Platforms and States, Governance and Sovereignty

It has become trite to observe that digital technologies are playing an ever-larger role in our lives. More overlooked is the role played by *platforms* in developing, spreading, and ultimately controlling these technologies. Platforms are at the forefront of Artificial Intelligence (AI) and the Internet-of-Things (IOT), the latest frontiers in software and hardware respectively.

Part 1 will establish the central analogy of this essay: platforms act like quasi-governor within their own domain and as quasi-sovereign in their interactions with states. Part 2 will use the platform-as-governor analogy to frame municipal issues arising from AI. Part 3 will discuss likely international issues arising from IOT that benefit from the platform-as-sovereign analogy.

This essay's overall thesis is that as platforms become an increasingly important part of the global political economy, understanding their state-like characteristics is essential to conceptualizing governance and sovereignty in a digital age.

1. *Platforms as Quasi-States?*

Platforms are a subset of Internet companies whose success is explained by aggregation theory.[1] Briefly, platforms (or 'aggregators') get started by exploiting an abundance of supply (e.g. Google and websites), lack of trust (e.g. Uber and drivers) or some other asymmetry through superior discovery and curation. After users join the platform, suppliers will follow, which in turn makes the platform more attractive to more users, creating a virtuous cycle of decreasing customer acquisition costs. By using automated processes to serve users across the Internet, platforms also enjoy near-zero marginal costs. On the demand side, there may also be network effects (e.g. Facebook's value as a social network increases as more users join). These virtuous cycles tend to result in a monopoly in each sector.[2]

This essay extends this analysis by arguing that the most powerful platforms go on to acquire state-like characteristics. Parallel to the internal and external sovereignty of states, these characteristics will be divided in terms of how platforms govern their own domains and how platforms interact with states.

A. *Platforms as Governors*

Platforms use State-like mechanisms to govern their domains.[3] They punish and reward conduct (e.g. Apple vis-à-vis its App Store developers). They adjudicate disputes (e.g. Airbnb mediates between 'hosts' and 'guests'). Content publication platforms probably go the furthest: they moderate content using 'detailed list of rules, trained human decision-making to apply those rules, and a system of external influence to update and amend those rules'.[4]

---

[1] Ben Thompson, 'Defining Aggregators' (*Stratechery*, 26 Sep 2017) <https://stratechery.com/2017/defining-aggregators/> accessed 21 Nov 2017.

[2] Even competing platforms exist, the user's limited choice is better compared to feudalism. See Bruce Schneier, *Data and Goliath* (W.W. Norton & Company 2015), 58-61. For adapting antitrust doctrines to a digital economy, see Ariel Ezrachi and Maurice Stucke, *Virtual Competition* (Harvard University Press 2016).

[3] Julie Cohen, 'Law for the Platform Economy' (2017) 51 UC Davis Law Review 133, 199-203.

[4] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) Harvard Law Review (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937985> accessed 21 Nov 2017.

More interestingly, governance by the most powerful platforms approximates *private discharge of public governance functions*. Klonick, for example, argues that content publication platforms substantially determine their users' online free speech rights, albeit without any direct accountability. Rather, their governance is motivated by US free speech cultural norms, corporate responsibility, and, most of all, the profit motive.[5] Another example is arguably Amazon's generous return policy exceeding consumer protection requirements: small businesses, which increasingly have no choice but to transact on Amazon, chafe at the policy, which reflects Amazon's interest in gaining market share and arguably threatens to supersede the legislatively determined balance of interests between sellers and buyers.[6]

Platforms have also been co-opted into carrying out public functions. Consider Google's EU-imposed role in administering the 'right to be forgotten': an applicant wishing to exercise her right must submit a removal request to Google, whose decision can be appealed to the local data protection agency. [7] More worryingly, Pasquale argues that the US government has used information-sharing arrangements with platforms, whose surveillance activities are less regulated and hence more extensive, to bypass constitutional constraints on its own surveillance activities.[8]

Unlike other monopolies or transnational companies, platforms blur the line between profit-seeking entities and public authorities. As they become more powerful, so too the need to accommodate them within our framework of domestic governance, as shown in Part 2.

B. *Platforms as Sovereigns*

The most powerful platforms generate huge amounts of revenues and have user bases on par with states. Combined with the abovementioned public characteristics of platform governance, these platforms have acquired geopolitical influence comparable to states.

Legally, this analogy should be applied carefully. Earlier literature has sought to apply the fourfold criteria of Statehood in Article 1 of the Montevideo Convention on Rights and Duties of States to platforms.[9] However, this is conceptually inappropriate because unlike traditional aspirant states, platforms do not seek international legal personhood by carving out rights (and territory) that formerly belong to actual states.

Nonetheless, their increasingly state-like conduct on the international legal order has increasingly defied 'the narrative of the transnational corporation as both constrained by and resistant to the international legal order'. They engage in diplomacy (e.g. Denmark even appointed a 'digital ambassador' to Facebook). They guard their independence through regulatory arbitrage. They advocate for their interests in international governance settings (e.g. Microsoft's call for a Digital Geneva Convention, in which platforms function as 'a trusted and neutral digital Switzerland').[10] More recently, states have turned to platforms for help in safeguarding the sanctity of their elections against Russian influence.[11]

---

[5] ibid.

[6] Ari Levy, 'Amazon's new refunds policy will "crush" small businesses, outraged sellers say' (*CNBC*, 2 Aug 2017).

[7] Case C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos* [2014] ECR 317.

[8] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015), 54-60.

[9] Anupam Chander, 'Facebookistan' (2012) 90 North Carolina Law Review 1807, 1817-1819.

[10] Cohen (n 3).

[11] Jason Horowitz 'Italy, Bracing for Electoral Season of Fake News, Demands Facebook's Help' (*New York Times*, 24 Nov 2017).

The platform-as-sovereign analogy emphasizes both the shifting power differentials between platforms and states and the geopolitical dimensions to their newfound power, which will be helpful in exploring international issues arising from IOT, as shown in Part 3.

2. *AI and Governance*

The AI industry is dominated by platforms. Google subsidiaries DeepMind and Waymo are leaders in AI research and autonomous cars respectively. Amazon has seized pole position in the virtual assistant race. This is unsurprising given that the virtuous cycles in the AI industry resulting from the mutually reinforcing effects of talent, quantity of data, quality of product, and market share, are an extension of aggregation theory.[12] In contrast to this thriving corporate scene, a recent report on AI ethics warned that '[c]urrent framings of AI ethics are failing'.[13] This Part will use the platform-as-governor analogy to frame AI-related governance issues, exemplifying its utility.

A. *Black Box Problem of AI*

Rule of law requires that public power be exercised in an intelligible and predictable manner. In the US, this is embodied in the procedural due process rights guaranteed by the Fifth and Fourteenth Amendment of the US Constitution. In the EU, Article 47(2) of the EU Charter of Fundamental Rights specifically imposes on public authorities a duty to give reasons for its decisions.

Although current AI technology is domain-specific, its decision-making process can be difficult or even impossible for humans to comprehend.[14] The problem this causes for public sector applications of AI (e.g. sentencing decisions in courts) is well-understood.[15] However, if the platform-as-governor analogy is correct, this significantly understates the problem: in principle, the same problem afflicts platforms that are effectively discharging public governance functions using similarly opaque AI.

This is arguably the normative thrust of Article 22 of the EU's General Data Protection Regulation (GDPR), which will come into force in May 2018. On one reading, Article 22 mandates a 'right to explanation' of all decisions made by automated/AI systems, a duty borne by data controllers (i.e. any persons who determine the purposes and means of the processing of personal data).[16] However, the limits of the analogy's normative reach should also be noted. Whereas a powerful platform with quasi-public powers should be held to similar standards as public authorities, it is not clear why this duty should be imposed on all data controllers. Conceivably, non-platform data controllers on equal footing with data subjects should be able to bargain over such right as part of the market process.

---

[12] Kai-Fu Lee, 'The Real Threat of Artificial Intelligence' (*New York Times*, 24 Jun 2017).
[13] Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford, 'AI Now 2017 Report' (*AI Now Institute*, Oct 2017).
[14] ibid. For ongoing efforts to make AI explicable, see Cliff Kuang, 'Can A.I. Be Taught to Explain Itself?' (*New York Times*, 21 Nov 2017).
[15] Campolo et al. (n 13).
[16] Kuang (n 14), though some dispute this interpretation; see e.g. Sandra Wachter, Brent Mittelstadt, and Luciano Floridi 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7(2) International Data Privacy Law 76.

According to two influential long-term AI safety experts, the black box problem could worsen as AI technology moves past its current domain-specificity to become sufficiently general.[17] Putting a dense argument briefly, an AI designed to act *generally* (i.e. across many contexts, including those not specifically envisioned by its designers, users or indeed any humans), even if perfectly designed to act safely, may not act predictably in a specific, local context. As such, rather than equating explicability with accountability, new methods of ensuring accountability without access to an AI's reasoning process should be pursued, such as by statistically auditing the AI's decisions as a class.[18] Specifying AI accountability mechanisms is thus a value-laden technical decision that should be made collectively.

B. *AI-Powered Algorithmic Manipulation*

Platforms can also use AI to manipulate users to an extent akin to coercion. Consider how Uber 'nudged' its drivers. As generalized psychological research suggests that its drivers are likely to stop driving after attaining their revenue targets, Uber sent tailored messages to drivers close to their targets, leading them to keep driving. Instead of psychological research, AI can super-charge such 'nudging': Uber can apply AI algorithms on the data it has collected on its drivers to identify exploitable behavioral patterns down to an individual level. Such asymmetric influence would be even more difficult for drivers to discover, much less the public and regulators.[19]

The specter of secret influence is compounded by the abovementioned black box problem. An AI instructed to optimize a given parameter (e.g. time spent on Facebook) could experiment with variables in highly ways and with side-effects (e.g. give prominence to outrage-provoking fake news) that its engineer would not foresee and could plausibly deny.[20]

The platform-as-governor analogy can inform this budding public discourse. Given that coercion, regardless of its form, demands justification and that AI-powered algorithmic manipulation approximates coercion, its use should be regulated by the political and legal process. Indeed, its subtlety and tendency to make its victim complicit in her own exploitation arguably render it more pernicious. Conversely, the analogy asks whether algorithmic manipulation, like coercion, can be directed towards collectively chosen and socially beneficial ends. Thus, the Chinese government's plan to build an AI-powered social credit system by 2020 would be exalted by the statist and criticized by the civil libertarian.[21]

C. *A New Social Order*

The platform-as-governor analogy's emphasis on the continuity between platforms and governance helps us imagine how society could be reordered in pursuit of different political visions.

---

[17] Nick Bostrom and Eliezer Yudkowsky 'The Ethics of Artificial Intelligence' in Keith Frankish and William Ramsey (eds) *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press 2014).

[18] See e.g. George Nott, 'Google's research chief questions value of "Explainable AI"' (*Computer World*, 23 Jun 2017) <https://www.computerworld.com.au/article/621059/google-research-chief-questions-value-explainable-ai> accessed 21 Nov 2017.

[19] Campolo et al. (n 13).

[20] Relatedly, that Facebook and Google possess the technical capability to surreptitiously influence public discourse and even election results has been noted by commentators: e.g. Schneier (n 2) 113-116.

[21] Rachel Botsman, 'Big data meets Big Brother as China moves to rate its citizens' (*Wired*, 21 Oct 2017) <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion/> accessed 21 Nov 2017.

For the civil libertarian, by locating the powers that platforms and government have over individuals on the same continuum, the analogy calls for a new separation of powers. Recall the US government's reliance on platforms for its surveillance activities: as private surveillance shades into public surveillance, constitutional protections that only apply to the latter make little sense.[22] Beyond restricting platform-government cooperation to forestall the rise of a platform-government complex, the civil libertarian would consider dismantling existing platform conglomerates that wield disproportionate influence in public life.

But this defensive stance must be balanced against the potential benefits of AI-enhanced governance. For example, San Francisco's SFpark program used IOT sensors to monitor parking availability and traffic conditions and AI to dynamically adjust prices and inform drivers of real-time availability. It was a success on multiple metrics: parking availability and net revenues increased, whereas search time, congestion, traffic volume and greenhouse gas emissions decreased.[23] With the current distribution of data and expertise, it is difficult to see how larger-scale applications of AI can be realized without greater platform-government cooperation. More nuanced institutional arrangements may better manage this trade-off.

For the statist, however, platform-government cooperation is the first step to further centralization. Advancements in AI and IOT may finally refute Hayek's defense of the free market: capturing and running the sum of all data through a sufficiently advanced AI could create a planned economy. Replacing the invisible hand with a platform-government digitized hand might be Lenin's 21st-century revenge.[24]

3. *IOT and Sovereignty*

Following personal and mobile computing, IOT promises to be the next wave in computing hardware. As IOT unlock new sources of data and enable ground-breaking applications, further inroads into the IOT industry by AI-powered data-hungry platforms are all but guaranteed, beginning with voice assistants (e.g. Amazon's Alexa) and thermostats (e.g. Google's Nest Labs).

This Part argues that the advent of platform-operated IOT is likely lead to technology protectionism and international efforts to regulate cyberspace. It also seeks to use the platform-as-sovereign analogy to remedy Part 2's wholly domestic perspective of governance. Such a perspective failed to consider the diverse and complex power relations between different states and different platforms. Whereas polities like the US, China, and the EU (hereafter collectively termed 'The Big Three') can impose top-down regulations on most powerful platforms (albeit with varying level of political will to do so), the average country probably lacks the leverage to do so, a perspective that is neglected in the literature. Relatedly, that platforms may pursue geopolitical goals (whether autonomously or under state influence) was not considered.

[22] Pasquale (n 8).
[23] Ezrachi and Stucke (n 2) 211-217.
[24] ibid.

A. *Technology Protectionism*

Technological protectionism is not new.[25] US platforms in China operate (if at all) under the shadow of the Great Firewall and face stringent cybersecurity laws, which are motivated in part by Snowden revelations that the US government has installed backdoors into US-made telecom equipment and had access to user data held by US platforms.[26] Likewise, the US has banned Chinese networking equipment amidst fears that they could be used for state-sponsored spying. Already, the same suspicions are now being raised against Chinese IOT makers like Hikvision, a surveillance cameras manufacturer,[27] and DJI, the market leader in drones.[28] EU regulators have brought enforcement actions alleging that US platforms – which dominate European markets – have violated antitrust, data protection, and tax laws, attracting accusations of protectionism. The exact interpretation and implementation by EU officials of the impending, vaguely-worded GDPR remains to be seen, but US platforms are almost certainly disproportionately affected.[29]

The advent of IOT suggests pressure to adopt protectionist policies will intensify as they provide a way for states to act unilaterally against platform-operated IOT. As platforms dominate IOT, each platform will control a world-size robot, whose sensors will be their eyes and ears and actuators their hands and feet, enhancing their ability to affect core state interests.[30] For example, the platform operating self-driving cars can monitor everything occurring along a country's roads. Worse, a software glitch (whether innocent, intentional or caused by malicious hackers) can wreak havoc to a country's transportation networks. Such fears will provide pretext for protectionism, especially by The Big Three, which are most capable of bearing the costs of protectionism (i.e. higher prices and developing local substitutes). Other states, however, may be forced to choose between economic benefits and independence from platforms (and, possibly, their parent states).[31]

All in all, the risk of IOT protectionism against platform-operated IOT is considerable, notwithstanding that these risks may not be successfully mitigated by protectionism[32] and that compromise solutions may work better.[33]

---

[25] For the rise of data localization laws, see e.g. Anupam Chander and Uyên Lê, 'Data Nationalism' (2015) 64(3) Emory Law Journal 678.
[26] Schneier (n 2).
[27] Dan Strumpf, 'Surveillance Cameras Made by China Are Hanging All Over the U.S.' (*Wall Street Journal*, 12 Nov 2017).
[28] Paul Mozur, 'Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say' (*New York Times*, 29 Nov 2017).
[29] See e.g. Kuang (n 14).
[30] A twist on Schneier's analogy: Bruce Schneier, 'Click Here to Kill Everyone' (*New York Magazine*, 27 Jan 2017).
[31] Relatedly, Lee speculates that AI may bipolarize geopolitics because, first, the AI industry will be dominated by US and Chinese companies; second, AI applications will result in mass unemployment and generate huge profits for these companies; and, third, only the US and China will be able to tax these companies. Thus, other countries will have to choose between poverty or being beholden to one of these two countries: Lee (n 12).
[32] Chander and Lê (n 26).
[33] E.g. the UK government allowed the sales of Chinese telecoms equipment that passed a GCHQ-imposed security review: Philip Chertoff, 'Why the US Government Shouldn't Ban Kaspersky Security Software' (*Wired*, 4 Sep 2017) <https://www.wired.com/story/why-the-us-government-shouldnt-ban-kaspersky-security-software/> accessed 21 Nov 2017.

B. *International Regulation of Cyberspace*

As IOT blurs the distinction between cybersecurity and physical security,[34] states (especially those not from The Big Three and with limited cyber-capabilities) will have stronger incentives to use multilateral instruments to collectively regulate cyberspace.

There are many candidate treaties to govern cyber-conflicts, platforms, or some specific subset of cyberspace. For example, the abovementioned Digital Geneva Convention proposed by Microsoft would prohibit governments from attacking civilian networks and infrastructure. Less ambitiously, the Tallinn Manual, which purports to merely state how international law applies to cyber-conflicts, could be ratified. Alternatively, specific agreements to, say, outlaw government-mandated vulnerabilities in domestically produced software and hardware could be sought.[35]

Whether unilateral or multilateral actions are taken by states to preserve their sovereignty, platforms can be expected to lobby states in pursuit of their own interests and to play a sovereign-like role in the international order.

Conclusion

This essay has been simultaneously ambitious and timid. It has ambitiously pursued a single analogy – platforms are like states – across a wide range of contexts. The essay thus stands or falls by the perspicuity of this analogy. However, it has timidly avoided firm conclusions in all the legal issues raised. This is done so in full awareness that these issues are complex and reasonable disagreement across individuals and societies is possible. Ultimately, while the analogy is a good first step in diagnosing the problematic status quo, it is rarely decisive of subsequent reform, which requires exercising far more specific and controversial judgments than what this essay can explore.

Prediction is difficult, especially about the future and only time will tell how these forces will play out. But as AI and IOT promise to make platforms more powerful, their self-conception becomes ever more important. If this essay's central analogy is right, it is not clear that their avowed position as neutral, shareholder-value-maximizing entities is tenable. With great power comes great responsibilities and how platforms understand their moral responsibilities will have far-reaching consequences for us all.[36] From today's vantage point, platforms' otherwise sunny prospects of ascendance are marred by a looming dark cloud: regulation of Big Tech has finally entered the Overton window in the US, home to the largest platforms and potentially their most effective regulator.[37]

We shape our tools, and thereafter our tools shape us. Anxieties over the stress modern technology exerts on the foundations of the liberal order are not new.[38] The eventual impact of AI, IOT, and other emerging technologies ultimately depends on the larger political economy,

---

[34] Schneier (n 31).
[35] Chertoff (n 34).
[36] See e.g. concerns over Mark Zuckerberg's manifesto and proposed free-market-oriented social-network-specific regulations targeted at Facebook, Ben Thompson, 'Manifestos and Monopolies' (*Stratechery*, 21 Feb 2017) <https://stratechery.com/2017/manifestos-and-monopolies/> accessed 21 Nov 2017.
[37] Ben Smith, 'There's Blood in The Water in Silicon Valley' (*Buzzfeed*, 12 Sep 2017) <https://www.buzzfeed.com/bensmith/theres-blood-in-the-water-in-silicon-valley> accessed 21 Nov 2017.
[38] Richard Danzig, 'An Irresistible Force Meets a Moveable Object: The Technology Tsunami and The Liberal World Order' (2017) 5(1) Lawfare Research Paper Series 1.

which will be reconfigured significantly by platforms. This author suspects that the foregoing platform-driven developments vis-à-vis governance and sovereignty are only the thin end of a much large wedge.