What Is Platform Politics? Foundations of a New Form of Political Power

By Michael Seemann, first published in 'Zeitschrift für sozialistische Politik und Wirtschaft' (SPW), S. 44 - 49. in December 2017.

In early 2017, shortly after the inauguration of Donald Trump, the rumor began to spread that Facebook founder Mark Zuckerberg himself was planning to enter the presidential race in 2020. Following Trump's victory, everything may seem possible, but this speculation was based solely on the so-called "Listening Tour", Zuckerberg's trip through the US, where he wanted to meet Facebook users in person.[1]

This rumor is only a symptom of the general lack of understanding of our times. For Mark Zuckerberg has long been a politician. He has an enormous impact on the daily lives of two billion people. He makes decisions that affect how these people get together, how they interact, even how they see the world. So Zuckerberg is already perhaps the most powerful politician in the world. Any job in traditional politics, including the office of US president, would be a step down.

In this text, I will try to determine and analyze the ways in which platforms act politically, examining how they organize their power base and in which fields their policies are already changing the world. But first we should eliminate three fundamental misconceptions about platform politics.

Three Misconceptions About Platform Politics

1. Platforms are not (only) the objects of politics, but also powerful political subjects

When we talk about "platform politics" or platform regulation, we tend to think of platforms as the subjects of regulation and policymaking. That isn't wrong as such, but it conceals the far more important point that today, the platforms themselves have become influential regulators and political actors.

Platforms provide the infrastructure for our digital coexistence – with an emphasis on "structure". For this structure is neither arbitrary nor neutral: Defining the structure of communication is a political act in and of itself, one that enables certain interactions and reduces the likelihood of other kinds of communication. This is a profound intervention into our social lives, and therefore in itself political.

[1] Alex Heath: Speculation is mounting that Mark Zuckerberg wants to serve in government, in Business Insider, http://www.businessinsider.de/speculation-mounting-that-mark-zuckerberg-wants-work-government-2017-1?r=US&IR=T, 01/05/2017.

So it makes sense to think about platforms not merely as companies that provide Internet services, but as political entities or even institutions.[2] Their impact on the political debate, on our society and coexistence, and therefore on all kinds of political decisions, is nothing short of the influence of traditional media. Platforms can be regarded as the Fifth Estate. But unlike the other four estates, platforms are not limited by the boundaries of the nation state; they act and think globally by design. And in contrast to other institutions, they don't try to overemphasize their socio-political significance; after all, political responsibility is bad for business. Platforms rather tend to downplay their political power and refuse to take responsibility. They are political actors in spite of themselves.

2. Platforms exercise a different form of power

One reason why platforms are still not taken seriously as political actors is the general lack of understanding of their power dynamics.

When politicians come up against platforms, they like to throw the weight of their political legitimation around. They talk about the “primacy of politics”, as if to convince themselves and others of their agency. This primacy is derived from the fact that the politician came into office by way of a sovereign, collective decision. But platforms, too, generate a kind of legitimation through collective decision-making, even though this works slightly differently.

In his book *Network Power*, David Singh Grewal argues that the adoption of standards can be understood as a collective decision.[3] And standards are but the conditions of possible interactions, which is why the social relevance of every decision for or against a standard is inherent political. The mere fact that these decisions are not all taken simultaneously as they would be in an election, but rather in staggered intervals (“aggregated”), does not diminish their social impact.

The power of these aggregated, collective decisions is nothing new. It relates to the languages we speak, the manners we cultivate or accept, and of course, to the choice of network service we choose to use. In the end, we join Facebook not because of its great product quality, but because all our friends are on Facebook.

In economics, this phenomenon is called the “network effect”, but Grewal is quite right to view it as a political power factor in its own right. Once a certain standard is widely established, the pressure on the individual becomes so great that there is little choice but to adopt that standard as well – the alternative often being social ostracism.

We accept the “network power” that these standards wield, because ultimately they can never be enforced by individuals. At least that applies to open standards. No one can prevent me from learning Russian, or from making a server available on the Internet with open protocols like TCP/IP. Social pressure always comes from the community as a whole, so it can never instrumentalized individually.

---

[2] Michael Seemann: Das Neue Spiel – Strategien für die Welt nach dem digitalen Kontrollverlust, Freiburg 2014, p. 204 ff.
[3] Grewal, David Singh: Network Power – The Social Dynamics of Globalization, p. 9.

Network power, however, becomes “platform power” when the standards adapted contain key mechanisms of exclusion. Facebook could withhold access to my friends at any time, or place temporal or local restrictions on it. On the one hand, access control of the standard is at the heart of the platform's business model, on the other hand, it is the basis of its political power.

To sum up: Platform Power = Network Power + Access Control.

3. Regulation of platforms increases their power

Of course, even in conventional politics it has become clear that platforms have this uncanny power, but since politicians don't understand that power, they are simply making matters worse. They are under the misconception that dealing with Google, Facebook, Apple and Co is much the same thing as the corporate power structures they might have encountered at Siemens or at Deutsche Bank. And so they resort to the playbook of political regulation to match these powers.

But platform providers are not just large enterprises; their power is based on more than just money and global expansion. Rather, the platform is **f**acing down the nation state itself, as a systemic competitor – even if neither side is prepared to admit it yet.

This is why all efforts in conventional politics to regulate platforms must lead to a paradox. Even while politicians are shaking their fists at Google and Facebook, they are granting these platforms more sovereignty by the minute. Any new constraints devised by policymakers just serve to strengthen the political power and legitimacy of the platform. One example is the European Court of Justice ruling on the so-called “right to be forgotten”, which forces Google to redact search results following a very vague list of criteria.[4] Another example is the notorious Network Enforcement Act, recently introduced by the German Federal Minister of Justice Heiko Maas, which obliges Facebook and other platforms to delete what is deemed **“**obvious unlawful content**”**.[5] In both cases, the state has relinquished its powers of jurisdiction and law enforcement to the platform in question. At first sight, this makes perfect sense, because platforms are the logical point of contact for regulating the digital world, thanks to their platform power and deep, data-driven insights. At the same time, this is fatal, because the state further increases the power of the platforms in this way, making itself dependent on its very competitors.

The Three Spheres of Platform Politics

The political influence of platforms takes many forms. I would like to examine three departments more closely where platforms are already very influential today and will gain even more influence in future (without this claiming to be an exhaustive list): Domestic Net Policy, Foreign Net Policy, and Security Net Policy.

Domestic Net Policy

[4] Michael Seemann: Das Neue Spiel – Strategien für die Welt nach dem digitalen Kontrollverlust, Freiburg 2014, p. 223.
[5] Markus Beckedahl: NetzDG: Fake-Law gegen Hate-Speech, in Netzpolitik https://netzpolitik.org/2017/netzdg-fake-law-gegen-hate-speech/, 06/30/2017.

The term “net politics” (Netzpolitik) has become widespread, in the German-speaking net in particular, since it originated here with the popular political blog of the same name.[6] The Netzpolitik site addresses topics like data protection, net neutrality, censorship and many other Internet-related areas of politics. It is important to regard the network as the *subject* of net politics in this case.

For now, the term “domestic net policy” is merely intended to highlight the concession that these internal/external or object/subject relationships no longer exist – political issues pertaining to the net increasingly arise from within the net. Which implies that these issues can only be solved from within. This is not only pertinent to those problems with hate speech, trolling and fake news we are currently discussing, but also to older issues such as identity theft or doxxing (publishing personal information with malicious intent).

Since these problems mostly arise on platforms, it is logical to expect the according countermeasures to come from the platforms themselves. While this does indeed happen occasionally, overall these interventions are still seen as insufficient. In fact, platforms display a lot of reluctance towards regulations in general. They are hesitant to make use of the political power they already wield, for instance by establishing and enforcing stricter community rules.[7] Still, the awareness of the problem seems to have sharpened. Facebook's new mission statement in February 2017 already indicated as much[8], and Twitter[9] and Google[10] have been giving similar indications. After the Nazi march that escalated in Charlottesville, many platform providers were pushed to action and subsequently banned right-wing accounts and websites from their services. Twitter and LinkedIn suspended a range of “White Supremacist” accounts, while Facebook, Google and GoDaddy, a popular domain registry, blocked domains and groups that were spreading hate. Most notably, the Nazi website Daily Stormer was blocked, and even kicked out of the content delivery network Cloudflare.[11] It is still not clear, however, whether these measures are really the most suited to address the aforementioned problems. The results so far give little cause for hope.[12]

---

[6] See: http://netzpolitik.org.

[7] On the one hand, this is due to the fact that these are still profit-oriented companies, and this kind of regulation doesn’t generate any more turnover, but a lot of additional costs instead. On the other hand, most company founders and employees in Silicon Valley hail from the startup culture largely dominated by libertarian thought – a context in which any intervention into current debates is interpreted as an assault against freedom of speech.

[8] Mark Zuckerberg: Building Global Community, https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634, 02/16/2017.

[9] Kerry Flynn: Twitter just took its biggest stance yet on hate speech, http://mashable.com/2017/10/17/twitter-hate-speech-abuse-new-rules-women-boycott/#vfo7gOJrokqD, 10/17/2017.

[10] Dan Seitz: Google Is Cracking Down On Fake News In Search Results, http://uproxx.com/technology/google-search-results-fake-news/, 03/13/2017.

[11] David Ingram, Joseph Menn: Internet firms shift stance, move to exile white supremacists, https://www.reuters.com/article/us-virginia-protests-tech/internet-firms-shift-stance-move-to-exile-white-supremacists-idUSKCN1AW2L5, 08/16/2016.

[12] Kerry Flynn: Facebook’s ‘Trust Indicators’ is apparently a gift to select media partners, http://mashable.com/2017/11/16/facebook-trust-indicators-fake-news-problem/, 11/16/2017.

Foreign Net Policy

While Facebook's handling of hate speech and fake news can be relegated to the *Domestic Net Policy* department, Heiko Maas' aforementioned *Network Enforcement Act* would be the subject of the *Foreign Net Policy* department. "*Foreign Net Policy*" mostly (but not exclusively) references the way in which platforms encounter the state, and how these parties meet and negotiate their mutual interests. Of course, the standard case is a state attempting to regulate a platform, as we have seen above. The EU, for example, has several lawsuits pending against Facebook and Google, and the conflicts between the US government and platform providers are becoming increasingly apparent as well.[13]

Relations between platforms and states have not always been this bad in the past. Notably, the US State Department under Hillary Clinton made use of various platforms for foreign policy purposes. In her influential speech on Internet and Freedom in 2010, Clinton described the platform providers as important partners in terms of global spreading of democracy and human rights.[14]

Jared Cohen played a particularly pivotal role here.[15] Cohen had joined the State Department while still under Condoleezza Rice, but rose to prominence during Clinton's office. When in 2009, a revolution was threatening to break out in Iran, Cohen called Twitter and convinced them to postpone their scheduled maintenance downtime.[16] Twitter played an important part in the coordination of the upheaval.

When the Arab Spring finally broke out in early 2011, Cohen was already working at Google, where he helped coordinate various inter-platform projects. Facebook, Twitter and Google in their own ways all tried to support the uprisings in the Arab World, and even cooperated with one another to do so. One example is the case of the service speak2tweet: Google provided a telephone number which people from Egypt could call to record a message. These messages were then published on Twitter, thus bypassing the Egyptian Internet shutdown.[17]

Since the Snowden revelations of 2013 at the latest, relations between Silicon Valley and Washington have cooled down significantly. Platforms have since been trying to protect and distance themselves from state interference. This is mostly achieved through the increasing use of encrypted connections, and through elevated technical and legal security.[18] In the US, this

---

[13] Julia Fioretti: EU increases pressure on Facebook, Google and Twitter over user terms, https://www.reuters.com/article/us-socialmedia-eu-consumers/eu-increases-pressure-on-facebook-google-and-twitter-over-user-terms-idUSKBN1A92D4, 07/24/2017.
[14] Hillary Clinton: Statement: Hillary Clinton on internet freedom, https://www.ft.com/content/f0c3bf8c-06bd-11df-b426-00144feabdc0, 01/21/2010.
[15] Wikipedia: Jared Cohen, https://en.wikipedia.org/wiki/Jared_Cohen.
[16] Ewen MacAskill: US confirms it asked Twitter to stay open to help Iran protesters, https://www.theguardian.com/world/2009/jun/17/obama-iran-twitter, 06/17/2009.
[17] Charles Arthur: Google and Twitter launch service enabling Egyptians to tweet by phone, https://www.theguardian.com/technology/2011/feb/01/google-twitter-egypt, 02/01/2011.
[18] Since 2013 Google and Twitter, for instance, have been contesting a number of secret court orders on the highest levels of jurisdiction. See for example: Sam Byford: Google challenges US government's private data demand in court, https://www.theverge.com/2013/4/5/4185732/google-fights-national-security-letter, 04/05/2013.

development in general, and the move towards more cryptographically secure systems in particular, is viewed with a mounting sense of discomfort.

The conflict than escalated in spring 2016, due to the iPhone that FBI investigators found with the perpetrator of the San Bernardino attacks. The phone was locked and encrypted, and so the investigators ordered Apple to assist with the decryption. Apple refused – in order to unlock the phone, Apple would have had to introduce a security vulnerability in its security software. A dangerous endeavor, from Apple's perspective, that would have reduced the security of all other Apple devices and therefore, consumer confidence. In the end, the FBI had to work with a third-party security company to unlock the iPhone.[19]

Beside these varied forms of cooperation and conflict between platforms and states, platform-platform relations should also be taken into account, of course.[20] One politically tangible example is the fact that Facebook is increasingly losing users from the extreme right and right-wing spectrum to its competitor, VKontakte.[21] VKontakte is the equivalent of Facebook in Russia, albeit with a completely different set of guidelines. For instance, while you might get into trouble for posting homophobic contents on Facebook, you might get into trouble on VKontakte for posting the Rainbow Flag.

A segregation of society along the boundaries of different platforms and their according policies seems to be a plausible scenario, and may well provide a lot more material for *Foreign Net Policy* in future.

Security Net Policy

For some time now, there has been growing debate on issues like “cyberwar” and “cyber security” in political circles. The expression simply references a new form of war, conducted with digital means. The United States and Israel were the vanguard here, and in 2010 managed to destroy a uranium enrichment facility in Iran, using a highly rigged and upgraded “*cyber weapon*”, in this case the custom-designed computer worm *Stuxnet*.[22] The so-called *Stuxnet shock* marked the beginning of a global arms race in terms of hacking capacity in general. Cyber-attacks have since become more and more commonplace, be it China's attacks on Google[23], North Korea's attack on Sony Pictures[24], or Russia's attack on the US elections. The “*cyber*” terminology is frequently explained by the fact that the military has different areas of operation: ground forces (army), water (navy) and air (air force) – and now, “cyber” opens up a

[19] Wikipedia: FBI-Apple encryption dispute, https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute.
[20] Not to mention the constant conflicts regarding interfaces, standards and market shares, even though these also have political weight, of course.
[21] Katie Zawadski: American Alt-Right Leaves Facebook for Russian Site VKontakte, https://www.thedailybeast.com/american-alt-right-leaves-facebook-for-russian-site-vkontakte, 03/11/2017.
[22] Wikipedia: Stuxnet, https://en.wikipedia.org/wiki/Stuxnet.
[23] The attacks went down in history as “Operation Aurora”. Wikipedia: Operation Aurora: https://en.wikipedia.org/wiki/Operation_Aurora.
[24] Axel Kannenberg: USA: Nordkorea steckt hinter Hackerangriff auf Sony Pictures, https://www.heise.de/newsticker/meldung/USA-Nordkorea-steckt-hinter-Hackerangriff-auf-Sony-Pictures-2504888.html, 12/19/2014.

whole new area of operations, complete with the demand that specific capacities be strengthened accordingly.[25]

That said, the core misunderstanding here is the assumption that cyber-wars primarily take place between nation states. Even today, that is hardly the case. On the one hand, almost every "cyberattack" is an assault on a platform at the same time. The attack might pertain to the Microsoft operating system (as in the case of Stuxnet and many others), or to specific services (the attack on Google was directed at Gmail mailboxes, as was the Russian hack of John Podesta's emails). Almost without exception, a software or service provided by a specific platform is involved.

Further, many attacks are directed at platforms as their primary target. Perhaps the most prominent case is the 2015 attack from China on the GitHub developer platform. GitHub is a popular website where software developers can store and synchronize versions of their code and share with other users. Nearly all popular open source projects can be found there – including one called "The Great Fire". The "Great Firewall" is what China's powerful Internet censorship architecture is usually referred to, and accordingly, "The Great Fire" is a special toolkit designed to circumvent the Chinese firewall. Of course, the Chinese government didn't find this at all agreeable.
While it is not unheard of that China simply shuts off services it objects to by activating the Great Firewall, GitHub was a notable exception. Blocking local developers' access to Github would have been tantamount to shutting down the Chinese software industry altogether, something not even China could afford. But with a censorship infrastructure that lets millions of requests per second come to nothing, the Chinese came up with another idea: redirecting the censored requests from China to one single destination on the net instead. This is the core idea behind "The Great Cannon".[26]

GitHub was hit by millions and millions of requests from all over China, pushing the website to its utmost limits. In IT security terms, this is called a DDoS attack, or "*distributed denial of service*".[27]

Finally, platforms are not only the target of cyber attacks, but more and more frequently the last line of defense for other targets. In 2016, a DDoS attack came down on the blog of security researcher Brian Krebs. His analysis of the attack revealed that the attack had been carried out mainly by Internet routers and security cameras. The underlying explanation was that a vulnerability in the operating system "Mirai", commonly used in such devices, had allowed hackers to take over millions of these devices. It was the largest bot army the world had ever seen.

---

[25] Handelsblatt: Zu Land, zu Wasser, in der Luft – und im Internet, http://www.handelsblatt.com/politik/deutschland/bundeswehr-erhaelt-cyber-truppe-zu-land-zu-wasser-in-der-luft-und-im-internet/13505076.html, 04/24/2016.
[26] Lead investigator of this incident was the Citizen Lab, which also published a detailed report on their findings. Citizen Lab: China's Great Cannon: https://citizenlab.ca/2015/04/chinas-great-cannon/, 04/10/2015.
[27] Wikipedia: DDoS: https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack.

And so Krebs had no choice but to look for cover with Google's proprietary server infrastructure, designed for precisely that purpose, and commonly known as “Project Shield”. A platform operated, incidentally, by Jigsaw, the Google spin-off think tank founded by Jared Cohen.[28]

So the inconvenient truth behind “cyber” is that it is not at all the state that is at the center of events, but the platforms. The platforms provide the infrastructure that comes under attack, and more importantly, they are increasingly becoming targets themselves. Most importantly, the platforms are the only players with sufficient technical capacity and human resources to fend off these kinds of attacks, or prevent them to save the day.[29] Either way – if the worst comes to the worst, the state might have no choice but to slip under the umbrella of a welcoming platform, just like Brian Krebs did. “Cyber Sovereignty” on a state level still remains a pipe dream at present.

Conclusion

Platforms are already holding a prominent position within the social order, which in itself is becoming more and more digitalized. Platforms regulate critical infrastructure for the whole of society, and provide protection and order on the Internet. Increasingly the platform is in direct competition with the state, which generates dependencies that could turn out to be a threat for nation states.

Whether the state will maintain its independence and sovereignty in the long term or not, will depend on its ability to operate and maintain digital infrastructure on its own. In the long run, the state needs to become a platform provider itself.[30]

Platforms, on the other hand, would be well advised to look at the democratic institutions of states that have evolved over time, to address their own Domestic Net Policy issues. Even a rudimentary rule of law instead of generic “Terms of Service”, even the most tentative embrace of transparency, checks and balances, and the possibility of appeal in all actions, would make the platforms' fight against hate speech and fake news more credible and fair, and most certainly more successful.[31]

---

[28] Brian Krebs: How Google Took on Mirai, KrebsOnSecurity, https://krebsonsecurity.com/2017/02/how-google-took-on-mirai-krebsonsecurity/, 02/03/2017.

[29] The main problem of states in this area is actually finding suitable staff. IT security experts are what might be called a rarity in human resources, and so the industry tempts them with exorbitant fees and career options. The state, and the military in particular, can hardly keep up with either of these.

[30] How that might work out was the topic of an opinion I presented the context of an expert hearing in the German Bundestag. See Michael Seemann: Stellungnahme: Fragenkatalog für das Fachgespräch zum Thema „Interoperabilität und Neutralität von Plattformen“ des Ausschusses Digitale Agenda am 14.12.2016, https://www.bundestag.de/blob/484608/b1dc578c0fdd28b4e53815cda384335b/stellungnahme-seemann-data.pdf, 12/12/2016.

[31] This suggestion of mine was first presented in my re:publica talk in 2016. See Michael Seemann: Netzinnenpolitik – Grundzüge einer Politik der Plattformgesellschaft, https://www.youtube.com/watch?v=eQ-a13ZL33g, 03/11/2016.

In short: platforms need to become more like nation states, and states need to become more like platforms.

In the meantime both sides, the state and the platform, don't have much choice but to cultivate their mutually critical-cooperative relationships and collaborate in all three departments – Domestic Net Policy, Foreign Net policy, and Security Net Policy. It should be noted that competition between the two might even be advantageous for the citizen (or user) in the long run. While the state is trying to protect me from the overbearing access of the platforms, platform providers are trying to protect me from the excessive data collection of the state.