Global Essay Competition 2026

Title: Reclaiming the Digital Self: A Global Framework for Sovereignty in the Age of AI

Essay:

Introduction

In 1215, the Magna Carta placed limitations on detention without legal justification; eight centuries later, we still lack established protections for our digital identities. As frontier artificial intelligence (AI) models[a] from technology companies become more relied upon by a network of global users, the colliding legal landscape of regulations across the world has not kept pace with current AI, and the current "extractive" data model has reached a breaking point. Human digital presence, such as creative licensing, online activity, and media exchange, has become raw material for training frontier models.

While this threat to digital sovereignty is global, the responses of world governments remain vastly different in terms of prioritisation and ideology. This problem, however, lies in the history of copyright law globally as it pertains to the public domain. In the European Union, "organisations are permitted to process a user's data without their consent if the processing is in the public interest and balanced against the individual's privacy rights" (Polonetsky et. al, 2013).[1] While the European Parliament added the Digital Single Market amendment in 2019 and amendments to the GDPR to create an exception for research organisations to obtain lawful access to data and reproductions for scientific research, it creates a regulatory loophole that fails to differentiate non-profit research from accelerated research-driven for-profit development of commercial AI models (Das, 2026).[2] In contrast, as of January 2026, the United States has plans to blueprint AI governance frameworks but lacks a singular, comprehensive federal-level AI privacy law to govern under.

I argue that enforcing digital sovereignty requires a three-tier architecture: a digital habeas corpus established through a new UN protocol, with a nation-level implementation framework; structural separation of research entities from commercial AI; and decentralised identity verification through cryptographic consent. This analysis focuses on the United States and the European Union to highlight their distinct approaches and propose a solution for global discussion.

Background

The global AI landscape is characterised by a polarity of policies between the US and the European Union.

United States

The United States retains a deregulatory, conservative stance towards artificial intelligence. California's Transparency in Frontier AI Act, which is effective January 1,

[a] **Frontier AI models**: A flagship, large-scale AI model.

2026 and Colorado's anti-discrimination mandates have created a provincial black box[b] of privacy rights depending on which postal code they live in. At the federal level, President Donald J. Trump signed an Executive Order, "Ensuring a National Policy Framework for Artificial Intelligence," that establishes a non-invasive federal-level framework for AI and creates a task force to challenge state-level AI regulations in states such as California and Colorado (Das, 2026). The deregulatory stance embodies a broader belief that innovation precedes public policy: a viewpoint historically supported in US tech policy, from telecommunications to social media, yet it has consistently led to retroactive, fragmented fixes.

European Union

The European Union is now in the enforcement phase. Under the General Data Protection Regulation (GDPR), seven core data protection principles safeguard users by enforcing data storage limits, verifying the purpose and use of data, and holding third parties accountable (GDPR.eu).[3] Starting late 2025, the European AI Office has taken a firmer stance on AI transparency, enforcing a Digital Omnibus of technical amendments to the GDPR. The EU's strategy embodies a precautionary principle lacking in US policy: that the systemic risks of unregulated AI use surpass the expenses of regulatory enforcement.

The omnibus allows the European AI Office to serve as the Union's central authority, acting as a privacy watchdog that audits model weights[c]. In addition, the Union has stated that it will create safe, government-regulated sandboxes for AI to test models using private data. This centralised institution of authority reflects the European consensus that AI models require independent auditing and benchmarking.

A Theoretical Lens – Digital Actor-Network Theory

Actor-Network Theory (ANT) provides a valuable lens for examining AI privacy. The theory treats the ability to act as a network of human and non-human 'actants'. Here, these actants consist of datasets, bots that scrape websites for metadata, model architectures, venture capital, and regulatory bodies – whose interactions produce outcomes that no single actor controls (Nickerson, 2025).[4] Traditional privacy law assumes a mutual agreement between consenting parties: the person whose data is taken and the collecting organisation. However, frontier AI development involves a chain of actants where accountability diffuses. A user uploads an image; a scraper[d] collects it; a data broker sells it; a lab trains a model; and a third party generates synthetic media. At which point in the chain is someone held liable?

ANT reveals that the "black box" is not just proprietary codebases where these models are shipped, but the network of interactions dissolving across the chain

[b] **Black box**: The nature of an AI or algorithmic system that takes in data inputs and produces an output without revealing specific steps or internal logic to reach a conclusion or prediction.
[c] **Model weights**: core statistical parameters in an AI model that define priors in its knowledge and computational neurons to transform model inputs and outputs.
[d] **Data scraper**: A software tool that automates website or data visits to mass extract data contents and copy over information in an organised way.

[**Figure 1]**. This framework suggests that governance and accountability must target network structure rather than just individual actors (Chung & Schiff, 2025).[5]

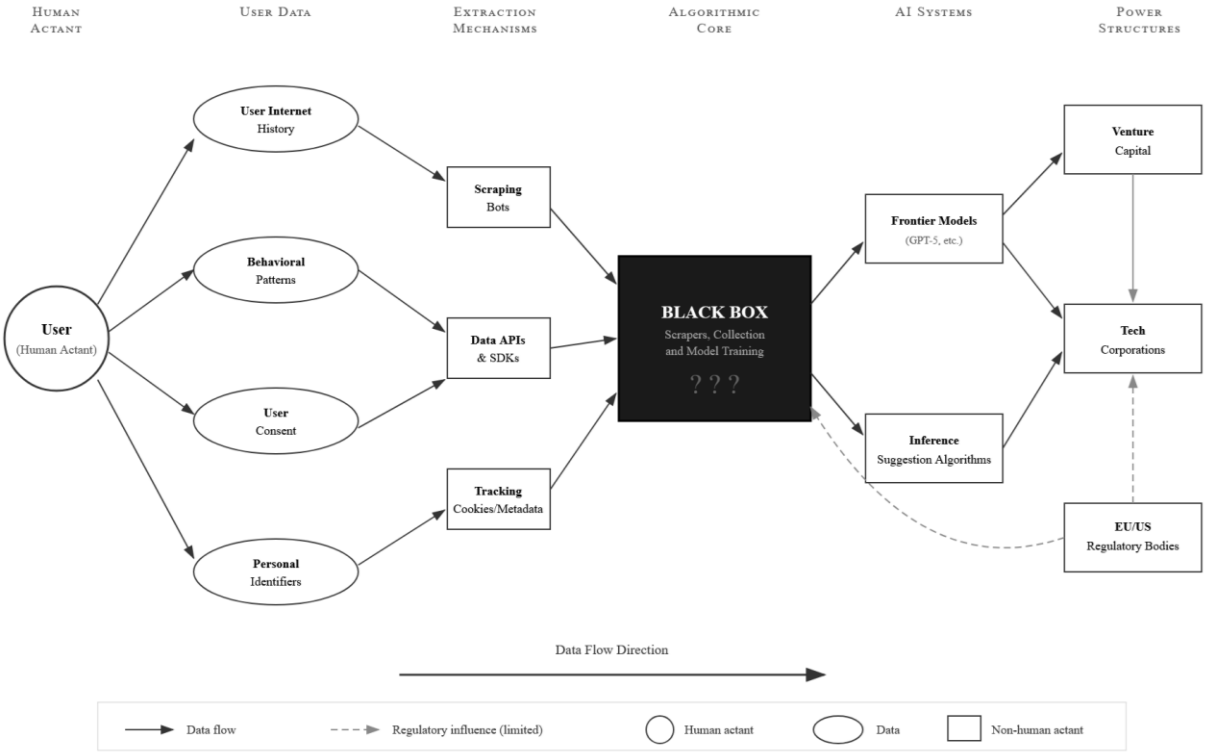

Figure 1. Actor-Network topology of user data flow through human and non-human actants. Solid arrows indicate data extraction; dashed arrows represent limited regulatory influence (Anthropic, 2025).

Current Challenges

The collision between the iterative nature of AI model deployment and the legacy legal framework has created a technical oversight gap and a foundational failure in the premises of the existing social contract to account for the digital extension of the self.

Data at Scale

The development of frontier models has transitioned from static pre-training mechanisms to iterative deployment and reinforcement learning. The relationship between model size and data ingestion remains a core research question. Models require constant alignment through human feedback loops and re-training for fine-tuning (Ouyang et al., 2022).[6] These processes value content only as a training resource versus their intrinsic value, fundamentally altering the implicit social contract of online participation.

The challenge for lawmakers lies in quality assurance. As more generative AI content becomes commonplace in society, mechanisms that adapt alongside frontier model advancements that flag AI-generated content must be required to avoid model

collapse[e]. In this state, AI begins to degrade as it learns from its own outputs (Freshfields, 2026).[7]

Demography Meets Tech

As reliance on technology becomes more widespread globally, we are beginning to see a new generation that has lived their entire lives with an online footprint. The younger generation has no analogue identity to fall back on.

In July 2025, consulting firm EY published a study that states “over seven out of 10 employees expect jobs to be cut in Switzerland as a result of competition from AI,” yet “almost nine out of ten respondents in Switzerland now use AI tools” (EY, 2025).[8] This paradox reflects both misconceptions about AI and lagging institutional adaptation. Workers tacitly acknowledge that by refusing to utilise AI technology, they will suffer a relative disadvantage. Conversely, workers displaced by technology face a transition in which skills lose market value faster than new opportunities can emerge. This represents a coordination failure that requires regulatory correction, where the labour market is driven by rational self-interest, yet the collective fallout remains unaddressed.

The Likeness Crisis

A legal and moral void exists around synthetic media generation, testing existing legal frameworks. In *Andersen v. Stability AI (N.D. California 2023)*, artists filed a class-action lawsuit against Stability AI for training on the LAION dataset, a 5-billion-image dataset scraped from the Internet used to train MidJourney, alleging copyright infringement. In August 2024, Judge William Orrick denied motions to dismiss, allowing these claims to proceed. Crucial to the verdict was Stability AI’s CEO's claim that “their company has developed a methodology to compress 100,000 gigabytes of digital images into a two-gigabyte file that could 'recreate' any of those images”, alongside research demonstrating that training images could be reproduced through precise prompting (Schor, 2024).[9] The trial, set for September 2026, will determine whether embedding copyrighted materials into model weights violates copyright law.

In legal proceedings such as *Andersen v. Stability* AI, copyright law is addressed, but neither likeness rights (appropriation of private individuals) nor the reverse is. Non-consensual AI-generated images of private individuals remain their own separate legal grey area. The victims of these abuses must navigate state laws regarding deepfakes, locate unknown perpetrators across multiple jurisdictions, and seek remedies within an unreasonable timeframe, given that these images are published before legal action can be taken. Thus, there is a fundamental imbalance in the system: legal proceedings take months, while the proliferation of synthetic media happens in hours.

Responses to the image-generation craze on individual social platforms remain ineffective. For example, when users generated non-consensual imagery through

[e] **Model Collapse:** Quality degradation when AI trains on its own outputs, compounding errors over successive iterations.

xAI's Grok in early 2025, the company's stated policy of penalising "illegal content" offered no practical remedy, as jailbreaking prompts routinely bypass in-place model safeguards (Fedorczyk, 2026).[10]

Reimagining Solutions for Digital Sovereignty

The challenges outlined above stem from a single source: all current legal frameworks presuppose a legally defined bilateral relationship. The AI ecosystem has broken down this assumption. Data is now flowing across multiple boundaries and from many participating parties; therefore, liability is now diffused across a chain of actors/actants, where individuals are no longer able to assert personal rights. The following proposed three-pillar architecture addresses this structural failure.

A Digital Habeas Corpus

The first pillar is establishing a digital *habeas corpus*, extending legal protection against unlawful detention to digital identity (Administrative Office of the US Courts).[11] In the algorithmic age, safeguarding the digital self is essential. I propose a framework convention under the United Nations, modelled on the Paris Agreement's[f] structure of internationally agreed principles with nationally determined implementation. Signatory states will implement national laws to provide three guaranteed rights: individuals may request to know if their data has been included for training in an AI system, request removal from future training iterations, and the right to compensation where commercial use is demonstrated.

Enforcement would occur through national courts, with a cross-border recognition modelled on the Hague Convention[g]. This approach helps create universal minimum standards, establishes a framework to avoid jurisdictional limitations across international bodies, and enables individuals whose likeness is abused to demand disclosure or remediation regardless of location or where the model was trained.

Separation of Research and For-Profit AI

Currently, the AI landscape allows a single company to gather user data, build models, and sell products, thereby consolidating power and making it difficult for stakeholders to hold a single entity accountable. As shown through Actor-Network analysis, this type of organisational structure allows for the dilution of accountability throughout the chain of command, to the point where no one entity can be held responsible. I propose a mandate to structurally separate frontier AI research and commercial use of those services. This mirrors the Glass-Steagall Act of 1933[h], which separated commercial banking from investment banking.

---

[f] **Paris Agreement:** 2015 climate accord combining universal principles with nationally determined frameworks for enforcement.

[g] **Hague Convention:** A series of international treaties aimed at streamlining cross-border legal, civil, and commercial matters between member states.

[h] **Glass-Steagall Act of 1933:** a US law separating commercial and investment banking to prevent conflicts of interest.

Research entities focused on advancing model capabilities would operate as non-profit institutions with a statutory mandate to serve the public interest. Commercial entities seeking to deploy AI products would license model training weights from research bodies at regulated rates determined by the UN, reflecting actual development costs.

Access to non-profit research funding will come from a tax on the commercial deployment of AI, such as telecommunications service fees, as well as UN country contributions. By establishing a mixed-funding model, the proposed solution enables research independence and financial sustainability. An international oversight committee consisting of signatory states will audit large-scale model releases against ethical compliance before models are allowed to be commercially licensed.

Decentralised Consent Verification

Current legal frameworks, no matter how comprehensive, do not work quickly enough to stop the damage caused by constant data scraping and dissemination of synthetic media. Legal remedies must be augmented by a technical solution.

I recommend that we insert consent markers (cryptographic signatures[i]) maintained by a technical joint US task force into digital media that describe how the creator has granted permission for their work to be used to train AI, specifying the applicable restrictions (Centre for Strategic Futures, 2018).[12] If a data collector wants to use marked materials, they will log their use into a distributed ledger[j], creating an audit trail for documented consent. To address the demand for high-quality training data at scale, monetary compensation determined by the home country would flow to creators who contribute to commercial AI development. If a model generates harmful content using someone's likeness, the ledger will serve as documentation of consent, helping shift disputes from technical discussions to simpler dialogues.

Conclusion

Digital habeas corpus, structural separation, and decentralised consent verification each build on existing legal mechanisms as new applications. At the collision of technology, politics, and demography, the window for intervention is narrow and closing. We must decide today to reform foundational rules to meet the challenges of the digital age, or risk future generations losing their freedom to safeguard their own identity. This is not a technical problem awaiting engineering, but rather a political choice anticipating collective action. The annals of history will not question whether we had the power to act. It will ask why we did not.

[i] **Cryptographic Signatures:** A tamper-proof digital fingerprint attached to a file or form of media using a unique signature only known to the creator.
[j] **Distributed Ledger**: A tamper-proof record of transparent transactions, basis of blockchain technology

Reference List / Bibliography / Sources:

1. Polonetsky, Jules and Tene, Omer, Privacy and Big Data: Making Ends Meet (September 3, 2013). Stanford Law Review, Vol. 66, No. 25, 2013, Available at SSRN: https://ssrn.com/abstract=2628412
2. Das, A. (2026, January 14). Artificial Intelligence Legislative Update. Wilson Elser. https://www.wilsonelser.com/publications/artificial-intelligence-legislative-update
3. GDPR.eu. (n.d.). What is GDPR? A summary of the EU's General Data Protection Regulation. https://gdpr.eu/what-is-gdpr/
4. Nickerson, C. (2025, September 12). Latour's actor network theory. Simply Psychology. https://www.simplypsychology.org/actor-network-theory.html
5. Chung, Chee Hae and Schiff, Daniel, AI and the Social Contract (August 11, 2025). Proceedings of the Seventh AAAI/ACM Conference on AI, Ethics, and Society (AIES-25), Available at SSRN: https://ssrn.com/abstract=5387141
6. Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C.L., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A., Schulman, J., Hilton, J., Kelton, F., Miller, L.E., Simens, M., Askell, A., Welinder, P., Christiano, P.F., Leike, J., & Lowe, R.J. (2022). Training language models to follow instructions with human feedback. ArXiv, abs/2203.02155.
7. Freshfields Bruckhaus Deringer (2026). Data Law Trends 2026: Collective Privacy Claims and Model Collapse. https://www.freshfields.com/globalassets/our-thinking/campaigns/data-trends/2026-data-law-trends/2026-data-law-trends.pdf
8. EY. (2025, July). Almost half of employees fear losing their jobs due to AI. https://www.ey.com/en_ch/newsroom/2025/07/almost-half-of-employees-fear-for-their-jobs-because-of-ai
9. Schor Z. (2024, December 2). Andersen v. Stability AI: The Landmark Case Unpacking the Copyright Risks of AI Image Generators. https://jipel.law.nyu.edu/andersen-v-stability-ai-the-landmark-case-unpacking-the-copyright-risks-of-ai-image-generators/
10. Fedorczyk, Federica. (2026, January 14). Expert comment: Chatbot-driven sexual abuse (Grok case) just tip of iceberg. University of Oxford. https://www.ox.ac.uk/news/2026-01-14-expert-comment-chatbot-driven-sexual-abuse-grok-case-just-tip-iceberg
11. Administrative Office of the U.S. Courts. (n.d.). Glossary of legal terms: Habeas corpus. https://www.uscourts.gov/glossary-legal-terms/habeas-corpus
12. CSC (Centre for Strategic Futures) (2018, January 18). The Digital Social Contract and e-Legitimacy. https://knowledge.csc.gov.sg/ethos-issue-18/the-digital-social-contract-and-e-legitimacy/
13. Anthropic. (2025). *Claude* (Nov 24 version) [Large language model]. https://claude.ai/chat

Auxiliary Aids Directory

Aid	Usage	Affected parts
Private proofreading	Spell check	Complete paper
Claude	Image Generation	Figure 1

Word Count (essay text only): (2100/2100)