to move away from the centralized cloud first model to the decentralised sovereign cloud paradigm[27]. Sovereignty-by-Design implies that global threat intelligence and fraud analytics can no longer be centralised, leaving security analysts without visibility, thereby increasing the costs associated with combating cyber-enabled fraud/data breaches[28].

The socio-economic consequence that arises from such disintegration is the loss of the digital single market on a global scale. In order to avoid an irreversible economic slump, international institutions have accelerated

m_experience=&cq_plac=&cq_net=g&cq_plt=gp&cq_cmp=23216937051&_bt=797905672028&_bk=cloud%20native%20software&_bm=p&_bn=g&_bg=185008795141&gad_source=1&gad_campaignid=23216937051&gbraid=0AAAADN2Vjbtt88kSAyDDnV9tKZVkvWk_&gclid=Cj0KCQjwh-HPBhCIARIsAC0p3cdz3tNjrjZPXNYSM51O-KxDuyvz_eJ1mqDoZY3v0wcr4GC0VXgTiFIaAu-tEALw_wcB

[21] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[22] https://www.imf.org/en/blogs/articles/2026/01/19/global-economy-shakes-off-tariff-shock-amid-tech-driven-boom

[23] https://www.imperva.com/learn/data-security/data-localization/

[24] https://pureadmin.qub.ac.uk/ws/files/625056928/Belluigi_2025_Being_in_Shadow_and_Light_Book.pdf

[25] https://trustarc.com/resource/webinar-2026-global-privacy-benchmarks-report-trends-and-perspectives/

[26] https://iirisconsulting.com/data-privacy-week-2026-how-dpdp-act-is-shifting-data-protection-from-it-teams-to-the-boardroom/

[27] https://www.gartner.com/en/newsroom/press-releases/2026-02-09-gartner-says-worldwide-sovereign-cloud-iaas-spending-will-total-us-dollars-80-billion-in-2026

[28] https://www.edgescan.com/why-data-protection-must-be-a-strategic-priority-in-2026/

the development of so-called "Data Bridges," including current negotiations on trans-Atlantic and Indo-Pacific cooperation in data exchange. This would help establish reciprocity in PETs, thus ensuring uninterrupted data transmission without the need to move sensitive personal data itself[29].

VI. CONCLUSION

The phenomenon of the "Global Fracture" that affects the issue of data privacy is no longer considered only as a process but rather a paradigm shift in the world's economy due to technological innovations. As was stated above, an epoch where a global network of the internet, whose security was provided by the extraterritorial application of the European Union's General Data Protection Regulation, has been completely substituted by another model based on digital sovereignty and algorithmic protectionism. The maturity of GAI systems and the adoption of the provisions stipulated by the EU AI Act have changed the contours of the regulatory framework from data protection to algorithmic containment.

Multinational firms trying to manoeuvre through this fragmented world find themselves facing equally fragmented tools to facilitate cross-border transfer of data, such as the EU-U.S. Data Privacy Framework (DPF) and standard contractual clauses (SCCs). The cases before the CJEU over the adequacy of data protection mechanisms within the U.S. highlight how this is a fundamental conflict of ideologies between market-centred economies and rights-centred states. Trying to solve this rift via endless rounds of legal negotiation results in "compliance fatigue" and increased "operational compliance tax," which hurts small- and medium-sized firms.

Thus, the way forward cannot be contingent on the futile chase of one global treaty. On the contrary, the sustainability of the interdependent digital economy demands a new mindset for technical interoperability. Through the decoupling of insight transport from data transport, sovereignty by design allows a viable approach to international business. The technologies of federated learning, differential privacy, and sovereign clouds allow corporations to analyse information locally in their country of origin but learn globally through AI models.

In the end, interoperability in the era of the "Splinternet" requires a two-pronged strategy: a starting point acknowledging distinct privacy philosophies of different countries and a common benchmark for PETs. As the standard-setting agencies and regulators develop common frameworks for data infrastructure, this technical approach guarantees that the essential human right to data privacy remains intact without hindering innovation and AI research globally.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[29] https://pandectes.io/blog/cross-border-data-transfers-in-2026-localization-vs-globalization/