A Hegelian Dialectic: Data Sovereignty in the views of Goldsmith vs. Johnson & Post

Jim Sill

University of Tulsa

jim-sill@utulsa.edu

Dr. John Hale

University of Tulsa

john-hale@utulsa.edu

SHORT PAPER SUBMISSION

Extended Abstract

At its core, data sovereignty pertains to the principle that digital data is subject to the laws of the country in which it resides. This concept, while straightforward in theory, encounters numerous challenges in practice, given the global nature of the internet and the ease with which data crosses international borders. Data is free-flowing and boundless. Data is also transactional and ephemeral. Put simply, data is leveraged and then forgotten. Given these factors, the inability to determine who or what entity truly owns the data in question is a prominent concern in this discourse.

The concept of data sovereignty has emerged as a focal point in industry and academic discussions alike surrounding the governance, privacy, and security of digital data. In today's digital economy, data assumes the role of a critical asset. Consequently, the need to understand and navigate the complexities of data sovereignty becomes paramount. This paper delves into this evolving discourse, examining its implications for privacy, security, and global governance against the backdrop of technological advancements and shifting legal landscapes. This is necessary as the determination of data's exceptionality becomes more crystalized.

This paper explores the tension between traditional notions of territorial sovereignty, as advocated by scholars such as Goldsmith (Goldsmith, 1998), and the calls for a more fluid, global governance approach, as proposed by Johnson & Post (Johnson, 1996) (Svantensson, 2016). Goldsmith's perspective emphasizes the jurisdictional authority of nations over data existing within their borders, as well as that possessed by, or owned by their constituents. Goldsmith's perspective, rooted in the concept of territoriality, asserts that data, much like tangible assets, should be subject to the laws of the nation within which it resides or is processed. Such a viewpoint, while grounded in traditional legal paradigms, struggles to address the multifaceted realities of modern cyber architectures. As data flows seamlessly across borders, through distributed networks, and is accessed globally, the very notion of a geographically bound *"home"* for data becomes untenable. The territorial approach, while offering clear legal boundaries, often finds itself in a state of *"legal lag,"* unable to accommodate the agile and borderless nature of contemporary digital interactions.

Johnson & Post argue for governance models that transcend national boundaries, reflecting the inherently international character of data. They posit a more fluid framework, suggesting that cyberspace exists as its own domain, distinct from traditional geophysical boundaries. Their viewpoint, which resonates more closely with the operational realities of global cyber architectures, posits that traditional territorial laws may be ill-suited to govern the unique challenges of the digital domain. By detaching data from strict geophysical jurisdictions, they acknowledge the inherent fluidity and dynamism of digital exchanges, paving the way for a modern legal framework that is more in sync with current practice, and future technological advancements.

In the face of rapid digital transformation, it becomes evident that clinging to rigid territorial-based legal frameworks might lead to misalignments and injustices. The modern digital landscape, characterized by cloud platforms, decentralized systems, and ubiquitous connectivity, finds a more natural ally in the non-territorial viewpoints of scholars like Johnson and Post. Both cases provide for such a variety of control mechanisms to be required by one view, and voluntarily applied by another.

Data sovereignty is further complicated by pressing concerns over personal privacy rights and national security. Revelations of mass surveillance programs and the exploitation of personal data by state and non-state actors have propelled data sovereignty to the forefront of public and academic debate. The paper examines how these developments, particularly the Snowden revelations and the enactment of significant regulations such as the Chinese regulatory model, the GDPR and the USA Freedom Act, have influenced public awareness and regulatory bodies. These regulatory platforms, and security events underscore the delicate balance between safeguarding privacy and ensuring national security in the digital age.

Either through litigation or regulatory findings, organizations are facing multimillion-dollar settlements. All of which reveals that many organizations are not performing at the minimum regulatory or contractual levels they proclaim. Legal and policy responses to the challenges of data sovereignty are varied and often complex. Here, we analyze landmark legal decisions, current case law, and the regulatory and legislative efforts of various jurisdictions, that seek to address the jurisdictional dilemmas posed by global data flows. Modern legal frameworks must account for the ongoing struggle to achieve a coherent and effective governance model for data sovereignty that respects privacy rights while accommodating the needs of law enforcement and national security.

These specific arguments set the stage and create the perfect groundwork for viewing data exceptionality as a Hegelian Dialectic. This dialectic will be applied to a thematic content evaluation of 776 data sources from academic journal & conference papers, corporate white papers, nongovernmental organizational reports, regulatory standards, and other documents. This analysis will elucidate organizational sentiments on the exceptional or nonexceptional nature of data. Such a study is a critical first step to understanding the posture of principal global actors regarding data sovereignty.

Navigating data sovereignty issues requires a nuanced understanding of the interplay between technology, legal frameworks, and the ethical imperatives of privacy and security. It calls for a balanced approach that recognizes the limitations of traditional territorial models while seeking to develop global governance structures that can protect individual rights and foster innovation in a digital world. From this a modern global framework will be developed.