

# **A Hegelian View of Data Sovereignty**

## **Completed Paper**

**Jim Sill**

University of Tulsa  
School of Cyber Studies  
College of Engineering and  
Computer Science  
[jim-sill@utulsa.edu](mailto:jim-sill@utulsa.edu)

**Dr. John Hale**

University of Tulsa  
School of Cyber Studies  
College of Engineering and  
Computer Science  
[john-hale@utulsa.edu](mailto:john-hale@utulsa.edu)

**Dr. Stephen Flowerday**

University of Tulsa  
School of Cyber Studies  
College of Engineering and  
Computer Science  
[stephen-flowerday@utulsa.edu](mailto:stephen-flowerday@utulsa.edu)

## **ABSTRACT**

This paper explores the contrasting perspectives on data sovereignty, focusing on the debate between data exceptionalism and non-exceptionalism. Data exceptionalism, as supported by Goldsmith (1998), advocates for territorial data control, emphasizing that certain data types, such as personal, biometric, and financial information, require unique governance and protection due to their inherent sensitivity and impact. In contrast, Johnson & Post (1996) argue for a borderless approach, where data flows freely across borders with consistent privacy protections, rejecting geographic localization. By employing the Hegelian dialectic, this paper critically analyzes these opposing views while proposing a federated approach to data sovereignty. This approach aims to reconcile the demands of territorial data control with the realities of global data flow, addressing the challenges posed by data exceptionalism in the context of artificial intelligence (AI), the Internet of Things (IoT), and data aggregation. The discussion highlights regulatory challenges, ethical concerns surrounding privacy and ownership, and the growing demand for sensitive data such as genetic information. The paper advocates for a more nuanced and unified global governance model that transcends current frameworks, offering insights for future legislative solutions that balance data sovereignty with the fluid dynamics of the digital age.

## **Keywords**

*Data Sovereignty, Data Territoriality, Data Exceptionality, Data Privacy, Data Aggregation, Mosaic Theory, Artificial Intelligence (AI), and Internet of things (IOT).*

## **1.0 INTRODUCTION**

In this paper we propose to answer the following research question: *"How do governments and stakeholders view data sovereignty, through the lens of data exceptionalism?"*

Data exceptionality refers to the idea that certain types of data are inherently more sensitive, valuable, or impactful than others, requiring special handling, protection, or regulation. Exceptional data often includes personal, biometric, genetic, financial, or health related information. In a governance context, data exceptionality often influences policies around data localization, privacy laws, and data's sovereignty. Acknowledging misuse or mishandling of this data can lead to significant legal, ethical, and social harm. Whereas data non-exceptionality regardless of sensitivity, should be treated uniformly without being given special status or requiring distinct handling. In this view data is considered part of the broader information ecosystem and is subject to general privacy, security, and governance frameworks without additional layers of protection or regulation. Proponents of this view argue that treating all data consistently helps create simpler, more uniform regulations and fosters a free flow of data across borders, whereas data is not geographically bound.

This paper contributes to the field of data sovereignty by reviewing artifacts and critically analyzing the contrasting paradigms of Goldsmith's territorial, jurisdiction-bound model and Johnson & Post's non-territorial, borderless framework. It addresses the core dilemma of whether data should be tied to specific geographic jurisdictions or managed within a borderless digital

ecosystem. By exploring the debate over the *"exceptional"* vs. *"non-exceptional"* nature of data, we offer insights into how data should be perceived and managed across different jurisdictions and organizations.

This exploration is crucial for developing a future regulatory framework that balances the benefits of both territorial and borderless approaches, supporting the advancement of cloud architectures and data mesh networks. Furthermore, we analyze current regulations and emphasize the need for a more nuanced approach that respects individual privacy rights, national sovereignty, and the global nature of data. We highlight the challenges posed by our rapidly evolving technologies and the need for more robust oversight, clearer regulations, and individual consent mechanisms. These contributions provide a foundational understanding for future legislative and technological strategies to effectively manage the complexities of global data governance, reflecting prevailing values and attitudes in the research area of data sovereignty.

As data has emerged as a power commodity in our modern world (Jadon, 2015; Fick 2020; Bhageshpur, 2019), it has also brought forth a novel and complex concept: Data sovereignty. This concept, with its far-reaching implications, pertains to the governance of data, involving the questions of who owns the data, who has the right to store and process it, and under which jurisdiction data-related issues should be resolved (Hummel, 2021; Ahern, 2021). The principle of data sovereignty is increasingly important in today's digital economy, where data is often viewed as an asset rather than merely as a medium (Bhageshpur, 2019). It forms the crux of discussions around data ownership, privacy, surveillance, user profiling, and security (Véliz, 2024). Each of these viewpoints, whether data is seen as an asset, being exceptional in nature, or merely a medium, being non-exceptional, presents their own distinct complexities and challenges.

The utilization of data mining, data extraction with scraping, and the misuse of AI have ethical implications that are only just now being questioned in the sphere of data sovereignty. Examining the ethics of data aggregation and the application or misapplication of the “*mosaic theory*” violates personal privacy in ways only a few years ago would have been considered science fiction. The use of mosaic theory analyzes disparate bits and pieces of innocuous information to reveal the whole person, their habits, their thoughts, and their being. Ethically these pieces in whole erode individual privacy rights (Htigel, 2007; CRD, 2009). Exceptional data and non-exceptional data proponents are at odds; on one side, there is a strong public demand for enhanced privacy protections and stricter data localization, while on the other, there is a push for greater liberty, autonomy, and broader access to data (Gavison, 1980). Exceptionalists who align with the Goldsmith viewpoint argue that data must be protected and kept localized under complex governance structures, while non-exceptionalists, following the Johnson & Post perspective, believe data should flow freely with uniform privacy protections, without being restricted by geographical boundaries. These contrasting perspectives of scholars like Goldsmith (1998) and Johnson & Post (1996) offer a dialectic framework for discussing the complex landscape of data sovereignty. Goldsmith's approach to data sovereignty is rooted in “*Western*” legal history, forming the principle of territorial sovereignty, which maintains that a jurisdiction's legal authority is paramount within its own borders (Svantensson, 2016). This viewpoint prescribes that the data is exceptional, advocating that the scope of authority for its management and control can be confined and managed within the jurisdictional boundaries of nations or states. Data exceptionalists demand that data remain localized. Conversely, Johnson & Post contend that the nature of data defies such exceptionalism, stating that data is non-exceptional, necessitating a global perspective on data sovereignty and localization (Yayboke, 2021; Zhang, 2023). These non-

exceptionalists support a federated, cloud-based system where data is not necessarily geographically bound or held to data localization governance and regulatory requirements. They advocate for governance structures that transcend traditional concepts of territorial sovereignty, recognizing the fluid and mobile nature of data in the digital age.

The internet and data networks are evolving rapidly, expanding to a global scale that surpasses the scope of localized privacy doctrines, regulations, and governance frameworks. As a result, nations have started exploring open strategies for data collection and protection. Data sovereignty, exceptionalism and non-exceptionalism become even more unclear when competing interests are involved.

The Economist characterizes data as a new kind of raw material, comparable to capital and labor (The Economist, 2010). Framing data as a resource allows for comparisons between data mining and the extraction of oil or other commodities. Law professor Scholz critiques this analogy, arguing that it is flawed because, unlike finite oil, data can be accessed and utilized by multiple parties simultaneously to generate information and value (Scholz, 2018). Other analysts suggest that data functions as a form of capital that can be leveraged within and across organizations, as seen in data-driven companies like Google, Facebook, Amazon, Microsoft, Snowflake, Alteryx, and Informatica, which commodify and monetize data to create new revenue streams or enhance operational capabilities (Sadowski, 2016; MIT Technology Review, 2016).

Some scholars further argue that personal data constitutes a form of property, allowing individuals to assert rights over its control and access (Scassa, 2018). This idea underpins the European Commission's General Data Protection Regulation (GDPR), which positions certain types of data as personal property. Under such a regulatory framework, corporations would be required to pay for permission to collect and use data, potentially eliminating the model of offering free services.

Non-exceptionalists would note that this approach could incentivize companies to keep data accurate and secure. However, exceptionalists would caution that viewing data as property frames it like a natural resource, where economic prosperity hinges on its extraction and processing. In this scenario, privacy becomes a competing claim for control, balanced against the ownership rights of those extracting and monetizing data, raising concerns about the potential for misuse of personal information.

Policymakers in China tightly control the flow of data, both across borders and within the country, to maintain social stability and the authority of the Communist Party (Aaronson and Leblond, 2018). As China participates in negotiations for the Regional Comprehensive Economic Partnership (RCEP)—involving nations like Australia, India, Japan, and ASEAN members—there is uncertainty about whether it will accept provisions on free data flow and privacy, given its strong stance on internet control. This uncertainty reflects broader divergences in data governance between major markets: the United States, the European Union, and China. Countries like Canada, Mexico, and Australia, which maintain trade ties with all three, face challenges due to differing regulatory standards. Aligning with multiple markets could increase compliance costs as they navigate these fragmented data governance systems (Carson, 2014). As data usage evolves, so must governance frameworks to ensure adequate protection (Aaronson, 2018). An example of the disparities which exist in the patchwork methodologies currently being applied can be seen below in *Table 1*, where a few of the over 140 different governance frameworks are on display.

	<b>Comprehensive</b> [European Union   China]	<b>Co-Regulatory</b> [Canada   Australia]	<b>Sectoral</b> [USA   Japan]	<b>Self-Regulating</b> [PCI / DSS]
<b>Bodily</b> [Physical Being]	<p><b>China:</b> PII &amp; PHI prohibited from transfer, without consent.</p> <p><b>EU:</b> PHI cannot be maintained outside of certain member states. Should data sharing of PII occur, with consent, “effectively equivalent” standards and protections must be met.</p>	<p><b>Canada:</b> PII &amp; PHI held by a public body will be maintained territorially. PII &amp; PHI maintained personally, is prohibited from transfer, without consent. If transferred “effectively equivalent” standards and protections must be met.</p> <p><b>Australia:</b> PHI cannot be maintained outside of Australia. Should data sharing of PII occur, with consent, “effectively equivalent” standards and protections must be met.</p>	<p><b>USA:</b> Local storage requirements are contract and clause dependent. Excluding PHI no restriction of data flow. Data sharing is conditional and varies by member state.</p> <p><b>Japan:</b> Data flow is conditional only by required “effectively equivalent” protection(s) are required for PII &amp; PHI</p>	<p><b>Contractual Clause:</b> All data flow is regulated by express and specific consent. Content, contract, and clause specific restrictions. Data sharing is conditional and varies by members affiliated or represented in the agreement(s).</p>
<b>Territorial</b> [Availability & Access Control]	<p><b>China:</b> Data Residency Requirement. (Banking; Health; Governmental; Social Content; Personal Data)</p> <p><b>EU:</b> Data Residency Requirement. Each data subject has the authority and right to modify, delete, and request to remove all PII &amp; PHI data. Some PHI data is prohibited from removal.</p>	<p><b>Canada:</b> Provincial territories must be respected. Data shall remain within each territory. Data sharing is conditional.</p> <p><b>Australia:</b> Excluding PII &amp; PHI, no restriction(s) of data.</p>	<p><b>USA:</b> Local storage requirements are contract and clause dependent. Data sharing is conditional and varies by member state.</p> <p><b>Japan:</b> Data flow is conditional only by required “effectively equivalent” protection(s) are required for PII &amp; PHI.</p>	<p><b>Contractual Clause:</b> All data flow is regulated by express and specific consent. Content, contract, and clause specific restrictions. Data sharing is conditional and varies by members affiliated or represented in the agreement(s).</p>

**Table 1** – Regulatory Evaluation of Some Current Laws of a Fragmented Internet

(CFR: Task Force Report No. 80)

<b>Communication</b> <i>[Confidentiality Standards]</i>	<p><b>China:</b> All electronic communication(s) will be filtered, and certain communication(s) will be prohibited.</p> <p><b>EU:</b> No restriction(s) of data. Data sharing is conditional and varies by member state.</p>	<p><b>Canada:</b> Excluding PII &amp; PHI, no restriction(s) of data flow.</p> <p><b>Australia:</b> Excluding PII &amp; PHI, no restriction(s) of data.</p>	<p><b>USA:</b> Local storage requirements are contract and clause dependent. Data sharing is conditional and varies by member state.</p> <p><b>Japan:</b> No current restriction(s) of data.</p>	<p><b>Contractual Clause:</b> All data flow is regulated by express and specific consent. Content, contract, and clause specific restrictions. Data sharing is conditional and varies by members affiliated or represented in the agreement(s).</p>
<b>Digitalization</b> <i>[Data Collection &amp; Data Storage]</i>	<p><b>China:</b> PII &amp; PHI required to be maintained territorially. Data sharing is prohibited.</p> <p><b>EU:</b> Data sharing is conditional and varies by member state.</p>	<p><b>Canada:</b> Excluding PII &amp; PHI. Data sharing is conditional.</p> <p><b>Australia:</b> Excluding PII &amp; PHI, no restriction(s) of data.</p>	<p><b>USA:</b> Local storage requirements are contract and clause dependent. Excluding PHI no restriction(s) of data flow. Data sharing is conditional and varies by member state.</p> <p><b>Japan:</b> No current restriction(s) of data.</p>	<p><b>Contractual Clause:</b> All data flow is regulated by express and specific consent. Content, contract, and clause specific restrictions. Data sharing is conditional and varies by members affiliated or represented in the agreement(s).</p>

**Table 1 (continued)** – Regulatory Evaluation of Some Current Laws of a Fragmented Internet  
(CFR: Task Force Report No. 80)

Whether data is considered exceptional or non-exceptional seems to be determined by a multiple of dependencies; the data product, the data processing, the location where data is stored, the type of storage, the way data is transferred, and how data is accessed. All of these are affected by the perspectives of both the exceptionalist and non-exceptionalist alike. At the heart of the data sovereignty debate lies a core concern: The ethical treatment of individuals' privacy and digital rights (Oktay, 2023). The internet has enabled individual surveillance on a new scale as the use of artificial intelligence is paired with personal data (Calderaro, 2022). Individuals and organizations, in the United States are caught between outdated legal systems and the expansion of the public's viewpoint of a reasonable expectation of privacy (Warren, 1890; Katz, 2023). Various nation-



states' data ownership and data sovereignty claims are igniting a digital cold war punctuated by technological advances in data aggregation methods and data analysis tools (Geist, 2015).

As discussed, nations, states, organizations, and individuals have competing interests in the use and limitations of data. Many applications track online activities, including geophysical location, raising issues of digital freedom, human rights, and the need for global cyber diplomacy. A significant number of data sources today come from scraping and aggregation efforts. Inferential data and data aggregation create a force multiplier effect on the impact of technology on data sovereignty (Jarke, 2020) capturing both personal identifying information (PII) and personal health information (PHI), fulfilling the mosaic theory with and without intent. The complexities surrounding data's classification as exceptional or non-exceptional, shaped by factors such as storage, transfer methods, and access, reflect broader concerns about the ethical treatment of privacy and digital rights. This debate becomes even more pronounced when considering the growing reliance on data aggregation and inferential analysis, which have transformed the landscape of data sovereignty. As technology advances, so does the demand for more sensitive forms of data, particularly genetic information. Indigenous sovereignty, in this context, emerges as a latent theme, as the highly prized nature of genetic data, driven by developments in biotechnology and bioinformatics, further complicates issues of privacy, ownership, and surveillance. These advancements blur the lines between personal privacy and state or corporate control, raising critical questions about the future of individual and collective digital rights. Our genetic data is the most highly prized commodity in data aggregation (Kukutai, 2023). The demand for it is fueled by advances in biotechnology, and bioinformatics which have delivered powerful new tools to medicine and law enforcement (ALRC, 2002; Alban, 2023; Whitmore, 2023). While

surveillance technologies track urban movements through facial recognition systems and sensors (Fussell, 2023; CBS News, 2013; Shivaskeshi, 2022).

## **2.0 INTRODUCTION TO DATA SOVEREIGNTY**

The golden age of borderless data, and “*free internet*” (Barlow, 1996) is coming to an end, giving way to a federated convergence of multi-jurisdictional standards and regulations across markets and geographical regions (Fick, 2022; Brehmer, 2018). Policy architects and politicians understand data sovereignty as national dominion over data within their territory (Jarke, 2020). Organizations across industries understand data sovereignty as ownership of data, regardless of territorial boundaries (Zhang, 2023). Traditionally, the concept of sovereignty refers to the full right and power of a body to govern itself without any interference from outside sources (Yayboke, 2021). In the context of cyberspace, data sovereignty posits that information is subject to the laws of the country where it is located, impacting how businesses operate and how countries govern. The debate around data sovereignty is not limited to a nation state’s control. It extends to private organizations, corporations, and individuals who generate, process, and store data, raising questions about territoriality, control, ownership, and privacy (Yayboke, 2020). At the birth of the internet in 1983 those involved agreed that there was a need for a set of rules and regulations surrounding data governance, data sovereignty and this new cyber domain (Rectenwald, 2015). It took thirty more years of subjecting data to abuse, before a global awakening occurred (Chilton, 2017).

Snowden's 2013 disclosure of classified information about the NSA’s PRISM program exposed how global data privacy could be compromised. The program had been systematically monitoring email communications worldwide. This data mining, farming, and propagation included those of Americans, directly violating the US citizens right to privacy, search, and seizure. In certain other

people groups it too violated their civil liberties. The programs collection and propagation tools scrutinized, and archived documents, photographs, and biometric data of those screened. These stunning revelations sparked widespread debate about an individual's privacy, civil liberties, and the role of government, continuing the argument over what is necessary vs. valid and served as a significant wake-up call to all global citizens, highlighting the potential for violations of individual privacy on an international scale (Brehmer, 2018). Revealing the misconceptions of territorial data governance, Snowden's disclosures uncovered the underlying power struggles over data ownership and highlighted the pervasive reach of the surveillance state.

The exposure of the NSA and Britain's GCHQ, along with their silent partners in the '*Big Tech*' space caused the intelligence community severe reputational damage (Kerry, 2020; Ünver, 2018). The release also forced Silicon Valley to appear to become more transparent and to advocate for the individual, the data subject. These revelations also brought into focus the critical debate between the notions of the classification of data. Should data be treated as exceptional data, or should it be treated as non-exceptional data? This dialectic is the basis and the fundamental question of individual sovereignty (Taichman, 2021; Daskal, 2015; Brehmer, 2018). The abuses by global governments, and the general mistrust in public consciousness, and policy concerning privacy, led countries to reevaluate their data policies, laws, and enforcement practices (HPR, 2013; Toomey, 2018; Chapman, 2024; Woods, 2018).

The United States Freedom Act, passed in 2015, was intended to close the door on the United States Patriot Act, including the Tempora, Dishfire, and PRISM programs. The United States Patriot Act never netted a terrorist, but the government still used the legislation as an excuse to expand the electronic surveillance platforms for itself and its allies (Preuss, 2018; Lind, 2015). The governmental initiative was meant to rebuild public trust in government. The increased

transparency requirements of the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Act (FISA) court proceedings were seen as positive, as were the frameworks to limit the amount of data accessible to government agencies without a warrant (Lin, 2017). In 2018, the implementation of the European Union General Data Protection Regulation (GDPR) marked a significant milestone in the field of data protection and digital rights. This landmark legislation not only reinforced data sovereignty on an individual level, allowing European citizens with an unprecedented level of control over their personal data (Kelly, et al., 2019). Additionally, it established stringent guidelines for businesses responsible for managing the data of EU residents. The GDPR constituted a complete overhaul of the 1995 Data Protection Directive (DPD). While this legislation is specific to the EU member states, and their citizens – globally many mimics of these regulatory concepts are being adopted. All to protect the sovereignty of the individual's data privacy rights, allowing them more control over their individual data.

Although the GDPR was not adopted until 2016, its broad new concepts and directives for an individual's data were based upon changes to data regulations from four decades prior, in the German Constitution, after being amended in 1977, which secured individual rights to have aggregated data deleted. Influence also came from an even more progressive modification and amendment to the French Constitution, in 1978, which secured the rights of the individual to make corrections to aggregated data (Bendiek, 2016). The adoption of the GDPR empowered “*data subjects*,” granting them the right to insist that digital data be corrected upon demand, deleted upon demand, and protected at an “*effectively equivalent*” level for all European Union citizen's sovereign data. Importantly, these rights are conferred irrespective of the geographical territoriality or the physical residency of the data. The GDPR facilitates ease of use of data by incorporating

provisions for data transparency and data portability. These functions, however, operate within the defined boundaries of the regulation, ensuring that the data remains safeguarded while also promoting its flexibility for legitimate use. In this way, the GDPR succeeded in instituting a comprehensive framework for data sovereignty. The data subject also gains significant control over what data can be maintained by data owners through the “*right to erasure*” clause within the regulation. Finally, with GDPR and its mimics, strong penalties act as a deterrent to companies and organizations that otherwise may fail to comply with its regulations.

The United States Clarifying Lawful Overseas Use of Data (CLOUD) Act enacted in 2018 creates a legal framework for United States law enforcement to access data across borders (Kosseff, 2020). Consequently, this act holds implications for data sovereignty worldwide. It required the establishment of conditional restrictions for the sharing and storage of United States Persons (USPER) data. This extension and expansion of United States data territoriality regulations have given rise to more confining data localization, mandating data residency. Other countries like Russia, China, and India have developed similar regulations for their citizens. Continuing the relationship with the European Union, the United States has become more aligned with the GDPR. However, through the CLOUD Act, organizations, states, and jurisdictions have all become an open book to law enforcement agencies regardless of where the data is located, once mutually lateral agreements, such as Structural Clause Contracts (SCC), have been applied. This has required certain assurances between agencies and data-controlling entities to support data sovereignty through legal and jurisdictional measures, all centering upon access need (Singi, 2020). This has been highly controversial, as some jurisdictions do not trust others’ direct adherence to the regulation. While the CLOUD Act has denied some law enforcement and intelligence gathering entities access to data they previously enjoyed, it has supported the data

subject more completely, therefore, upholding data sovereignty for the data subject and data owner.

Data sovereignty for individual rights has been at the forefront of most regulatory decisions in the past five years. Data brokers and data capitalists, like Google, Facebook, Amazon, Microsoft, Snowflake, Alteryx, and Informatica and their lobbyists have contributed to an overall regulatory lag in the governance of personal data rights. These entities have developed sophisticated risk management frameworks to safeguard corporate data, much of which comprises the personal information of individual users. However, within the evolving regulatory landscape, data capitalists must remain cognizant of the significant financial and operational costs associated with noncompliance. Beyond regulatory penalties, breaches of data security also carry substantial risks, including the loss of sensitive information and potential damage to corporate reputation, which can have long-term impacts on business sustainability.

The legal system in the European Union and the United States have fined and penalized many organizations, as they have been found negligent in their duties to provide effectively equivalent protections. In May 2023 Meta was fined \$1.3 Billion dollars (USD) by the European Union and \$5 Billion by the United States (Cook, 2022). In the Schrems II case from 2020, the European Union Court of Justice invalidated the European Union–United States Privacy Shield agreement, as effectively equivalent protections were not being provided, highlighting the legal complexities of data transfer and data storage (Brehmer, 2018). Prior to the Schrems decision the European Union and the United States loosely governed personal data between the various jurisdictions (Yayboke, 2021). However, the discoveries uncovered in the Schrems I & II cases (Norton Rose Fulbright, 2023), and the fine imposed on Meta, precipitated a disruption throughout the telecommunications and technology sectors forcing jurisdictions to realign their governance and

regulatory environments to enforce effectively equivalent protections. This nullified many older regulations and brought into question the validity of Structural Clause Contracts (SCC) (Zanon, 2022).

### **3.0 HELEGIAN DIALECTIC OF DATA EXCEPTIONALISM**

The Hegelian dialectic is a philosophical method that explains the progression of ideas and historical events through a three-stage process: “*Thesis*,” “*antithesis*,” and “*synthesis*.” This process suggests that conflict and contradiction drive the evolution of thought and societal changes, continually leading to new states of understanding and development (de Meij, 2016). Hegel posits that the internal relationships between entities—whether people, ideas, or in this case, data—are characterized by inherent tensions. These tensions, he argues, are what lead to their definition or synthesis into a greater truth. We apply this philosophical methodology to Goldsmith’s and Johnson & Post’s viewpoints on data exceptionality. Proponents of exceptional and non-exceptional data governance are divided on issues of privacy and data localization. Exceptionalists, aligned with Goldsmith's viewpoint, argue for strict privacy protections and localized data governance, emphasizing that data should remain within national borders and be managed under complex regulatory structures. This view is rooted in the traditional principle of territorial sovereignty. Conversely, non-exceptionalists, following Johnson & Post’s perspective, advocate for the free flow of data across borders with uniform privacy protections, rejecting the notion of data localization. They argue that data is inherently global and should be governed through cloud-based systems that transcend national boundaries. As data networks rapidly evolve, nations are exploring new strategies for data collection and protection, with both developed and developing countries expressing concerns over safeguarding sensitive information.

Goldsmith's perspective is rooted in the concept of territoriality and asserts that data, much like tangible assets, should be subject to the laws of the nation within which it resides or is processed (Goldsmith, 1998; Svantesson, 2016). An exceptionalists viewpoint, while grounded in traditional legal paradigms, struggles to address the multifaceted realities of modern digital architecture. As data flows seamlessly through distributed networks, and across borders the very notion of a geographically bound home for data becomes untenable (Kosseff, 2018). This 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 (Cook, 2022; Véliz, 2024). As stated before, data capitalists and their adherents resist change, as change creates costs and can expose data when risk management frameworks are new and being implemented.

On the other hand, the perspectives of Johnson & Post posit a more fluid framework, suggesting that cyberspace exists as its own domain, distinct from traditional geophysical boundaries (Johnson, 1996; Woods, 2016; Chilton, 2017). The non-exceptionalist's viewpoint, which resonates more closely with the current operational realities of global cyber architectures, observes that traditional territorial laws may be ill-suited to govern the unique challenges of the digital domain. While this is only one possibility, 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 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 (Kilovaty, 2020). The modern digital landscape, characterized by cloud platforms, decentralized systems, and ubiquitous connectivity, finds a greater affinity with the non-territorial viewpoints of scholars like Johnson & Post.



Landmark regulations like the European Union's General Data Protection Regulation (GDPR) and its mimics have set standards, granting individuals extensive control over their personal data, and challenged organizations to protect that data, regardless of territoriality (Huddleston, et al, 2023). These developments also bring forth challenges. Issues of consent, data breaches, invasive surveillance, and the lack of effectively equivalent data protection policies, have created environments where discriminatory profiling has become more prevalent with the misuse of data mining and harvesting techniques by individuals and artificial intelligence systems (Martin, 2020). Modern organizations need to process and analyze data in real time, or risk being left behind (MIT, 2023).

In the domain of data sovereignty and ethical application of AI, the United States grapples with its own regulatory problems, manifesting a patchwork of multifaceted and occasionally contradictory legal frameworks (Huddleston, 2023; Ferracane, 2018). These encompass various stipulations pertinent to data territoriality, data storage, data usage, and ethical AI deployment. As visited earlier, the fines and penalties for noncompliance can be punitive. The regulations mandate rigorous penalties for non-adherence (Ferracane, 2017; Kochovski, 2022). The heterogeneous and potentially conflicting nature of these regulatory frameworks elicit notable challenges for compliance and uniform implementation across diverse digital platforms and industries.

Industry specialists and subject matter experts' express apprehension concerning the progressively stringent regulatory environment. A prevailing perspective among these experts is that the rigid regulatory mechanisms, particularly those involving exorbitant fines and rigorous compliance standards, may inadvertently hinder technological advancements (Véliz, 2024). Within the 'Big Tech' space there is a palpable concern that such a restrictive regulatory milieu could regress the United States' position in the digital and AI sectors by several decades (Thierer, 2023).

In the final decade of the 20th century Goldsmith elucidated a perspective asserting that, notwithstanding the extensive global integration facilitated by the internet, data cannot extricate itself from the frameworks of territoriality and sovereignty (Goldsmith, 1998). To distill his argument, Goldsmith maintained that data invariably remains subject to the laws of the nation within which it is housed or undergoing processing. In contrast, Johnson & Post argue that data cannot be held to Goldsmith's standard, because cyberspace is its own geo-meta-physical domain, having its own territoriality, invalidating those of the actual physical world, through detaching data from its physical jurisdiction, and their traditional standing sovereignty laws (Johnson, 1996).

Goldsmith   Exceptional Data		Johnson & Post   Non-Exceptional Data	
<b>Key Beliefs   Concepts</b> <ul style="list-style-type: none"> <li>Data is "<u>Exceptional</u>."</li> <li>Data holds intrinsic value, such as an asset.</li> <li>Data is localized.</li> <li>Data has established territoriality.</li> <li>The creation of data, and the storage of data will be governed by the rules of the sovereign under whose geo-physical domain it resides.</li> <li>The localization of physical devices "<i>storing, processing, or using</i>" data is a primary function.</li> <li>The dynamism of data is challenging and can be hindered by territoriality requirements.</li> <li>Data is monolithic.</li> </ul>	<b>Advantages</b> <ul style="list-style-type: none"> <li>Supports strong data protection.</li> <li>Allows independent collaboration, by interested third parties, due to no banned access transfer rules.</li> <li>Nation-State sovereignty is clearly defined and is supported through data localization, and territoriality.</li> </ul> <b>Disadvantages</b> <ul style="list-style-type: none"> <li>Immobility of data.</li> <li>Not always adaptable or suited to "<i>Cloud Architecture</i>."</li> <li>Requires Independent Security Standards.</li> <li>Regulatory complexity, through adoption of a patchwork of standards and practices.</li> </ul>	<b>Advantages</b> <ul style="list-style-type: none"> <li>Best suited for modern distributive systems and "<i>Cloud Architecture</i>."</li> <li>Data is flexible &amp; agile.</li> <li>Data is "<i>Global</i>" holding no "Geophysical" territoriality.</li> <li>Greater data availability and redundancy.</li> <li>Supported by a federated governance framework.</li> </ul> <b>Disadvantages</b> <ul style="list-style-type: none"> <li>Data is "<i>ephemeral</i>." No long-term storage exists.</li> <li>Regulatory complexity can become cumbersome due to expanded data availability, requires balanced governance and adaptability.</li> <li>Data is not localized and has no established "<i>natural home</i>."</li> </ul>	<b>Key Beliefs   Concepts</b> <ul style="list-style-type: none"> <li>Data is "<u>Non-Exceptional</u>."</li> <li>Data is a medium, much like money. It holds value, in its use.</li> <li>Data has no borders. It resides in varied states and can cross multiple borders instantaneously. Therefore, data cannot be constrained to any individual geophysical location or sovereign.</li> <li>Data should be deleted after its use, or function is completed.</li> <li>Data sovereignty is global in nature and must be treated as so. It is independent of individual regulations or standards.</li> <li>Requires unified governance framework.</li> </ul>

**Figure 1 - Views of Goldsmith vs. Johnson & Post**

These two positions only become more tense and adversarial once the actors have decided whether data ought to be considered exceptional, an asset linked to and stored in a geographical location,

or non-exceptional simply a temporal or ephemeral medium, regardless of its various storage locations, or in which state the data resides.

As we continue to grapple with the ethical, legal, and technical ramifications of data sovereignty, it is likely that our understanding and treatment of data will undergo significant changes in the years to come. The modern cloud architectures utilize a data mesh framework, which is aligned with the Johnson & Post viewpoint. But it is consistently bombarded with the constraints of legal and regulatory frameworks that represent the Goldsmith viewpoint (Dehghani, 2022). Under Goldsmith's approach, the potential legal harms include varying levels of data protection, privacy standards, and surveillance regulations across different jurisdictions. In addition, the decentralized nature of modern data storage architecture is reflective of the legal and policy documents governing them. This inconsistency leads to situations in which data is monolithic and less protected and more susceptible to misuse (Gold, 2019). In our current immature state, multinational corporations might exploit these disparities, leading to social harm such as privacy breaches and the exploitation of personal data for commercial gain. By contrast Johnson & Post's perspective raises concerns about the absence of a unified global legal framework to address issues such as data privacy, security, and surveillance, which promulgates the risk of a "*race to the bottom*" in terms of data protection standards, where entities choose jurisdictions with the least stringent regulations (Ahern, 2021). Moreover, global surveillance practices might infringe on individual rights and freedoms, leading to social harms like loss of autonomy, increased state control, and the erosion of democratic norms (Solove, 2008; Toomey, 2018). This exploration of data sovereignty through the lens of data exceptionalism, using the Hegelian dialectic offers an insightful perspective on the challenges and tensions at play amongst the competing stakeholders.

## **4.0 STUDY METHODOLOGY**

In alignment with the methodological framework established by Peters (2020), this paper provides a scoping review structured to encompass three distinct phases, affording a comprehensive examination of the literature. The phases included are:

- *Study Retrieval:* During this initial phase, we conduct an extensive search of relevant databases and sources. This phase involves identifying potential documents that align with the predefined criteria set for this review. The search is systematic, using specified keywords and Boolean operators to ensure that all pertinent literature is considered (Appendix A: *Keyword Search String Values*).
- *Study Selection:* This phase involves a critical appraisal and selection of documents. Using inclusion and exclusion criteria derived from the research questions and objectives, we carefully evaluate the documents for relevance and rigor.
- *Data Analysis:* The final phase of the research design strategy involves analyzing the data extracted from the selected documents. Using an inductive thematic analysis approach, we identify, and document key themes related to values, attitudes, and beliefs. This qualitative analysis allows us to explore underlying patterns and relationships among themes, providing insights into the sentiment and perspectives prevalent in the existing body of research.

Through these phases, the scoping review aims to thematically interpret the prevailing values, attitudes, and beliefs within the research area. Inductive analysis facilitates a deeper understanding of the interconnections and sentiments that characterize the discourse in the field, thus contributing to a nuanced synthesis of the extant literature. This structured approach not only aligns with the guidelines set forth by qualitative research methodologies (Peters, 2020; Saldana, 2021) but also

enhances the clarity, depth, and breadth of the analysis, providing a solid foundation for future research endeavors in this domain.

### ***4.1 Study Selection***

According to the methodology, the PCC Framework (Population, Concept, Context) defines the inclusion criteria (Munn, 2018). To gather and extract the most relevant literature, a comprehensive search strategy was implemented. This approach included traditional academic sources, such as scholarly publications. Additionally, we included grey literature from industry white papers, governmental working group reviews, and their respective publications.

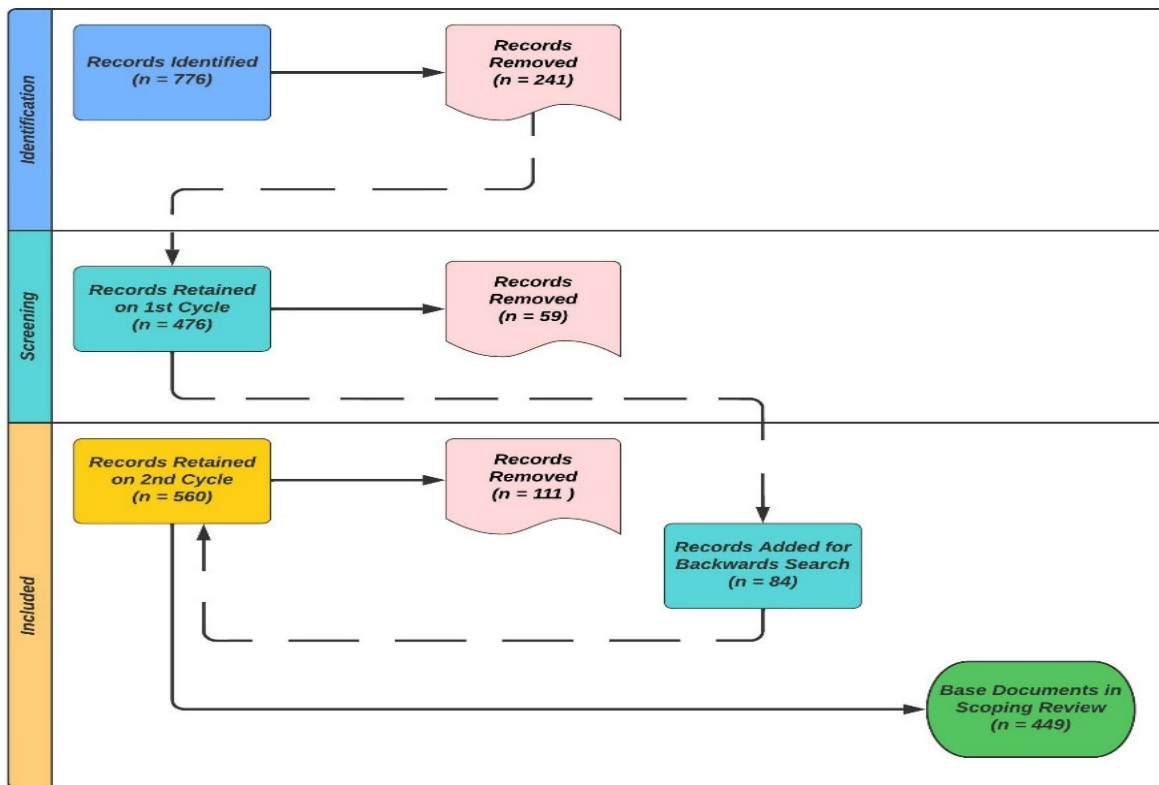
### ***4.2 Scoping Review Exclusions***

Original source documents were prescreened by reviewing the titles, keywords, abstract and conclusions. Remaining documents were placed in a secondary review process requiring a focused in-depth review of each remaining document. The exclusion process was designed to identify and remove source documents which were not specifically relevant to the research question(s). Articles or artifacts that were purely anecdotal, redundant, tangential, lacked research methodology, or were outside the scope or topic of interest were excluded from the review. These exclusion criteria were applied consistently throughout two distinct, focused, and targeted content reviews of all source documents.

### ***4.3 Population***

The population of this scoping review comprises source documents that align with the predefined criteria as per the sample size guidelines and qualitative research sampling methodologies outlined by (Levitt, 2018; Sadelowski, 1995; Tranfield, 2003). Using the search queries developed, the initial review consisted of 776 documents that were imported into NVivo14<sup>®</sup> for analysis. A

secondary examination of the collection was conducted, performing two distinct comprehensive reviews of the initial search results of 776 artifacts. Utilizing the exclusion criterion defined, 411 artifacts were removed. During the review and exclusion process 84 documents were introduced and added through backward search results. This made the total of 449 artifacts included in the scoping review. These 449 artifacts underwent comprehensive qualitative coding until we reached the point of “saturation” (Mocănașu, 2020; Mack, 2005), culminating in a total of 118 documents being manually coded. The decision to cease coding was grounded in the recognition that including more documents would not provide new insights substantial enough to enhance the understanding of the topics. Further, we used the NVivo14<sup>®</sup> automated functions, and thematically coded the remaining 331 using the 118 artifacts as the training set for this coding.



**Figure 2** – Scoping Review (PRISMA) diagram.

## ***4.4 Concept & Context***

The development of a consistent application of the coding across all the documents was paramount. To do this a sentimentality scoring framework and relationships rubric were constructed and applied. The adoption of and implementation of accepted standards were required to add rigor to the holistic, qualitative coding methodology.

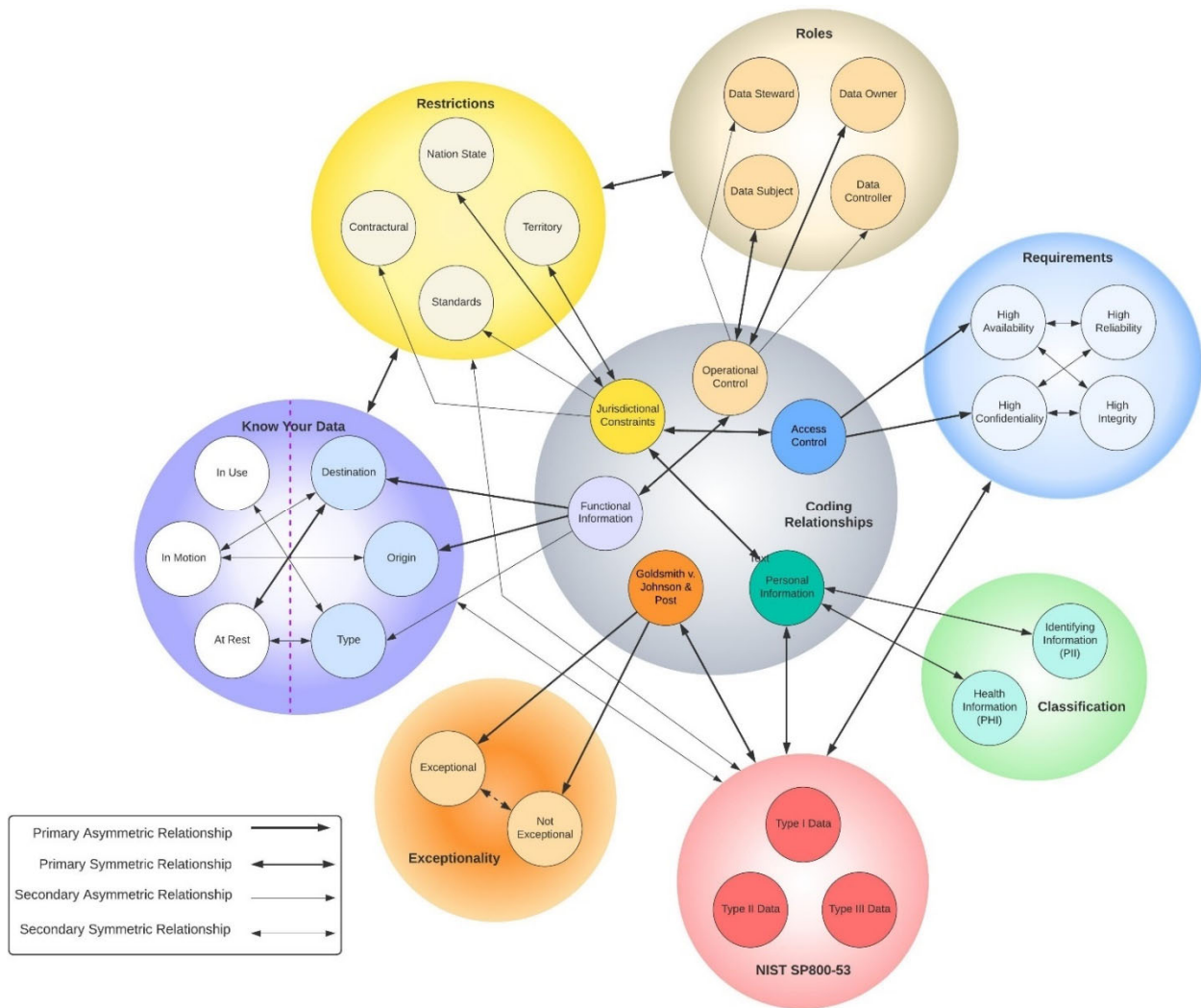
### **4.4.1 Sentimentality Scoring Framework**

A comprehensive coding framework was developed to evaluate the perceived exceptional nature of data. Auditors were instructed to categorize sentences or paragraphs based on the document's stance on data exceptionality, using four codes: *"very positive," "moderately positive," "moderately negative,"* or *"very negative"* (Vagias, 2006). These Likert-type scales were applied qualitatively, reflecting the implied degree of data exceptionality, and were also applied automatically based on the system's capabilities. Notably, the more negative the assigned sentiment, the greater the indication that the data was being viewed as non-exceptional.

### **4.4.2 Relationships Rubric**

A coding rubric was developed to analyze the interaction between various data types and their classification as either exceptional or non-exceptional. The rubric posits that data is perceived as more exceptional when it necessitates greater protection, offering a structured approach to qualitatively code the scoping review by aligning data protection levels with perceived exceptionality. These relationships were found to be both symmetric and asymmetric, depending on the roles, requirements, and jurisdictional constraints that shape the control and classification of data, impacting security and privacy concerns. A total of 135 codes were designed and applied following qualitative coding standards. These codes were organized into parent, child, and grandchild relationships. The codes encompassed data's roles, requirements, classification,

jurisdictional limitations, and impact factors within its normal life cycle. Due to the extensive nature of this coding matrix, a full display is beyond the scope of this document, though a simplified model of the asymmetric and symmetric relationships is provided below in *Figure 3*.

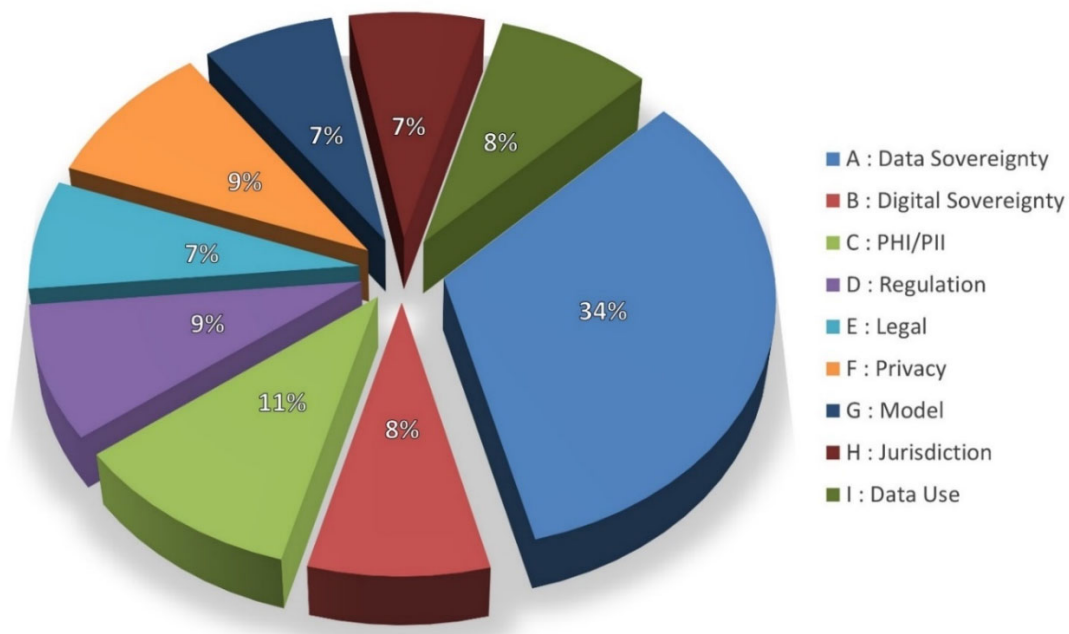


**Figure 3** – Coding Hierarchy: Parent/Child Relationships.

The core of the qualitative evaluation utilized the existing framework from The National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls for Information Systems and Organizations, which classifies data systems into three categories: Type I (*Low Impact Data*), Type II (*Moderate Impact Data*), and Type III (*High Impact Data*). Each category



requires distinct approaches to security, access, and storage, with protections increasing as the potential impact of the data rises. The rubric was designed to map these categories onto three levels of data exceptionality: *"not exceptional," "moderately exceptional,"* and *"highly exceptional."* Each classification demanded different levels of availability, accessibility, and reliability, establishing relationships between exceptional and non-exceptional data. From this framework, conceptualizations of interoperability and sentiment scoring were considered essential in determining the final *"nature"* of the data.



**Figure 4** – NVivo14<sup>®</sup> Semantic & Latent Theme Analysis from Scoping Review

#### 4.4.3 Semantic & Latent Theme Analysis

The NVivo14<sup>®</sup> automated thematic analysis was then performed on all 331 documents, using the coding ruleset established and trained previously on the 118 qualitatively coded documents. This process facilitated the emergence of both semantic themes, which are explicitly stated within the data, and latent themes, which are interpreted from underlying concepts present in the data.

Thematic analysis methodologies were applied, based upon accepted standards promulgated in qualitative research (Braun & Clarke, 2006). The development of thematic maps further illuminated these patterns. In addition to the qualitative analysis, a quantitative dimension was introduced to summarize the data and provide measurable insights into the predominant, nascent, or underrepresented areas of research. The detailed expansion of the theme map is illustrated by percentages seen in *Figure 4*.

## **5.0 FINDINGS**

This scoping review of articles reveals a dominant inclination towards Goldsmith's "exceptional data" model. The predominant exceptionalist viewpoint advocates a geophysical, territorialized approach to data governance. From the reviewed artifacts, the prevailing perception is that jurisdictional territoriality dominates data governance. However, actual data usage and management often belie this data exceptionalism viewpoint. Goldsmith's view protects monolithic data structures, but it conflicts with our modern decentralized cloud infrastructure. Our current data use and storage practices more closely follow Johnson & Post's concepts of a free-flowing transnational concept of data, as seen in data mesh networking, and modern cloud computing architectures (Dehghani, 2022). The globally interconnected internet, and dynamic nature of data, coupled with modern data mining and aggregation methods, allow organizations to farm and misuse sensitive, private, or confidential data, and cause financial and reputational damage (Martin, 2020). Such acts not only undermine trust in digital sovereignty, but also pose direct challenges to the concept of data sovereignty (Véliz, 2024).

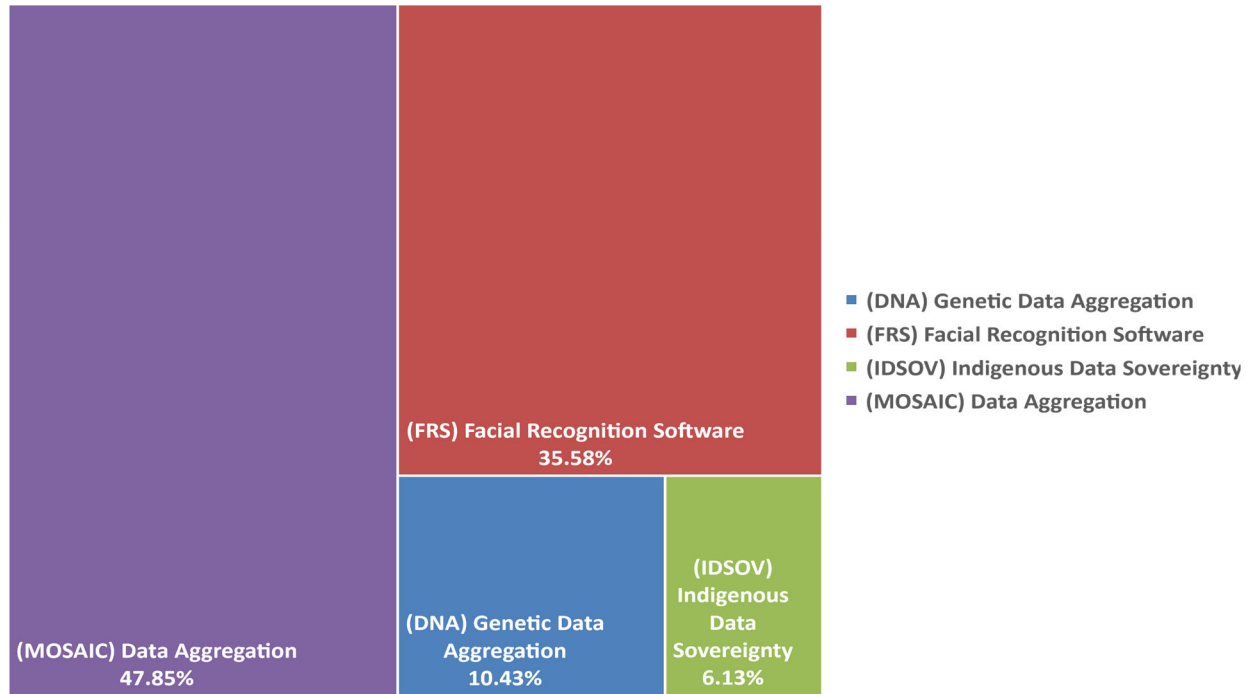
Goldsmith's exceptionalist viewpoint is favored by 60.71% of the papers reviewed and supports the traditional stance on data localization, promulgating jurisdiction-bound frameworks. This

finding reflects a substantial scholarly preference for maintaining data control within geographically defined boundaries.

Despite the prevalent support for territorial data governance, a significant portion of the literature, 39.29%, supports Johnson & Post's non-exceptionalists vision of a borderless digital ecosystem. This non-traditional perspective argues for the liberation of data from traditional territorial constraints to better align with the fluid nature of digital data flows across global networks, a free, independent, and borderless internet. Additional to the thematic analysis conducted, a concept coding application was also deployed. It categorized themes, artifacts, relationships, and sentiments within the sourced documents into "*Micro*", "*Meso*," and "*Macro*" levels to pinpoint discussions around data sovereignty. The concept coding results revealed that 47.85% of the documents analyzed focus on issues related to AI and "aggregated data" using the "mosaic theory" underscoring the urgent need for more stringent oversight and clear regulatory AI frameworks. Additional issues arose, such as the use of facial recognition technology and the inclusion of personal health data, particularly genetic information, significantly influenced the discussion on aggregated data. Facial recognition accounted for 35.58% of this discourse, while genetic data contributed 10.43% to the academic dialogue. The analysis also noted an emerging focus on indigenous data sovereignty, representing 6.13% of the discussions.

These highlighted a growing concern for ethical and governance issues, specific to the misuse of AI in the aggregation and synthesis of data, known in litigation as the mosaic theory. Further it further identified the harms facing societies, specifically indigenous communities, emphasizing the need for culturally sensitive data governance strategies that respect and uphold the rights of these communities. These use cases include "*mosaic theory*," "*facial recognition software*,"

“genetic data,” and “indigenous data sovereignty.” These use cases, based on latent themes are illustrated in *Figure 5*.



**Figure 5** – Use Case: Data Classification Findings.

### 5.1 Data Reflecting Goldsmith’s “Exceptionalist” Viewpoint

A notable sentiment towards the exceptionalist’s viewpoint, or Goldsmith’s theory of “*exceptional data*” emerged, indicating a substantial inclination among sources towards this belief. Upon analysis, it became clear that most sources, regardless of their primary focus, supported Goldsmith’s attitude that data is exceptional, with 60.71% of respondents affirming this. Delving deeper, 32.4% moderately agreed, while a significant 67.6% expressed a strong agreement that data possesses an exceptional nature. The Goldsmith viewpoint emphasizes the continuing relevance of territorial sovereignty in the context of the internet and data regulation. They argue that despite the global nature of the internet, traditional concepts of territorial sovereignty remain

significant in the governance of data. Aligning in most cases with the governing laws of the territorial location or geographic location as to where data is stored.

## ***5.2 Data Reflecting Johnson & Posts’ “Non-Exceptionalist” Viewpoint***

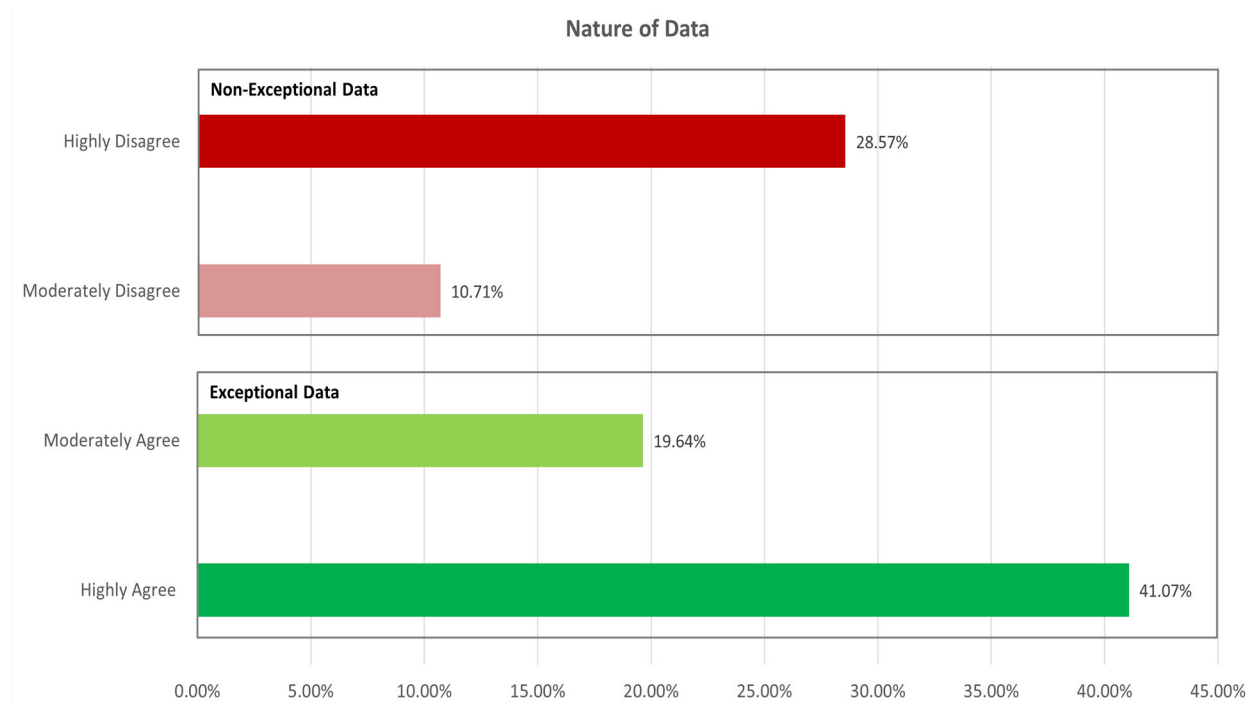
Conversely, the scoping review revealed a substantial body of literature supporting the non-exceptionalist’ view, or Johnson & Post's argument that data should be considered “*non-exceptional*,” diverging from Goldsmith's thesis on exceptional data. This perspective was endorsed by 39.29% of the analyzed documents, highlighting a significant academic preference for a more flexible, global approach to data governance rather than strict territorial constraints. Interestingly, 72.7% of the scholars supporting the “*non-exceptional*” view were strongly committed to this position, although they represented a minority in the overall review, their advocacy to their belief was stronger. This suggests robust yet less prevalent advocacy for treating data as a universal entity, unbound by traditional jurisdictional boundaries.

The proponents of this viewpoint argue for a reconceptualization of data sovereignty that aligns with the inherently borderless and interconnected nature of the digital realm. This faction suggests that traditional territorial paradigms are insufficient for the digital age, where data crosses boundaries with ease, necessitating governance structures that transcend national jurisdictions. The support for Johnson & Post's perspective reflects a critical discourse within the academic community that seeks to challenge the status quo of data governance and adapt it to the dynamism and scale of global data flows, as has been detailed in the preceding sections of this research.

## ***5.3 Summary***

The review presents a spectrum of perspectives, reflecting both consensus and divergence. Proponents of both data exceptionalism and non-exceptionalism are represented; however, the

extent to which data is perceived as exceptional or non-exceptional tends to reflect idealistic situational interpretations. The findings indicate that the predominant view regards data as exceptional, requiring specialized governance and protection mechanisms, while a notable minority advocates for a non-exceptional stance, supporting a federated governance framework in contrast to conventional approaches. These results emphasize the complexity and the ongoing discourse within the field, as illustrated in *Figure 6*.



**Figure 6** – Data Sentimentality: Nature of Data – Data is “Exceptional.”

## 6.0 DISCUSSION

This investigation into data sovereignty identifies several limitations in the field of data sovereignty and suggests paths for future research. It grapples with the conflicting territorial versus non-territorial approaches to data governance, as discussed by Goldsmith and Johnson & Post. A notable limitation that is consistent is the reliance on outdated existing legal frameworks and antiquated philosophical theories, which do not capture the rapidly evolving landscape of digital

data, particularly with the growth of artificial intelligence and the Internet of Things (IoT). This discrepancy highlights a potential misalignment between current risk mitigation strategies, legal practices, and technological advancements. While the locus of this review was primarily performed using "*Western*" perspectives, it is notable that latent themes provided the need to explore different cultural and legal views for greater context.

We reveal that most reviewed documents align with Goldsmith's perspective, viewing data as exceptional. Nevertheless, a discernible shift towards the Johnson & Post perspective indicates a change in technological trends. This division is representative of the exacerbation of the industry concerning regulatory confinement and policy creep, potentially slowing, or stopping technological advancements globally. Scholars continued to restate their concerns that absent a unified or federated global framework to address legal and regulatory lag to address issues such as data privacy, security, and surveillance, there would be a race to the bottom widening the stances of the exceptionalist and non-exceptionalist and deepening the divide between these viewpoints.

Additionally, we reveal that views predominantly fail to acknowledge the global shift towards decentralization and the adoption of cloud architectures and data mesh networks, and it is becoming increasingly problematic. This transition away from Goldsmith's perspective on data sovereignty is overlooked. As data breaches and ethical concerns over data misuse continue to rise, there is a pressing need for robust protective measures. This includes advancing privacy-preserving technologies and creating ethical AI frameworks capable of adapting to the swiftly evolving landscape of data sovereignty. Addressing the disconnect between reality and academic perception is critical and cannot be postponed any longer. A new approach to governing cross-border data flows is imperative to data sovereignty, and individual rights of data subjects.

## **7.0 CONCLUSIONS & FUTURE WORK**

This review uncovers a disconnect between the realities of data usage, industry practices, legal frameworks, and academic perspectives on data sovereignty. While there is consensus on the fundamental nature of data, sharp divergences arise concerning its treatment, storage, and usage. Notably, 60.71% of the reviewed documents perceive data as exceptional, emphasizing its unique and valuable qualities. However, this perception fails to align with current data practices, where data increasingly shifts from monolithic, centrally controlled structures to agile, cloud-based architectures. This misalignment underscores a larger issue: traditional views of data exceptionalism, as articulated by Goldsmith, contribute to legal lag and a lack of forward-thinking regulations. The territorial approach to data governance, though historically rooted, conflicts with the fluid and transnational reality of modern data practices.

Goldsmith's territorial model, while providing clear jurisdictional boundaries, hampers the efficient and secure flow of data across borders, stifling innovation and perpetuating a fragmented regulatory landscape. This outdated legal framework leads to regulatory lag as global data flows surpass the limitations of geographical boundaries. In contrast, Johnson & Post's non-exceptionalist approach advocates for a borderless governance model that better reflects the nature of contemporary digital architecture. The persistence of Goldsmith's model, despite the evolving digital ecosystem, reveals a reluctance to adopt new paradigms, exacerbating inefficiencies in cross-border data practices.

Moreover, the misconception that data is a finite resource further complicates the discussion. Data is infinite, ephemeral, and expansive, crossing borders with or without sufficient regulations. To address these challenges, we advocate for a balanced, federated approach to data sovereignty, one that reconciles exceptionalist and non-exceptionalist perspectives while acknowledging the global



dynamics of data. In line with Hegelian philosophy, a synthesis of these tensions would emerge, bridging the gap between national sovereignty and data's transnational nature.

The study also emphasizes the inclusion of non-Western perspectives, recognizing that data is a global asset. Indigenous communities, whose concerns are increasingly relevant, should be involved in shaping an inclusive and individual-centric model of data sovereignty. A modern, federated governance framework is essential to fostering a regulatory landscape that both promotes technological innovation and ensures equitable global data governance.

Building upon the finding of this review, several key areas of future academic inquiry emerge, each offering the potential to bridge existing gaps between data governance practices, legal frameworks, and the evolution of our technological landscape, securing data sovereignty for individuals. Here are the three areas that emerged from this review:

- Exploring alternative governance models for data sovereignty.
- Incorporating non-western and indigenous perspectives into data governance.
- Addressing the legal lag in data sovereignty frameworks, globally.

## REFERENCES

- Aaronson, S. A. 2018. "Data is different: Why the world needs a new approach to governing cross-border data flows." Working Paper.
- Aaronson, S. A. 2018. "Data minefield: How AI is prodding governments to rethink trade in data." Institute for International Economic Policy Working Paper Series Elliott School of International Affairs, George Washington University, IIEP-WP-2018-11.
- Aaronson, S. A., & Leblond, P. 2018. "Another digital divide: The rise of data realms and its implications for the WTO." *Journal of International Economic Law*, 21(2), 245–272.
- Alban, S. J. 2023. "Your DNA is for sale on the black market: 23andMe data breach exposes customers." *MIT Technology Review*. Retrieved from <https://www.technologyreview.com/>
- Ahern, D. 2021. "Regulatory lag, regulatory friction and regulatory transition as fintech disenablers: Calibrating an EU response to the regulatory sandbox phenomenon." *European Business Organization Law Review*, 22(3), 395–432. <https://doi.org/10.1007/s40804-021-00217-z>
- Anonymous. 2013, August 11. "The NSA leaks: A summary." *Harvard Political Review*. <https://harvardpolitics.com/the-nsa-leaks-a-summary/>
- Barlow, J. P. (n.d.). "A declaration of the independence of cyberspace." Retrieved from [https://www.eff.org/cyberspace\\_independence](https://www.eff.org/cyberspace_independence)
- Bendiek, A. 2016. "Due diligence in cyberspace: Guidelines for international and European cyber policy and cybersecurity policy." SWP Research Paper 7/2016. Berlin: Stiftung Wissenschaft und Politik.
- Bhageshpur, K. (n.d.). "Data is the new oil—and that's a good thing." *Forbes*. Retrieved June 7, 2024, from <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/>
- "Boston Marathon investigation: Are CCTV cameras the answer?" 2013, April 16. *CBS News*. <https://www.cbsnews.com/news/boston-marathon-investigation-are-cctv-cameras-the-answer/>
- Braun, V., & Clarke, V. 2006. "Using thematic analysis in psychology." *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brehmer, H. J. 2022. "Data localization: The unintended consequences." *American University Law Review*, 67, 927–961.
- Calderaro, A., & Blumfelde, S. 2022. "Artificial intelligence and EU security: The false promise of digital sovereignty." *European Security*, 31(3), 415–434. <https://doi.org/10.1080/09662839.2022.2101885>
- Capitalizing on the data economy. 2021. *MIT Technology Review*. Retrieved September 13, 2024, from <https://www.technologyreview.com/>
- Carson, A. 2014. "European regulators, FTC unveil cross-border data transfer tool." *International Association of Privacy Professionals*. Retrieved September 13, 2024, from <https://iapp.org/news/a/european-regulators-ftc-unveil-cross-border-data-transfer-tool>
- Chapman, S. 2022, October 16. "Edward Snowden & the NSA PRISM program: 2024 update." *Privacy Journal*. Retrieved from <https://www.privacyjournal.net/edward-snowden-nsa-prism/>
- Chilton, A. S. 2017. "A reply to Dworkin's new theory of international law." Working Paper.
- Choupiri Shivakeshi, N. S., Sachin, S. G., Sagar, & Krishna. 2022. "Face recognition at varying angles." *International Journal of Scientific Research in Science, Engineering and Technology*, 534–536. <https://doi.org/10.32628/IJSRSET2293157>

- Cook, M. M. 2022. "Bringing down big data: A call for federal data privacy legislation." *Oklahoma Law Review*, 74(4), 733–764. <https://digitalcommons.law.ou.edu/olr/vol74/iss4/8>
- Daskal, J. 2015. The un-territoriality of data. *Yale Law Journal*, 125, 326. <https://doi.org/10.2307/795891>
- Dehghani, Z. 2022. "Data mesh: Delivering data-driven value at scale." O'Reilly.
- de Meij, P. 2016. "Hegelian dialectics as a source of inspiration for the intelligence community." *American Intelligence Journal*, 33(1), 65–69. <https://www.jstor.org/stable/26202167>
- Ferracane, M. F., & Lee-Makiyama, H. (n.d.). "Digital trade restrictiveness index." Working Paper.
- Ferracane, M. 2017. "Restrictions on cross-border data flows: A taxonomy." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3089956>
- Fick, N., Miscik, J., Segal, A., & Goldstein, G. M. (n.d.). "Confronting reality in cyberspace." Retrieved from <https://www.jstor.org/>
- Fussell, S. (n.d.). "As cities curb surveillance, Baltimore police took to the air." *Wired*. Retrieved December 12, 2023, from <https://www.wired.com/story/cities-curb-surveillance-baltimore-police-took-air/>
- Geist, M. A. 2015. "Law, privacy, and surveillance in Canada in the post-Snowden era". University of Ottawa Press.
- Gold, J. (n.d.). "Toward norms in cyberspace: Recent progress and challenges." Working Paper.
- Goldsmith, J. L. 1998. Against cyber anarchy. *Chicago Law Review*, 1199.
- Huddleston, J., & Salihu, G. 2023. "The patchwork strikes back: State data privacy laws after the 2022–2023 legislative session." *CATO Institute*.
- Hummel, P., Braun, M., & Dabrock, P. 2021. "Own data? Ethical reflections on data ownership." *Philosophy & Technology*, 34(3), 545–572. <https://doi.org/10.1007/s13347-020-00404-9>
- Johnson, D. R., & Post, D. 1996. Law and borders: The rise of law in cyberspace. "Stanford Law Review", 48(5), 1367–1402.
- Katz and the adoption of the reasonable expectation of privacy test. 2023, September 18. *U.S. Constitution Annotated*. Retrieved from <https://www.law.cornell.edu/constitution-conan/amendment-4/katz-and-the-adoption-of-the-reasonable-expectation-of-privacy-test>
- Kelly, M., Furey, E., & Blue, J. 2019, June. GDPR Article 17: "Eradicating personal identifiable information & achieving compliance in a hybrid cloud." In *2019 30th Irish Signals and Systems Conference (ISSC)*. IEEE.
- Kerry, C. F. 2020, February 10. "Protecting privacy in an AI-driven world." *Brookings*. <https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/>
- Kilovaty, I. 2020. "An extraterritorial human right to cybersecurity." *Notre Dame Journal of International & Comparative Law*, 10(1), 34–62. <https://doi.org/10.2139/ssrn.3225691>
- Kosseff, J. 2018. "Defining cybersecurity law." *Iowa Law Review*, 103, 985–1023. <https://doi.org/10.2139/ssrn.3225691>
- Kochovski, A. 2022, May 23. "U.S. data privacy laws in 2024: A guide to online privacy laws." *Cloudwards*. <https://www.cloudwards.net/us-data-privacy-laws/>
- Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., et al. 2023. "Māori data sovereignty and privacy." Working Paper.

- Levitt, H. M., Motulsky, S. L., Wertz, F. J., Morrow, S. L., & Ponterotto, J. G. 2017. "Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity." *Qualitative Psychology*, 4(1), 2–22. <https://doi.org/10.1037/qup0000082>
- Lin, T., & Fidler, M. 2017. "Cross-border data access reform: A primer on the proposed U.S.-U.K. agreement." *Berkman Klein Center for Internet & Society*.
- Lind, D. 2015. "Everyone's heard of the Patriot Act. Here's what it actually does." *Vox*. Retrieved June 18, 2023, from <https://www.vox.com/2015/6/2/8701499/patriot-act-explain>
- Mack, N., & Woodsong, C. 2005. "Qualitative research methods: A data collector's field guide". FLI USAID.
- "Making data matter in real time." 2023. *MIT Technology Review*. Retrieved November 6, 2023, from <https://www.technologyreview.com/2023/06/21/1075155/making-data-matter-in-real-time/>
- Martin, K. 2020. "Breaking the privacy paradox: The value of privacy and associated duty of firms." *Business Ethics Quarterly*, 30(1), 65–96. <https://doi.org/10.1017/beq.2019.24>
- Mocănașu, D. R. 2020. "Determining the sample size in qualitative research." *International Multidisciplinary Scientific Conferences on the Dialogue between Sciences & Arts, Religion & Education*, 4(4). <https://doi.org/10.26520/mcdsare.2020.4.181-187>
- Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. 2018. "Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach." *BMC Medical Research Methodology*, 18(1), 143. <https://doi.org/10.1186/s12874-018-0611-x>
- Özdal Oktay, S., Heitmann, S., & Kray, C. 2023. "Linking location privacy, digital sovereignty, and location-based services: A meta-review." *Journal of Location Based Services*, 1–52. <https://doi.org/10.1080/17489725.2023.2239180>
- Peters, M. D. J., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., et al. (2020). "Updated methodological guidance for the conduct of scoping reviews." *JBIM Evidence Synthesis*, 18(10), 2119–2126. <https://doi.org/10.11124/JBIES-20-00167>
- Preuss, M. 2018, September 14. "What is the USA FREEDOM Act? What's so free about it?" *Cloudwards*. <https://www.cloudwards.net/freedom-act/>
- Rectenwald, M., & Carl, L. 2015. "Academic writing, real world topics". Broadview Press.
- Sadowski, J. 2019. "When data is capital: Datafication, accumulation, and extraction." *Big Data & Society*, 6(1), 205395171882054. <https://doi.org/10.1177/2053951718820549>
- Sandelowski, M. 1995. "Sample size in qualitative research." *Research in Nursing & Health*, 18(2), 179–183. <https://doi.org/10.1002/nur.4770180211>
- Scholz, L. 2018. "Big data is not big oil: The role of analogy in the law of new technologies." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3252543>
- "Schrems II landmark ruling: A detailed analysis." (n.d.). *Norton Rose Fulbright*. Retrieved December 17, 2023, from <https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis>
- Singh, K. 2020. "Data sovereignty governance framework." In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. ICSE '20: 42nd International Conference on Software Engineering, Seoul, Republic of Korea. <https://doi.org/10.1145/3387940.3392212>
- Solove, D. J. 2008. "Understanding Privacy". Harvard University Press.

- Svantesson, D. J. 2016. "Against 'Against' data exceptionalism." *Stanford Law Review*, 68(4), 405–450. <https://doi.org/10.5817/MUJLT2016-2-4>
- Taichman, E. (n.d.). "Defend forward & sovereignty: How America's cyberwar strategy upholds international law." Working Paper.
- "The rise of data capital." 2016. *MIT Technology Review*. Retrieved September 13, 2024, from <https://www.technologyreview.com/2016/03/21/161487/the-rise-of-data-capital/>
- Thierer, A. 2023, September. Blumenthal-Hawley "AI regulatory framework escalates the war on computation." *Medium*. Retrieved from <https://medium.com/>
- Toomey, P. 2018, August 22. "The NSA continues to violate Americans' internet privacy rights." *American Civil Liberties Union*. <https://www.aclu.org/news/national-security/nsa-continues-violate-americans-internet-privacy>
- Tranfield, D., Denyer, D., & Smart, P. 2003. "Towards a methodology for developing evidence-informed management knowledge by means of systematic review." *British Journal of Management*, 14(3), 207–222. <https://doi.org/10.1111/1467-8551.00375>
- "Turning data into data capital: Here's how to make the most of this huge hidden asset." 2024. *Google Cloud Blog*. Retrieved September 13, 2024, from <https://cloud.google.com/transform/turning-data-into-data-capital-takes-cloud>
- Ünver, H. A. 2018. "Politics of digital surveillance, national security and privacy." *Centre for Economics and Foreign Policy Studies*. <http://www.jstor.org/stable/resrep17009>
- Vagias, W. M. 2006. "Likert-type scale response anchors". Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management, Clemson University.
- Véliz, C. 2024. "The ethics of privacy and surveillance" (1st ed.). *Oxford University Press*. <https://doi.org/10.1093/oso/9780198870173.001.0001>
- Warren, S. D., & Brandeis, L. D. 1890, December. "The right to privacy." *Harvard Law Review*, 4(3), 193–220.
- Whitmore, L., McCauley, M., Farrell, J. A., Stammnitz, M. R., Koda, S. A., Mashkour, N., et al. 2023. "Inadvertent human genomic bycatch and intentional capture raise beneficial applications and ethical concerns with environmental DNA." *Nature Ecology & Evolution*, 7(6), 873–888. <https://doi.org/10.1038/s41559-023-02056-2>
- Woods, A. K. 2016. "Against data exceptionalism." *Stanford Law Review*, 61, 405–456.
- Yayboke, E., & Brannen, S. 2020. "Promote and build: A strategic approach to digital authoritarianism." *CSIS*. <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism>
- Yayboke, E., Ramos, C. G., & Sheppard, L. R. (n.d.). "The real national security concerns over data localization." Working Paper.
- "Your data is my data: A framework for addressing interdependent privacy infringements." (n.d.). *Journal of Legal Studies*. <https://doi.org/10.1177/0743915619858924>
- Zanon, N. B., Erlingsson, H.-P., & Tohmo, J. 2022. "Enabling GDPR/Schrems II compliance." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3415777>
- Zhang, C., & Morris, C. 2023. "Borders, bordering and sovereignty in digital space." *Territory, Politics, Governance*, 11(6), 1051–1058. <https://doi.org/10.1080/21622671.2023.2216737>
- "The protection of genetic information of Indigenous peoples." 2023. *Human Rights Commission*. Retrieved October 27, 2023, from <https://humanrights.gov.au/our-work/legal/protection-genetic-information-indigenous-peoples>

## APPENDIX

Database	Search String	Quantity
JSTOR (41)	<b>Objective #1</b> Title, abstract or author-specified keywords ("All Metadata": "Data Sovereignty" OR "All Metadata": "Digital Sovereignty" OR "All Metadata": "Data Territoriality" OR "All Metadata": "Data Localization" OR "All Metadata": "Digital Localization" OR "All Metadata": "Data Privacy" OR "All Metadata": "Digital Privacy" OR "All Metadata": "Data Steward" OR "All Metadata": "Data Subject" OR "All Metadata": "Data Owner") AND ("All Metadata": "GDPR" OR "All Metadata": "China" "All Metadata": "PIPL" OR "All Metadata": "LGPD" OR "All Metadata": "PIPEDA" OR "All Metadata": "Schrems" OR "All Metadata": "OCED" OR "All Metadata": "DOA" OR "All Metadata": "SCC")	25
	<b>Objective #2</b> Title, abstract or author-specified keywords ("All Metadata": "Data Sovereignty" OR "All Metadata": "Digital Sovereignty" OR "All Metadata": "Data Territoriality" OR "All Metadata": "Data Localization" OR "All Metadata": "Digital Localization" OR "All Metadata": "Data Privacy" AND ("All Metadata": "Facial Recognition" OR "All Metadata": "Genetic Data" OR "All Metadata": "DNA")	16

Appendix A – Scoping Review: Search String Prompt Examples.