Scenario 3 – Barlow's Revenge

As digital security deteriorates dramatically at the end of the 2010s, a broad coalition of firms and people around the world come to a shared recognition that the patchwork quilt of governments, firms, engineering standards bodies and others that had evolved to try to regulate digital society during the previous decade was no longer tenable. But while there was consensus that partial measures, piecemeal reforms and marginal modifications were not a viable path forward, there was also radical disagreement on what a comprehensive reformulation should look like. Two very different pathways emerged. In some parts of the world, governments have essentially removed themselves from the game and ceded the playing field for the largest firms to manage. This felt like an ironic reprise of the 1996 ideological manifesto of John Perry Barlow, "A Declaration of the Independence in Cyberspace". In other parts of the world, governments have taken the opposite path and embraced a full-bore internet nationalism in which digital power is treated unabashedly as a source and objective of state power. In 2025, it is at the overlaps and intersections between these two self-consciously distinctive models, existing almost on different planes, that the most challenging tensions but also surprising similarities are emerging.

Could a constitutive moment for internet society be postponed any longer? This was the question on the minds of just about every delegate at the multistakeholder Internet Society meeting in Manama, Bahrain, in December 2020. It was a collective recognition of the end of innocence or, more realistically, the pretence of innocence, that had continued to characterize the digital world even into the second decade of the century.

The year 2020 marked 45 years since the founding of the Homebrew Computer Club and 38 years since TCP/IP became the only approved protocol on the ARPANET, but even those long stretches of time were not the real impetus behind the appetite for an internet "constitutional convention". Rather, it was the events of 2019 that crossed some collective threshold of tolerance where the now ancient founding myths (ancient in internet time) could no longer be sustained.

Some of this was good news about growth: it was in 2019 that all of the world's 11 largest companies by market capitalization were for the first time digital technology companies (six American, four Chinese and one South Korean firm made the list). It was in 2019 that e-commerce in China rocketed past 50% of all retail sales (in the US, it reached the 25% yardstick). And 2019 was the year that global internet penetration hit 75% of the world's population.

But 2019 was also the year that digital security collapsed to such a degree that the internet became widely recognized as a failed infrastructure for commerce, discourse and social interaction. Not just dangerous, challenged, risky or compromised – but failed. It wasn't any single event – a cyber "Pearl Harbor" or an attack on global banks or a stolen election – that pushed consensus beliefs over that threshold, but rather a level of corrosion of trust from a steadily increasing cadence of data breaches, network attacks, information operations and questionable attribution claims. This hit a milestone when a one-day Facebook boycott, organized first by European consumers, essentially shut down the platform as global traffic fell by 70%. The action spread virally around the globe and led to subsequent one-day boycotts of other digital platforms and e-government services.

Quixotic and complicated arguments from consumers about privacy and surveillance and "You should own your own data" were now put aside for a much simpler proclamation: trust in the digital world was fundamentally broken. If digital society was going to move forward from here, something significant, visible and perhaps even revolutionary had to be done about security issues writ broadly.

John Perry Barlow had a point when he wrote in 1996 that industrial-era governments had come to look like "weary giants of flesh and steel" trying to manage a digital world that was inextricably escaping their grasp. After all, 19th- and 20th-century government bureaucracies were designed, as Max Weber understood, to seek control through mastery of detail and predictable processes, yet large-scale information networks were simply too complex and dynamic to master in this way.

This had become painfully visible in rapidly worsening public-sector cybersecurity. And governments had in fact become desperately weary of the mismatch. In 2025, the hopeful notion that governments could be light-touch regulators and permissive umpires of the digital world – providing just enough structure to keep things going while not getting in the way of private-sector innovation – just doesn't ring true any more. When it comes to the intersection of bureaucratic control and digital networks, the time has come to either "get real or go home". Put differently, governments are facing a stark choice between stepping out of the game more or less entirely, or reasserting forceful sovereign control. The fuzzy middle ground that most governments tried to occupy for 30 years is no longer there – because citizens, firms and government agencies themselves have abandoned it.

This is the recognition that fuels a true constitutive moment for the digital world, where societies find they must make a real choice about which direction to take, either towards Barlow's vision or towards a new Westphalian imposition of control. Some of the choices made were quite surprising.

The first big surprise was how quickly and definitively the European Union turned towards Barlow. European governments that had sought at the end of the 2010s to regulate the use of data much more closely confronted a major and surprising dilemma: neither citizens nor service providers wanted the intervention. The massive failure of Europe's General Data Protection Regulation (GDPR) in 2020 made clear that regulating according to vague and uncertain privacy preferences would not work. Every attempt to create a minimum viable consensus on privacy has failed, not only at a global level but increasingly at a national level. The backlash against the GDPR from citizens across the EU decimated the moral "right of enforcement" argument, by which governments claimed to be protecting their citizens and reinforcing a social order, because when it came time to enact the ambiguous provisions of the GDPR, citizens rejected them. It was easy for people to say they wanted more privacy, but the Europeans' market behaviours told another story.

Privacy in the EU is now something that firms, not governments, fully get to define. Large companies' terms of service have become the de facto social contract for commerce and discourse. Many governments, not least at the EU level in Brussels, are quietly relieved that they can leave this tortuous set of issues behind and remove them from the legislative and regulatory agenda. Also, because 90% of public-sector institutions in 2025 run their digital systems on commercial cloud services, the terms-of-service social contract is now equally a contract between governments and citizens. It works rather well, because these were terms that citizens had come to understand, expect and accept, in particular with regard to the use of their data in return for valuable services.

The United States turned towards Barlow for reasons that had more to do with core security. US regulators came to understand that the more regulations they wrote around security, the more monocultures they encouraged – and the more guidance they effectively provided to attackers, since every regulation came to be seen as a blueprint for attack. On top of that, technology won the battle of encryption. When backdoors were required for some secure communications platforms in 2019, the result was exactly as predicted by the naysayers: users moved onto other platforms based outside the US that were more secure. The race continued, but the numbers and the economics were definitively arrayed against Washington, and the National Security Agency's budget hit a ceiling.

The year 2020 saw a dramatic reversal towards deregulation in the US. Major firms were relieved by the regulatory pullback because they felt they had been spending too much effort on compliance and not enough on solving real security problems – a self-serving argument to be sure, but also one with a grain of truth. The leading firms started to create a culture of competition around security, internally and with each other. "Active defence" was something firms tried for a while, but soon found they were attacking each other due to insufficient confidence in attribution. The firms ended up in a deterrence equilibrium, and by 2022, "active defence" measures were rare. After learning about those kinds of boundaries, what emerged was a race to the top. Firms got to choose their own "optimal" security levels, and the market segmented them rather effectively. Some set their "customer-centric security" at higher levels than others; the market responded with greater demand for their services. Many firms invested heavily in insider threat reduction, and because they held the strongest control over that environment, they achieved good results.

It is less surprising to many observers that China is moving in exactly the opposite direction, towards a definitive reassertion of Westphalian control. China's 2016 cybersecurity law, a blueprint for digital techno-nationalism, was just the beginning. By 2019, a growing distrust of foreign products was driving "China First" technology and digital supply chains, cryptocurrencies and data flows. Cyber weapons and ML-enabled autonomous weaponry emerged as the leading edge of Chinese military investment and deployment. Social credit systems linked to government surveillance programmes grew to oversee much of daily life for citizens. A few voices of opposition political activists in Beijing and other major cities have been drowned out by the vast majority of the population, who are enjoying rapid economic growth along with a sense of schadenfreude with regards to the West.

China's performance is now seen as proof that it is indeed possible to combine sovereign, non-democratic control with rapid economic growth and innovation in technology.

India's trajectory may be the most important signal of what many other countries will do over the next few years as they confront the Barlow-Westphalia decision. India's raucous political economy, extending as it did to the digital world, seemed uncontrollable and destined for the Barlow approach … until a massive cyber-attack on the country's electric grid in 2021 shut down major systems for days and caused thousands of deaths, which radically changed the debate. By 2022, India was moving definitively towards a Westphalian synthesis, essentially borrowing the Chinese template and deploying it as best as the Delhi government could. Some of India's large companies and many of its most sophisticated digital citizens wanted to resist this trajectory, but in practice they have lost credibility and are seen by the majority of Indians as precisely the organizations and people who failed to provide social order in the digital world when they had the chance.

By 2025, there are still countries both large and small that are on the fence, but the perspective from places such as Jakarta, Lagos and São Paulo is that time is running out to choose sides. The digital world has in practice been Balkanized – but with a geography that is now much more complex. Some "regions" are governed and bounded by commercial providers' terms of service, and these cross national boundaries and physical geography as if they barely exist, a relic of the 20th century. Other regions are made up of hard national boundaries where sovereign authority is more restrictive, efficient and controlling than any physical state border had ever been.

The Barlow world works surprisingly well in some respects. The experience of being threatened by government control during the late 2010s drove internet communities to become more serious about actively building social contracts, rather than blithely assuming (as in 1996) that functioning societies would simply emerge from "natural self-organizing processes", which underpinned iconic examples such as Wikipedia and some open-source communities. So when governments pulled back, digital society was ready to step up to its constitutional moment. As an iconic example of this maturity, platform firms and citizens negotiated new data covenants that made usage and pricing of personal data clear and transparent in one-page agreements everyone could understand. These were moments of clarity as internet users were no longer either coddled by governments or deceived by firms into believing there were no trade-offs and that they could have all things digital for free.

The Westphalian world also works but in different ways; it is less constitutional and runs more along the lines of traditional power-based equilibria. Deterrence seems to constrain major cross-border digital conflict, though it equally allows for a constant stream of slow intellectual property theft, minor attacks on data repositories and financial systems, and other low-grade conflicts that serve as a constant reminder of insecurity at the subcritical level. Nationally bounded IoT systems mean that older multilateral trading regimes are dying, since most tradable goods are now IoT-enabled. A clear manifestation of this occurred when, in 2002, Beijing declared that only Chinese-made autonomous vehicles would be permitted on Chinese roads, and South Korea followed with the same restrictions for Korean transportation. In 2024, Jordan and Qatar accused Israel of using cyberweapons to violate the Green Line and effectively expand Israeli borders by shutting down competing internet hosting and network sites. Extensive negotiations led by the Canadians and Swiss defused this particular crisis, but everyone is certain that there will be a succession of similar crises for the foreseeable future, and no one is sure just how robust those deterrence equilibria will turn out to be.

Difficult problems are now arising in places – physical and digital – where the Barlow and Westphalia worlds intersect. There is a fundamental mismatch between the driving forces that motivate and regulate these two syntheses, and the friction between them manifests in economic, political, philosophical and occasionally even military domains. For example, aspiring global-platform firms face an extremely awkward interface, as they have gained extraordinary freedom to create their own political economies in Barlow regions, but they must at the same time create domestically configured parastatal structures in Westphalia regions. The process of moving technologies, data and, to a greater extent, people between these two regions involves massive transaction costs and is often simply not worth trying.

Each system probes the other for weaknesses and vulnerabilities, but it is a complicated and ambiguous game where the risks are often seen as greater than the potential benefits. As in the early days of the Cold War, there's an intensive philosophical and ideological competition at work in which each system proclaims that the other is destined for the ash heap of history. But those words belie the observed reality of two very different syntheses, both of which, at least for the moment, appear to be functioning better in many respects, particularly in regards to security, than the global internet mess of 2019.

One major irony of this ideological competition is that, on both sides of the divide, engineering and economic considerations have trumped speech and discourse in importance. Barlow believed that, in the internet era, "anyone, anywhere" would be able to express beliefs without fear of being coerced into silence or conformity. In fact, private social order in Barlow regions turns out to be at least as coercive as government-defined social order in Westphalian regions. Economic growth and digital security go hand in hand no matter where you are, and very few governments or large firms act to preserve the notion that diversity of opinion is a public good worth fighting and sacrificing for. Rather, they both end up wanting "just enough". In the Barlow world, it's true that anyone can enter any domain, but to stay in, you have to play by the rules (here, the terms of service). It's not exactly vigilante justice, but those that deviate face social isolation.

In the Westphalia world, governments provide enough bread-and-circus distractions (in the form of, for example, immersive VR games) to drain off most of the disruptive political energy. Public-facing speech is carefully monitored on a real-time basis and sometimes even pre-real time, using predictive analytic policing of discourse (and, it is rumoured, perhaps even of thought). Rule-breakers don't have to be arrested, thrown in prison or tortured; they simply lose access to the digital services such as banking, healthcare and communications that are necessary for "normal" life. Dissidents are physically present in Westphalian regions and walk the streets freely, but they are radically isolated from each other and from anyone they could convince in digital space, and are thus rendered impotent.

The global internet in 2025 has become much like a set of small towns – pretty safe, largely conformist and basically uncaring about what happens elsewhere.