



An Essay by
JOHN SEVERINI
Georgetown University





John Severini

Digital Frontiers, Corporate Sovereignty, and the Future of the CEO

The realities of international power politics will thrust powerful CEOs into the new, dynamic role of statesman-executive. Corporations are quickly beginning to demonstrate a new form of digital sovereignty as they begin outpacing the capabilities of state actors to establish and police rules across new internet platforms. As a result, CEOs of companies contesting ownership over these “digital frontiers” will increasingly have to balance the needs of their firms’ nominal profit-maximization with the demands of politically aware consumer bases demanding the institutionalization of moral frameworks in their products. Correspondingly, world leaders must seriously consider the tradeoffs of leveraging future public-private alliances for the sake of international realpolitik, as the continued empowerment of corporations will solidify their status as independent sovereign authorities in a future global system increasingly reliant on the internet.

State governments remain the most powerful institutions operating in the physical world today; their prevailing ability to establish and enforce rules over land, air, sea, and space is still uncontested for the most part.¹ These same state governments, however, do not wield an equivalent amount of power to establish and enforce rules over a “cyberspace” that is becoming increasingly intertwined in the physical world today.²

The predominance of the platform business model has created an international economy populated by large and powerful multinational companies that lead in the creation and distribution of novel forms of interaction across the internet. The mightiest are capable of wielding vast and diversified economic power; if Amazon’s gross annual revenue were GDP, for instance, it would constitute the 27th largest economy in the world.⁴ Moreover, the labor supply in highest demand has become increasingly consolidated in the most prominent tech firms offering the most competitive compensation packages. Public sector organizations, constrained by smaller budgets and legal hurdles like drug enforcement and clearance concerns, often have a much more difficult time competing for the most talented and qualified software and hardware engineers on the market.

1 For one recent example, see Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” *Internet Policy Review* 9, no. 4 (December 17, 2020): 1–19, <https://doi.org/10.14763/2020.4.1532>.

2 Jordan Branch, “What’s in a Name? Metaphors and Cybersecurity,” *International Organization* 75, no. 1 (2021): 39–70, <https://doi.org/10.1017/S002081832000051X>.

3 K. Sabeel Rahman and Kathleen Thelen, “The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism,” *Politics & Society* 47, no. 2 (June 2019): 177–204, <https://doi.org/10.1177/0032329219838932>.

4 For a further treatment on the power of modern corporations like Amazon and the platform business model, see Pepper D. Culpepper and Kathleen Thelen, “Are We All Amazon Primed? Consumers and the Politics of Platform Power,” *Comparative Political Studies* 53, no. 2 (February 1, 2020): 288–318, <https://doi.org/10.1177/0010414019852687>.



This relative accretion of corporate power has created a gap between the capabilities of state governments and private entities within the digital domain. This capability gap is critical because the internet now not only serves as the foundation for the modern international economy but is rapidly becoming a contested arena between both public and private actors. Accordingly, state governments that want to successfully compete in cyberspace must 1) increasingly call upon powerful corporate allies to augment their ability to contest rivals, 2) ensure that these powerful corporate allies remain internationally competitive, and 3) concede practical authority over areas of the internet where their corporate allies are better positioned to ensure enforcement of rules and norms.

Unlike the physical domains of land, air, sea, and space, the digital domain is constantly expanding in scope as the servers, networks, and programs constituting the internet grow more numerous and better connected. This process of expansion is almost entirely the result of the private sector massively investing in new physical equipment, but it also comes about as novel forms of digital interaction get invented, distributed, and experienced. These especially new areas of the digital domain are often only immediately understood by the engineers who create and operate in them; their knowledge eventually diffuses outward as the new ecosystems become more populated, but authority will always originate in the architects who build these spaces in the first place. Because the population of new digital ecosystems can happen rapidly, state governments will have none of the same capability to enforce rules as they might otherwise in the physical world. As a result, de facto control will often be ceded out of practical necessity. Just as many colonial entities of old were given the authority to effectively govern over territorial space that the state had nominally expanded into but was otherwise unacquainted with, so too does rapid expansion of the digital domain today result in states yielding authority to corporations over aspects of cyberspace that are new and unknown.⁵

In practice, these “digital frontiers” will often coalesce around new platforms and applications created by private firms. Like physical frontier regions, these digital frontiers are populated by people who will demand the establishment of rules and norms that create expectations for acceptable behavior. Acceptable behavior is often distinct to specific environments and its assurance requires both the knowledge and discrete administrative capabilities unavailable to most public sector organizations. If states lack the capacity to govern these frontiers and acquiesce to the private sector, then the creation and execution of these rules, norms, and eventually laws will inevitably fall to the prerogative of corporate interest.⁶

5 I take the comparison at least in part from Swati Srivastava, “Corporate Sovereign Awakening and the Making of Modern State Sovereignty: New Archival Evidence from the English East India Company,” *International Organization* 76, no. 3 (March 2022): 690–712, <https://doi.org/10.1017/S002081832200008X>.

6 This establishment of enforced rules, norms, and laws in the digital world has also been described at times as a sort of “digital colonialism,” especially as it relates to the contrast between the global north and global south. See, for instance Renata Avila Pinto, “Digital Sovereignty Or Digital Colonialism,” *Sur - International Journal on Human Rights* 15 (2018): 15–27.

7 Marion Fourcade and Daniel N Kluttz, “A Maussian Bargain: Accumulation by Gift in the Digital Economy,” *Big Data & Society* 7, no. 1 (January 2020): 205395171989709, <https://doi.org/10.1177/2053951719897092>.



Even if early concession of authority over these frontiers to their original architects is a practical (and often unconscious) decision by states lacking the necessary mechanisms themselves, the effect can quickly reinforce over time. Early forms of corporate authority often take the structure of reciprocal relationships between consumers and corporations, eventually leading to consumers viewing corporations rather than states as their immediate legal principal within the context of the digital frontier regions they are participating in.⁷ If state governments remain largely absent from these environments out of practicality, the cost of re-entering as an authority increases as the spaces get larger, more populated, and more dynamic. Accordingly, the knowledge required for the creation and maintenance of this authority will become further entrenched in their corporate founders, further widening the capability gap between state and corporate entities in the digital domain.

Eventually, the complexity of the digital frontiers will reach a point where corporations may require similarly more complex institutions to successfully maintain their authority as the principal enforcer of rules, norms, and laws. Facebook's recent attempt to create its own version of a "Supreme Court" stands as an augur to this theory in contemporary practice.⁸ The establishment by a non-state organization of institutions aimed at the instantiation of its governing authority is not unprecedented, but it is also not a particularly common practice among entities that don't also contain a substantial coercive force. When the rational calculus of a corporation results in the creation of a system closely mimicking aspects of political structure, the difference between its economic and moral interests will begin to blur. In the future, corporations may compete against each other not necessarily based on the economic viability of their respective products alone, but also on the political frameworks that they purport to abide by as authority figures themselves. As a result, CEOs of these corporations will be forced to act simultaneously as both business leaders and political figureheads concerned about their company's customers not just as consumers, but increasingly as constituents as well.

In geographic spaces bereft of humans like the Arctic, it took the establishment of institutions claiming authority before sovereignty could ever be disputed in the first place. The future of cyberspace may revolve around corporate contestations based on the relative ability to enforce rules, norms, and laws within certain parts of the internet. More importantly: not only are states no longer the principal actors in these spaces now, the digital and physical worlds are rapidly beginning to overlap. As a result, corporations are likely to wield substantial power relative to state governments, and this gap in capability is unlikely to shrink given the cost-calculus of the most prominent states in the international system today.

⁸ Kate Klonick, "Inside the Making of Facebook's Supreme Court," *The New Yorker*, February 12, 2021, <https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court>.



Correspondingly, if cyberspace is likely to revolve around this new type of corporate sovereignty, then it stands to reason that CEOs of the most powerful corporations must enter the political arena if they are to successfully lead in a coming period of stronger non-state authority. These new CEO cohorts will have to weigh their decision-making more towards political realism than ever before, and the hybrid role of statesman-executive may end up looking like a new and unfamiliar amalgam of Otto von Bismarck and Bill Gates. These statesmen-executives will be increasingly entrusted to make choices with immediate implications for the global system, and the most influential will likely wield far more power than many states in the world today. The CEO of the future will inevitably become a political figure, and both domestic and international institutions need to recognize that the coming era of the information age may rapidly become centered around corporate power and the statesmen-executives who wield it.