

A conceptual framework for analysing different nation state approaches to the assertion of digital sovereignty

Context

Nation states maintain stable existence through the use of physical force. The military maintains the territorial, and in many cases economic, boundaries of the state. The police and legal system maintains state power within those boundaries. While many nation states have stability challenged both by external and internal forces, and some have failed to maintain their existence in the face of these challenges, the means necessary to maintain stability have remained unchanged. Until the 21st century, when the internet and related technologies have created threats to state power which cannot be addressed through traditional mechanisms. A new, digital 'space' has been created which is a best orthogonal to the state's territory and over which traditional methods of exerting power have been shown to be ineffective.

These new technologies arrived with clear and tangible benefits to the state itself, to the economy, to businesses, and to consumers. As a result, nation states were slow to perceive and have been even slower to respond to these threats to their ability to exert power, to maintain the integrity of their borders and the effectiveness of their legal systems in controlling their populations. A very few countries, maybe just China, North Korea and Iran, started responding some time ago with varying degrees of effectiveness. But the majority of countries have been in thrall to the neoliberal dreams of infinite growth and the promise of these new technologies to deliver that, which has until the 2020s blinded them to the risks to their own power. However, the need to respond has become urgent and is now widely accepted.

Responses to the threat to state power posed by an 'ungoverned' digital space have been conceptualised and thus justified under two main themes: **online safety**, especially for children but also more generally from organised crime and terrorists, and **digital sovereignty**. What is striking for the political theorist is that attempts to exert power over digital space under these two themes often result in forms of policing and border control which would be politically unacceptable in that state if exercised over physical space. In many countries, especially 'liberal democracies', attempts to govern digital space result in legal frameworks which are incompatible with the basis of legitimacy of that state.

Take, for example, the UK Prime Minister's recent announcement that Apple and Google must 'ban nude images on children's phones'.¹ On the one hand, this feels just like an extension of the existing restrictions on the previous age restrictions on sexual

¹ <https://www.bbc.co.uk/news/articles/clj752ydw6o>

content that have been applied to print publications and films for almost a century. Of course, there is a difference in that it covers sending images and also receiving them from an individual rather than a publisher, but that appears an appropriate updating of older approaches to the affordances of the smartphone. On the other hand, it goes way beyond the old laws which concentrated on age-verification at point of sale rather than onwards use of the material. To prevent the digital equivalent of under 18s being shown or lent material restricted to 18 year olds, this ban would require checking everything they see on their phones. It is the digital equivalent of the state - or its agents - peering into young people's bedrooms to check they are not accessing (or creating) sexual content. For this ban to be implemented, absolutely every image sent or received, and in practice every image created, will have to be checked for inappropriate content, which is loosely defined by the state in such a way that the phone companies have an incentive to over-police, to ban more rather than less to keep themselves on the right side of the law. This is an inevitable result of passing police functions to businesses who, unlike genuine police in a democratic state, have no interest in the public good, merely their own business interests. As such they have no reason to build systems which exercise discretion or adapt to unusual circumstances.

Furthermore, the announcement said: the ban 'will not affect the use of devices owned and used by adults who verify their age'. This suggests the digital equivalent of making everyone prove their age before entering a shop which sells age-restricted material, whether or not they want to buy any.² Thus, in a country which has systematically resisted any attempts to have national ID cards since they were implemented as a temporary measure in WW2, it will be necessary for everyone to prove their age, which requires handing over identity, in order to use something as fundamental to modern life as a smartphone. Having done this, everyone's smartphone, which is an essential in modern life, not least for interacting with the government, will serve as an ID card for the purposes of state policing, because it will have to be tied to the user's identity. By refusing to back the ban by implementing a system of national digital ID, a project the UK government would very much like to implement, they have hidden the fundamental change in what the British people consent to by way of state control behind private companies.

In this episode we see how an attempt to govern the digital space justified by appeals to online safety for children has in fact introduced an invasion of children's privacy, a level of over-policing, and a system of de facto compulsory identity cards, all of which would be politically impossible to implement in physical space in the UK. Whether by intention or carelessness, attempts to govern digital space by nation states risk having side effects of changing the political character of the state, and usually in the direction of paternalistic or even authoritarian restrictions on individual freedoms of citizens.

² In fact it is even worse than this, since all that proving your age will do is turn off the blocking of nude images. It leaves in place the technology to scan every image on the phone, whether created, sent or received. In fact, it doesn't even have to turn off the scanning, merely the blocking. So, depending on how it is implemented, the privacy invasion extends to adults as well.

This paper focuses on approaches to digital governance which claim legitimacy under the broad concept of digital sovereignty, and attempt to give a conceptual framework which allows us to see the political character of the approach. One important consequence of applying this model will be to the evaluation of specific proposals. Many will come with justifications which make them seem benign, but when properly analysed, will be shown to have political characteristics which may be unwelcome to the population at large, may be illegitimate given the existing governance principles, or may undermine the specific basis of legitimacy to govern that nation-state possesses.

While recent attempts at regulation provide illustrations of many points, the framework is not intended to be descriptive but conceptual - mapping out the range of options available in a manner that aims to be exhaustive - and normative.

Definitions

'Digital sovereignty' has become a broad label for any attempt by a nation state to control technology, exercising its powers as a state to enforce restrictions or promote development in particular ways, favouring the goals of that nation state or a particular government. However, this label, due to its very broadness, covers a wide range of different approaches with different motivations, different objectives, different scope, and different effectiveness. It also masks the fact that these approaches may have a distinctive political character, some aligning with the political character of some states more closely than those of other states.

This paper seeks to locate specific approaches within a conceptual space organised around three variables, within which we can locate those approaches.

The three variables are:

- 1) the scope, that is the range of digital services, technologies and functions that the state seeks control over;
- 2) the political goals that they're seeking to achieve by exercising this control; and
- 3) the commercial or organizational approaches they use in order to enforce or that control.

'Digital Space' refers to the full stack underpinning digital activity across a whole society. This includes: end-user client devices and the software running on them, whether 'personal' (owned and managed by an individual within the jurisdiction, i.e. locally) or 'managed' (owned and managed locally by an organization, be it commercial, educational, or governmental); servers, the data centres which host them and the software running on them, whether local or not; and the network of cables, relays and servers which connects them both locally and internationally.

Client devices are now universally connected to the network because the software they run either requires data from servers to install and update, data from servers to

fulfil its function (e.g. web access or communication), or to offload processing onto more powerful compute (e.g. many AI applications). As such, any nation state seeking to exercise control over digital space needs to consider all three aspects, however, the conceptual framework will be articulated in terms of the generic 'digital space', with the client-server-network distinction becoming relevant when we consider applications of the framework.

The Digital Space of a given nation state includes all and only local client devices, all servers which client devices engage with, whether local or international, all local network infrastructure, any international network infrastructure required to connect client devices to non-local servers.

Digital Space vs Virtual Space

We can distinguish Digital Space so defined, the elements of which exist in the physical world, can be distinguished from Virtual Space, the realm of entities and actions which supervene upon Digital Space.

Should nation states also be attempting to regulate Virtual Space?

At least until the development of autonomous AI agents operating within Virtual Space, actions and events in Virtual Space had fairly clear chains of causal responsibility back to actions by physical agents interacting with Digital Space. Consequently, nation states interested in regulating VS have done so by regulation which clarifies and deanonymises those causal chains - primarily by attaching real-world identities to client devices and application server accounts.

Moral philosophers have raised the question of purely virtual wrongs. For example, could an avatar in a multiple player online gaming space commit theft, rape, or murder against another avatar in that space? If, and there is certainly no consensus on this, such purely virtual moral wrongs are possible and sufficiently similar to the physical wrongs the nation state already criminalises, then there may be a need to extend criminal law into Virtual Space in new ways. Defining offences and sanctions and implementing the apparatus of the criminal justice system would be an immensely challenging legal problem.

However, we must remember that the criminalisation of moral wrongs such as rape is an instrumental decision by the state to protect its citizens from certain harms. There is nothing inherent in the nature of the nation state that requires it to criminalise any particular moral wrong. Many forms of adultery are morally wrong but few states see the need to criminalise them.

Consequently, most nation states take a different approach to protection of citizens from virtual harms: they treat Virtual Space as a collection of private spaces entered into voluntarily and each with explicit norms of behaviour (in Terms of Service)

enforced by the platform. Legislation like the UK's Online Safety Act (2025) attempts to protect citizens within such private spaces by requiring Terms of Service to meet certain standards of explicitness and be enforced effectively. There are problems with this approach - mainly to do with platform monopolies, switching costs, arbitrary and unaccountable 'justice', and changing Terms of Service - but they can be mitigated through the regulation of Digital Space.

For these reasons, it is not possible and may not be desirable to regulate Virtual Space directly.

The Functional Scope of Digital Governance

A state seeking to exert greater control over the digital space may have in scope any of the following:

1. Core state functions which are implemented digitally and the data associated with those functions, both collected by the state and used by the state.
2. Data collected about its citizens, not necessarily limited to that data collected by the state, but collected by any other organization operating within the nation
3. Digital services used by consumers, businesses and educational organizations.
4. Specific technologies such as end to end encryption, virtual private networks or, increasingly, technologies used in social media like Infinite Scroll.
5. The information that is transmitted across digital technologies, both within the country and across its borders.

While we might assume that all states would focus on 1) as a matter of priority, this turns out not to be the case, with many Western countries, especially those with more neoliberal economies, allowing 1), 2) and 3) to be largely dealt with through the market and consumer protection legislation and focussing more on 4) and 5) when asserting digital sovereignty.

Political Objectives

Here we can identify nine distinct political objectives which the control of digital space by a nation state is intended to achieve. These objectives are not exclusive. However, there may be certain combinations which are inconsistent or at least normatively in tension with each other.

Concept	Political Objective	Relationship Logic	Implementation
Digital Libertarianism	Minimization of state	State - Citizen Digital space is part of the private sphere, state only interferes to rectify right infringements	No special regulation or control of digital space; onus on affected parties to bring laws to bear.
Digital Republicanism	Avoidance of domination	State - Citizen State regulates and controls digital space to prevent emergence of new forms of arbitrary power over citizens	Regulation of tech companies to ensure meaningful consumer (B2C and B2B) choice, clear Terms of Service, avenues for redress.
Digital Paternalism	Protection of population	State - Citizen Mandatory: State overrides user choice/privacy for the sake of collective "safety."	State-mandated "safety" regulations about acceptable technologies (e.g., banning infinite scroll or requiring client-side scanning for CSAM).
Digital 'Nationalism'	Control of population	State - Citizen Force multiplier: State uses tech as an instrument for national identity and narrative control.	Maximum control of software and data or information available to client devices.
Digital Mercantilism	Wealth of nation	Economic Protectionist: State fosters "National Champions" to secure global trade dominance.	Provision of financial and regulatory advantage to selected domestic providers.
Digital Liberalism	Efficiency of market	Economic Laissez-faire: State acts as a light-touch referee to ensure open, innovative markets.	Minimal state friction to maximize investment, efficiency, data flow, and market-led innovation.
Digital Socialism	Provision of services	Economic Interventionist: State does not trust private companies to deliver tech to benefit of citizens	State ownership of aspects of digital space, most obviously at infrastructure level but can be anywhere (e.g. pupil devices in state schools)
Digital Sovereignty	Authority of state	State - Tech Regulosolutionism: State asserts the legal right to rule over the digital space and its data.	Enforcing the 'rule of law' within digital space and excluding any non compliant providers through legal sanctions.

Concept	Political Objective	Relationship Logic	Implementation
Digital Autonomy	Resilience of state	State - Tech Engineering/Technical: State/citizens build systems that are protected from external control or influence.	Building a resilient infrastructure that bypasses global monopolies and removes ongoing dependence on foreign technology or expertise.
Digital Feudalism	Loyalty to state	State - Tech Transactional: State trades deregulation/monopoly for tech company loyalty and service.	Providers of digital technologies and services are contracted to take over core state functions in return for state-like monopolies in large regions of digital space, enabling very high levels of profitability and extractive capitalism.
Digital Diplomacy	Stable world order	State - Tech Peer Power: State and very large Tech providers treat each other as (non-territorial) diplomatic peers in recognition of similar power and wealth.	Regulations governing the behaviour of providers within digital space operate like treaties arising from negotiation between the state and the providers respecting each other's different fields of power within digital space.
Digital Fellowship	Shared values	State - Tech Moral discourse: State and tech providers collaborate in seeking the common good in virtue of shared values such as liberalism and democracy.	Seek a consensus between the state and the providers of digital services and technologies on how to manage the digital space for the common good.

Business models

Within a given digital space there will be a mix of providers of digital technologies and services, some state owned and managed, others privately owned and state managed, and privately owned and managed. This creates a range of different business models for the delivery of digital technologies and services to end users be they an individual, a business, a state organisation or some other grouping within the state. As the state seeks to exercise its chosen form of control over a given in-scope area of digital

space, it will do so by selecting a specific business model or relationship with a provider.

There are six control relationships we can consider which might be applied to different end user / technology pairings. These approaches are not exclusive, and are often applied separately to different in-scope areas of digital space. In particular, 1) may combine with any of 2) to 7).

1. Selective banning of specific platforms or technologies.
2. Software as a service from the best providers in an open market.
3. SaaS from providers within a regulated market or specific regulated providers.
4. SaaS from providers within a controlled or coordinated market.
5. Self-hosting using physical infrastructure from the best providers in an open market.
6. Self-hosting using physical infrastructure from providers within a regulated market or specific regulated providers.
7. Self-hosting using physical infrastructure owned and managed by the end user.

Conclusions

- There is no one correct way to govern digital space
- Appeals to 'digital sovereignty' to justify governance approaches can be misleading about the political character of proposals
- Each nation state has to choose in accordance with its own political and economic goals and the basis on which the authority to govern is legitimate
- This may conflict with the goals of powerful, transnational tech companies