The Emergent Technopolitics of Big Tech Domination

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Arvind Anand

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

Introduction

Before the pervasiveness of the world wide web, computation was accessible only via large mainframe systems and expensive personal computing solutions. However, in the modern computing era, personal devices like smartphones and laptops receive computed data from large server clusters operated and maintained by large tech companies like Amazon. Amazon's Web Services provide server-side computation as a service, which allows individuals and large startups alike to provision powerful servers without the overhead of buying and maintaining the physical hardware. The consolidation of computational power invariably provides certain actors with the ability to influence the landscape of the open internet by governing content on their services.

The computational artifacts generated by these large systems can also provide certain actors with the unfettered ability to manipulate communities, nations, and society (Smyth, 2019). Policy excuses like "self-regulation" provide asymmetries between tech companies and their users. Regardless of the intention behind big tech giants, the market economy and data mining technical capabilities have inevitably given rise to societal and political ideologies that result in mass surveillance and unwarranted privacy violations.

This paper will examine the technopolitics of internet governance and the need for regulations in "big tech." This paper will also evaluate the current situational asymmetries in the tech industry and the proposed solutions to fix them.

Policing the Open Internet

In 2019, AWS maintained a healthy lead in the market, which positions it as the most popular, innovative, and influential among all the cloud services providers on the planet (Raj Bala, 2021). Amazon now maintains and operates the service for a significant portion of the global internet indirectly by providing infrastructure-as-a-service to hundreds of tech companies around the globe. In terms of influence, AWS outcompetes the rest by virtue of its engineering prowess and innovation (Raj Bala, 2021). As a result, AWS indirectly controls large portions of the internet globally by providing computation-as-a-service to their customers.

For AWS to maintain its market dominance, its customers must trust in its ability to deliver on maintaining customer data security and ensuring high availability of services (Page, 2021). On top of that, AWS and its customers mutually benefit from each other via branding and marketing (AWS, 2022). Tech companies that operate at a massive scale like Snap and Intuit include their AWS use case in their marketing to bolster their technical abilities and brand image, as seen in Figure 1. AWS also publishes case studies on how its products have revolutionized companies across 25 different industries (AWS, 2022). These case studies also bolster AWS's brand as a reputable and dominant player in the cloud space by showcasing the breadth of their products' success.

Snap

Snap migrated to a microservices architecture on AWS to improve scalability, optimize availability, minimize latency, and reduce costs. Freed from managing infrastructure, Snap engineers can focus on developing new, unique offerings and experimenting with new services and features to enhance visual communication and storytelling for its users.

Figure 1: Snap's case for using AWS (AWS, 2022)

As AWS expanded its market, its services became available to any willing customer: including problematic social media sites and malware. For instance, In July 2021, the Israeli government used an IOS malware exploit named Pegasus to spy on high-profile figures and

journalists (Johansson, 2021). They used several cloud service providers, including AWS, to store data (Johansson, 2021). AWS eventually took down Pegasus's cloud access since it was rightfully deemed an illegal activity (Johansson, 2021). AWS's marketing could take a hit if it were associated with illegal behavior; one could argue that it would dissuade potential customers from using the cloud services. Given that AWS's customer base is critical for its successful domination and resulting success in the cloud industry, it would be in AWS's best interest to prohibit harmful actors from using their services.

The following case study observes an instance of AWS shutting down a harmful actor: Parler. It examines how AWS's actions play into its power over the open internet and other cloud service providers.

Case Study: Content and Free Speech

Parler was founded in 2018 as a social media site that is "free speech-driven" (Vengattil, 2021). However, it served as a breeding ground for hate speech and violence, so much so that the activity on the platform directly resulted in the U.S. Capitol riot on January 6, 2021 (Vengattil, 2021). As a result, Apple and Google removed Parler from their respective app stores, and AWS shut down all of the compute resources Parler provisioned for web hosting and data storage (Vengattil, 2021). The removal of Parler from AWS shortly after January 6, 2021, was a display of AWS's influence on the free internet (Dang, 2021). The removal, ultimately, prevented the company of Parler from developing and deploying their applications. Critics of this move say that it showcased how far down the stack big tech companies can restrict free speech; however, others would argue that it is necessary to remove violence from the public internet, wherever it may be (Dang, 2021). AWS's action to remove Parler from using infrastructure is an instance of them exercising their influence to enforce the political idea of restricting free speech in the case

of extremism. According to Dang, AWS is expanding its Trust and Safety team to "monitor for future threats" (Dang, 2021). It is not viable for AWS to sift through the massive amounts of content in data storage and applications running on compute platforms, but they plan to "get ahead of future threats" to better regulate their cloud service (Dang, 2021). Amazon expanding their Trust and Safety team is another example of their influence to enforce their political stance on restricted free speech because it will prevent future extremism from spreading misinformation at the infrastructure level.

While the removal of Parler from AWS did not directly impact the cloud industry, it did force AWS and other players in the tech industry to revisit what is and what is not acceptable on the public internet within their platforms (Gillespie, 2020). According to Gillespie, many tech platforms "keep an eye on each other" and "act in concert" when it comes to deplatforming individuals and internet-scale applications alike (Gillespie, 2020, p. 6). Gillespie also mentions that Cloudflare, a large network infrastructure company, was inspired by the actions taken by Twitter and Facebook to no longer host extremist sites like Daily Stormer (Gillespie, 2020). Infrastructure services are also enrolled in the set of players in the tech space; they also respond and influence other players. Cloud companies are a very influential subset of the tech company bubble because of their engineering prowess and reputation. As a result, AWS's move to deplatform Parler will not only influence the policies surrounding content moderation in the tech company bubble but will significantly influence how cloud service providers should moderate content on their platforms.

Tech Company Intentions & Smyth's Argument

The Parler cases study reveals that large tech companies operating public clouds, like AWS, prefer to maintain the safety of their platforms and services over allowing freedom of

speech in extreme cases, such as hate speech. It can also be argued that the tech industry at large also behaves in the same way, according to the analysis done by Gillespie. Furthermore, one could argue that AWS shut down Parler to maintain the sanctity of their brand image; no modern, progressive startup would choose a cloud service that supports hate speech. The actions taken by AWS are instances of tech industry self-regulation – the notion that a company or group of companies control ethical best practices by virtue of market and customer demands (Smyth, 2019). The spirit of self-regulation has been upheld and celebrated by entrepreneurs and engineers alike in the tech industry. However, self-regulation is only a societal good when the profit-driven compass needle is pointed in the right direction. In *The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech*, Smyth argues that large tech companies like Amazon follow the same commercial incentive structure as other for-profit ventures in our economy and, ultimately, argues that the self-regulation of the tech industry is not sustainable.

Web 1.0

Smyth begins her argument by breaking down the ethos of the early internet and Web 1.0 technologies. Silicon Valley's founding principles are rooted in "the spirit of idealism, transformation, and cooperation" (Smyth, 2019, p. 580). Silicon Valley fundamentalists were strongly associated with the hippie counterculture; they detested consolidated power structures in favor of decentralized contribution, collaboration, and freedom (Smyth, 2019). Smyth states that the "spiritual prophesies about the revolutionary potential of technologies, and the underlying manifesto they preached – which saw technology as a tool of liberation and collaboration – has been echoed by leading technology firms ever since," which is a directly observable result of the aforementioned hippie counterculture (Smyth, 2019, p. 580).

Web 1.0 was the "wild west" of information due to its ideals for openness and decentralization. Smyth says it was indeed a "marketplace of ideas"; early criticisms and calls for regulation were met with immediate backlash from the internet community (Smyth, 2019). Self-regulation was paraded as the solution to these criticisms (Smyth, 2019). For instance, if privacy is important to the end-users, then the market will select for it. However, Smyth's analysis suggests that the markets do not always act in the best interest of the users, which leads to technological innovation surpassing privacy concerns surrounding the "commodification and misuse of personal information" (Smyth, 2019, p. 582).

Consolidation & Web 2.0

Web 2.0 was dominated by the consolidation of technological ownership; companies like Amazon, Facebook, Twitter, etc. became more powerful as their userbases grew. The self-regulation ideas perpetuated by the code of the early internet had no intention to keep it free from commercial interest (Smyth, 2019). Smyth states, "the institutional forces that overcame this utopian dream came from the internet itself" (Smyth, 2019, p. 582). What ensued was a large-scale replication of the external commercial world: full of asymmetries, monopolies, and unfair hierarchies (Smyth, 2019).

The sheer scale of behemoths like Facebook brought the unintended consequence of advanced mass surveillance and data mining. The widespread adoption and acceptance of collecting user-generated data were not instantaneous, and it started as a side effect from the promises of automation and widespread connection (Smyth, 2019). Companies like Facebook justify targeted ads and data monetization by keeping services like Instagram and WhatsApp free. However, while the idea of seamless monetization makes sense to the average consumer, "they become complicit in the violation of their own confidentiality" (Smyth, 2019, p. 584).

Data Capitalism

In her paper *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, Sarah M. West defines "data capitalism" as the system in which "the commoditization of our data enables an asymmetric redistribution of power that is weighted toward the actors who have access and the capability to make sense of information" (West, 2017, p. 23). Data capitalism is the underlying principle that arises due to mass surveillance and data mining. Data capitalism promotes minimizing the cost of acquiring data while maximizing the use of aggregated data sets (Smyth, 2019). The companies that thrive can convince their users that their engagement is a social activity, not an economic activity (Smyth, 2019). In that case, it is in the best interest of big tech companies to exploit their users' data for profit. As a result, it is a trivial decision for a tech company like Facebook to increase engagement time through promoting politically provoking content and creating echo chambers of isolated content, among other unfavorable product choices.

One could argue that the intentions behind individual technical actors cannot be determined unless objective evidence arises. However, Smyth suggests that the emergent market conditions select for actors who can produce data asymmetries. The survivorship bias of technical actors is the byproduct of the data capitalism that arises from reproducing the market structure on the open internet (Smyth, 2019). The technology companies that grow at exponential rates must commonly adhere to data capitalism. In other words, evidence for userbase exploitation is unnecessary because the political system of data capitalism forces highly successful technical actors to produce products and systems that exploit personal user data. By leveraging Smyth's argument, one could see that Amazon and the tech industry's action to take down Parler is not necessarily motivated by morality but rather the political conditions installed by data capitalism.

Decentralization as a Possible Solution

The works of West and Smyth showcase that the politics of data capitalism naturally emerge from the evolution of the internet. In *Defining Web 3.0: opportunities and challenges* by Riaan Rudman and Rikus Bruwer, the goal of Web 3.0 is not to redefine how people use the internet but to distribute the storage and access of data (Riaan Rudman, 2016). Fundamentally, the consolidation of powerful actors, like Facebook, provides the asymmetrical power paradigm observed in data capitalism. Removing that asymmetry is what newer technological paradigms in Web 3.0 seek to do by decentralizing compute and authorized transactions. Decentralized computing seeks to provide users with power over their data and authorization of other users on the network.

Foundations of Cryptocurrency and Ethical Intentions

In the landmark paper *Bitcoin: A peer-to-peer electronic cash system*, Satoshi Nakamoto outlines the social motivations and technical implementation for a completely decentralized network for authorizing and maintaining payments called Bitcoin. Satoshi emphasizes that financial intermediaries "mediate disputes" and charge the end customers for mediation (Nakamoto, 2009). The main problem with mediation lies in the necessary dependence on a third party (Nakamoto, 2009).

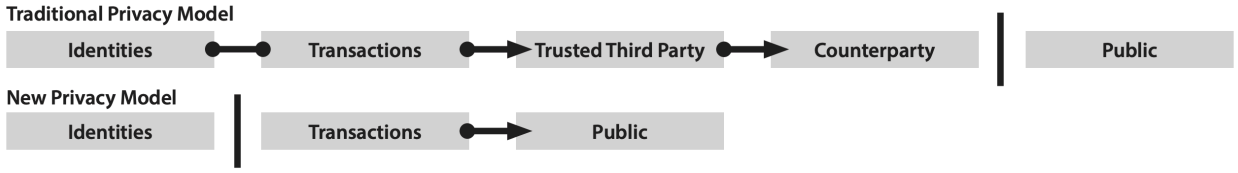

Figure 2: Bitcoin Privacy Model (Nakamoto, 2009, p. 18)

Third-party mediation "achieves a level of privacy by limiting access to information to the parties involved and the trusted third party" (Nakamoto, 2009, p. 18). To solve this issue of third-party black boxing, Bitcoin uses cryptography to anonymize identities and validate transactions.

The paradigm shift to public ledgers ensures that transactions are both public and anonymized. The public nature of Bitcoin is akin to decentralized compute; the public network evaluates every transaction (Nakamoto, 2009). In essence, Bitcoin users can have faith in their transactional validations if and only if the network of other Bitcoin users is disjoint and produce symmetrical outcomes. Consolidated institutions produce asymmetrical outcomes because the user cannot query the said institutions regarding their methods for validation, data storage, etc.

According to West, data capitalism is an extension of surveillance capitalism – a "regime that emerged from pervasive computer mediation and which produces its own social relations and with that its conceptions and uses of authority and power" (West, 2017, p. 23). As shown by Nakamoto in Figure 2, the notions of decentralized compute can remove mediation as a necessary transaction in the customer data pipeline. In this case, tech companies can no longer hold the data control asymmetries essential for surveillance capitalism because the userbase must operate peer-to-peer. On the surface, Nakamoto's approach to decentralized compute combats the asymmetries of data capitalism by virtue of eliminating intermediaries. However, it does not address the potential problems with a completely free system. A hypothetical information network built on this technology could enable bad actors to spread misinformation and hate speech with no authorized intervention.

Case Study: Mastodon & Trump's Truth

After former President Donald Trump was banned from Twitter and Facebook, he decided to build his own social media application: Truth Social. Truth is a Twitter-like app that allows users to view "truths" (similar to tweets) on a home timeline, with likes, follows, etc. (Kenneth Li, 2022). Truth was created by forking a popular open-source social network known as Mastodon. Mastodon is a decentralized social media platform that encourages community moderation over centralized moderation, community creation over tailored experiences, and

genuinely free experiences coupled with data autonomy (Mastodon, 2020). Trump chose to fork this open-source project to build a platform where he will not be accountable for the violence he generates. Trump's app originally violated the AGPLv3 license used by Mastodon's open-source code: Trump and his team failed to publish their code as open-source, violating the license (Rochko, 2021). Failure to comply with the license would have entailed severe legal action by Mastodon's team; however, Trump's team ended up complying in the months following the original legal inquiry (Rochko, 2021). Ultimately, Truth Social remains an unfettered and unregulated social media platform capable of spreading hate and violence.

Truth Social is different from Parler because it's based on a decentralized compute model. Hate speech is, in effect, tolerated and allowed to spread as a consequence; there is no AWS regulating this space. This case showcases that while decentralization is an answer to combat data capitalism at scale, it can be poor in addressing issues of hate and violence. The argument for tight regulation of social media is strong in this case because it can span centralized and decentralized systems. However, proponents of free speech would see that as a move to limit freedom of expression since social media is a medium for discourse.

Conclusion

AWS's content moderation policy showcases that self-regulation might be helpful to limit harmful voices that insight violence. However, the current market that companies like Amazon and Facebook adhere to is governed by the principles of data capitalism. While decentralized solutions might solve the inherent issue with data capitalism and mass surveillance, it is still unclear how decentralized services can regulate their networks to encourage freedom and discourage violence. Initiatives like Mastodon show that social media is changing from centralized solutions, like Twitter, to community-owned solutions, where individual moderators

determine the rules of discourse. Potential solutions could involve regulating on a case-by-case basis, wherein an online community can be scrutinized for spreading violence and hate rather than the platform itself. Ultimately, as large tech companies shift to decentralized models, solutions to limiting harmful actors will emerge as more cases become relevant.

Bibliography

AWS. (2022). *Customer Success Stories*. Retrieved from aws.amazon.com: https://aws.amazon.com/solutions/case-studies/?hp=tile&tile=customerstories&customer-references-cards.sort-by=item.additionalFields.sortDate&customer-references-cards.sort-order=desc&awsf.content-type=*all&awsf.customer-references-location=*all&awsf.custo

AWS Cloud Security Team. (2022). *Data Privacy FAQ*. Retrieved from aws.amazon.com: https://aws.amazon.com/compliance/data-privacy-faq/

Dang, S. (2021, September 5). *Amazon considers more proactive approach to determining what belongs on its cloud service*. Retrieved from Reuters: https://www.reuters.com/technology/exclusive-amazon-proactively-remove-more-content-that-violates-rules-cloud-2021-09-02/

Gillespie, T. A.-F. (2020). Expanding the debate about content moderation: Scholarly research agendas for the coming policy debates. *Internet Policy Review*, 29-41.

Johansson, E. (2021, July 20). *Amazon actually does something against Pegasus spyware.* Retrieved from Verdict: https://www.verdict.co.uk/amazon-pegasus-nso/#:~:text=Amazon%20has%20shut%20down%20cloud,journalists%20and%20human%20rights%20activists.&text=AWS%20unplugged%20its%20services%20to,wires%20on%20Monday%2C%20Vice%20reports.

Kenneth Li, J. L. (2022, Febuary 21). *Trump's Truth Social tops downloads on Apple App Store; many waitlisted*. Retrieved from Reuters: https://www.reuters.com/technology/trumps-truth-social-app-launches-apple-app-store-2022-02-21/

Mastodon. (2020). *What is Mastodon?* Retrieved from docs.joinmastodon.org: https://docs.joinmastodon.org/

Nakamoto, S. (2009). *Bitcoin: a Peer to Peer Electronic Cash System.* Retrieved from http://www.bitcoin.org/bitcoin.pdf

Page, V. (2021, August 12). *What Is Amazon Web Services and Why Is It So Successful?* Retrieved from Investopedia: https://www.investopedia.com/articles/investing/011316/what-amazon-web-services-and-why-it-so-successful.asp

Raj Bala, B. G. (2021, July 27). *Magic Quadrant for Cloud Infrastructure and Platform Services.* Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb

Riaan Rudman, R. B. (2016). Defining Web 3.0: opportunities and challenges . *The Electronic Library*, 132-154.

Rochko, E. (2021, October 29). Trump's new social media platform found using Mastodon code.

Smyth, S. M. (2019). The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech? . *International Journal of Cyber Criminology* , 578-595.

Vengattil, E. C. (2021, January 21). *Reuters*. Retrieved from reuters.com: https://www.reuters.com/business/media-telecom/what-is-parler-why-has-it-been-pulled-offline-2021-01-12/

West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 20-41.