Who Will Shape the Internet's Future: States or Individuals?

Peter MacMillan

School of Cybersecurity, Old Dominion University

CYSE 526: Cyber War

Saltuk Karahan

December 3, 2023

Abstract

The future trajectory of the Internet is a subject of paramount importance as it intertwines with the dynamic relationship between states and individuals. This paper explores the pivotal roles of both entities in shaping the digital landscape and influencing the direction of the Internet. Delving into the realms of governance, regulation, innovation, and societal impact, the research investigates the interconnected dynamics between states and individuals. As we navigate through the complexities of centralization versus decentralization, control versus freedom, and security versus privacy, this study aims to shed light on who holds the key to the Internet's future. The analysis considers potential consequences, impacts on cybersecurity, and the delicate balance required to preserve constitutional rights in the evolving digital era. By scrutinizing the roles of states and individuals, this research seeks to contribute valuable insights to the ongoing discourse on the Internet's governance and its implications for the global digital community.

The Internet, a vast and intricate network that transcends geographical boundaries, has become an integral facet of modern society, reshaping communication, commerce, and social dynamics. As the Internet continues to evolve, a fundamental question emerges: Who wields greater influence over its future trajectory—states or individuals? This inquiry delves into the heart of the ongoing discourse surrounding Internet governance, exploring the roles played by governmental entities and individual actors in shaping the digital landscape. The Internet has evolved from a decentralized, academic network to a worldwide platform that pervades every area of modern life since its birth. As the Internet's importance has increased, so has the debate about who should be in charge of its governance and development. On one end of the spectrum, states argue that regulatory control is necessary to address issues of national security, privacy, and economic interests. Individuals, on the other hand, as end consumers and content providers, advocate for the principles of freedom, creativity, and unlimited access to knowledge. Policy, regulation, and technical designs are actual manifestations of the conflict between these two perspectives, rather than merely being a theoretical concept. While individuals traverse the ever-expanding digital sphere, contributing to its growth and affecting societal narratives, governments worldwide struggle to strike a balance between encouraging innovation and limiting possible hazards. Navigating this complex terrain raises a fundamental question: States or individuals, who is more important to the development of the Internet? This research aims to explore the various facets of the state-individual dynamic in Internet governance in order to decipher this complexity. In what ways do governmental policies and activities affect the digital landscape, and in what ways do individual acts influence the course of the Internet? What are the repercussions, both planned and unexpected, of each entity's influence on issues such as cybersecurity, privacy, and constitutional rights in the digital age? Through a close examination

of these interconnected themes, this study seeks to provide insightful perspectives to the current discussion about Internet governance moving forward.

States possess significant power in establishing the contours of the Internet, thanks to their regulatory frameworks and enforcement capabilities. Internet governance includes topics like cybersecurity, data sovereignty, and online content regulation. It is frequently entwined with national interests. Some claim that a state-centric approach is required to combat malevolent actions, safeguard citizens, and preserve order in the digital domain. However, concerns have been raised regarding the possibility of state overreach, censorship, and the erosion of individual liberties in the quest of security and control. States engage in cybersecurity measures, regulate online content, and promote domestic technological advancements in order to protect national security. States are parties to international agreements and treaties pertaining to cybersecurity and data protection, which reflects their influence on the development of global frameworks for Internet governance. In a scenario in which states have complete control over the Internet, the landscape would most likely be characterized by centralized governance, stringent regulatory frameworks, and a greater emphasis on state interests. Governments would have control over the distribution of content and could reshape the digital story to suit their political objectives. Strict censorship policies could restrict free speech and thus reduce the variety of opinions and viewpoints available online. Concerns about national security would almost certainly lead to increased surveillance, with citizens' online activities being monitored. While such measures may improve cybersecurity in some ways, the concentration of power in the hands of the state may raise concerns about potential abuse, privacy violations, and the stifling of dissent. The future of a state-controlled Internet could see a trade-off between security and individual liberties, potentially affecting the digital environment's vibrant and dynamic nature. Under state

control, determining how to best shape the Internet's future would require striking a balance between the imperative of defending national interests and the need to uphold democratic values and individual liberties.

The question of whether having the state or government control the internet is a good or bad idea is subjective and depends on the specific context, the degree of control, and the values prioritized. For example, China provides an example of heavy state control, where the Great Firewall regulates and censors online content. While this has been effective in maintaining societal stability, it has also led to restricted access to information and curtailed freedom of expression. Estonia, on the other hand, exemplifies a more decentralized approach. The government focuses on digital innovation, ensuring high-speed internet access as a basic right. This has contributed to the country's advancement in e-governance and tech innovation. Here are arguments on both sides: National Security, Regulatory Oversight, and Infrastructure Development.

As far as national security goes, governments may argue that central control is necessary to safeguard national security. State intervention could help prevent cyber threats, terrorism, and the spread of harmful content. When it comes to state control over the internet, national security measures are most likely to consist of a mix of cybersecurity procedures, surveillance programs, and regulatory frameworks. To identify and stop possible threats to national security, governments can pass strict laws governing the monitoring and regulation of online activities. Monitoring communication channels, tracking online behavior, and analyzing digital data could all be part of enhanced surveillance mechanisms to detect and counteract cyber threats, terrorism, and other forms of malicious activity. Furthermore, strong cybersecurity measures would be implemented to protect sensitive data and vital infrastructure from cyberattacks. Even though the

goal of such measures is to strengthen national security, they frequently give rise to questions about how best to balance security and individual privacy, which makes the implementation of state-controlled internet policies more transparent and careful.

With the idea of regulatory oversight, state control might ensure consistent and enforceable regulations. This could lead to better management of issues such as online fraud, hate speech, and the dissemination of false information. It is likely that governments would set up frameworks to monitor and regulate different facets of online activities in a state-controlled scenario where the internet is regulated. In order to guarantee that regulatory supervision corresponds with public needs, governments could conduct periodic evaluations and discussions with relevant parties, including civil society, technology specialists, and members of the general public. A possible implementation of this adaptive strategy would be the establishment of regulatory agencies tasked with monitoring digital policies and periodically revising them in light of societal and technological developments. However, difficulties may arise when attempting to balance the need for security and order with the preservation of individual liberties. Potential obstacles include the possibility of regulatory capture, in which regulations are more influenced by special interests than by the larger public good, worries about censorship and privacy violations, and the risk of overregulation leading to stifled innovation. Striking the right balance between regulatory oversight and individual liberties becomes critical for a state-controlled internet that serves a diverse range of people's needs and aspirations.

In the realm of infrastructure development, governments could play a crucial role in funding and overseeing the development of robust internet infrastructure, ensuring widespread and equitable access to digital services. Governments would probably take the lead in organizing, carrying out, and overseeing projects to guarantee a strong and resilient digital infrastructure in

the framework of state control over the development of internet infrastructure. States may make significant investments in R&D to ensure continued relevance and adaptability to technological advancements, encouraging the adoption of cutting-edge technologies like fiber-optic broadband and 5G networks. Modern infrastructure could be installed more quickly, and knowledge-sharing could be facilitated through strategic alliances with private businesses and global partnerships. But problems like political ramifications, financial limitations, and ineffective bureaucracy might potentially obstruct development. Furthermore, privacy and security issues could surface, requiring the creation of thorough laws and guidelines to deal with these issues and guarantee the long-term growth of internet infrastructure under state control.

Arguments against governmental regulation of the internet emphasize issues with privacy, innovation, freedom, and the possibility of power abuse. The threat to freedom of expression is one of the main causes for concern, since state control may result in the repression and censorship of dissident voices, reducing the range of viewpoints and impeding democratic discourse. Another important concern is privacy, as there are worries that widespread government monitoring for national security purposes may violate people's right to privacy. Another risk associated with state-controlled internet use is that it may stifle innovation due to strict regulations and centralized decision-making, which may deter entrepreneurship and prevent the natural advancement of new technologies. Furthermore, concerns exist regarding the consolidation of power and the possibility of misuse by autocratic governments in situations where they have control over the internet. Concerns exist regarding the concentration of power and the possibility of abuse by authoritarian regimes, who could use their control over the internet as a means of repressing opposition and manipulating politics. State control over the internet might, if not handled carefully, result in a fragmented global digital space where various

nations impose differing levels of surveillance and censorship, obstructing the free flow of information across national boundaries. To avoid these pitfalls and guarantee a future internet that upholds democratic values, promotes innovation, and safeguards individual rights, it is imperative to strike a balance between the necessary regulation and the preservation of individual freedoms. When thinking about how the internet will influence the digital landscape of the future, these issues must be carefully considered. The question of whether state control of the internet is good or bad is nuanced and depends on the balance between security, regulation, and individual freedoms. Striking the right balance is crucial for fostering innovation, protecting civil liberties, and ensuring a secure and open digital environment. A collaborative approach that considers input from various stakeholders, including civil society, private entities, and the public, may be essential in crafting policies that mitigate potential risks while maximizing the benefits of state involvement.

In a scenario in which individuals have significant control over the internet, the landscape would most likely be characterized by decentralization, user-driven content creation, and a focus on democratic principles. A more individual-centric approach would emphasize user empowerment in shaping the digital environment, fostering a diverse range of platforms and services. Individuals would be able to share ideas, opinions, and information without direct interference from a central authority in this decentralized internet landscape, which would likely prioritize freedom of expression. A dynamic and competitive digital environment would result from entrepreneurs and tech innovators responding to market demands, which would foster innovation. The open structure of this kind of internet would encourage innovation, teamwork, and the democratization of knowledge. On the other hand, problems with disinformation, cyberattacks, and making sure digital platforms are used responsibly may present difficulties. In

the event that individuals control the internet in the future, there will probably be a careful balance struck between the requirements of effective regulation to maintain the integrity and security of the digital space and the principles of openness. This method reflects a more democratic and participatory vision for the internet's future by seeing it shaped by the collective decisions and actions of its users.

The idea of having individuals or society at large control the internet carries both potential benefits and risks. Here are arguments on both sides: freedom of expression, innovation and creativity, and democratic governance.

In the realm of protecting the freedom of speech, a more decentralized internet puts a premium on freedom of expression, allowing individuals to share diverse perspectives without fear of censorship. This is exemplified by the open nature of platforms like Wikipedia and open-source communities. Individual internet control, which decentralizes power and lets people voice their thoughts without worrying about censorship, can greatly support freedom of speech. Platforms could place a higher priority on transparency in an individual-centric model, allowing users to freely discuss and exchange differing points of view. Adopting strong measures to protect free speech would entail creating open policies for content moderation, where choices are made collaboratively with user input to prevent an excessive consolidation of power. Platforms that prioritize user privacy should be prioritized in order to avoid excessive surveillance that might stifle free speech. Furthermore, it's critical to support digital literacy initiatives that give users the tools they need to assess information critically and spot false information. In order to guarantee that freedom of speech continues to be a fundamental component of the online environment, an individual-centric approach necessitates a careful balance between promoting

free expression and limiting harmful content. This balance calls for thoughtful regulation and active user involvement in platform governance.

As far as innovation and creativity goes, an internet shaped by individuals fosters innovation and creativity. Examples like the open-source software movement showcase how collaborative efforts by individuals can lead to groundbreaking technological advancements. Control over one's own internet can greatly increase creativity and innovation by promoting a diverse and decentralized digital environment. Entrepreneurs, developers, and content producers can explore creative ideas in an individual-centric model without being restricted by strict rules or centralized decision-making. This strategy promotes the creation of a broad range of platforms, services, and applications to meet the various needs of users. Creating an atmosphere that encourages competition, cooperation, and open-source projects is crucial to maximizing innovation and creativity. Technological advancements can be stimulated by promoting a culture of knowledge-sharing and encouraging individual partnerships. Sensible regulation ought to prioritize safeguarding intellectual property rights without impeding the natural development of novel solutions. To keep the digital environment dynamic, open, and supportive of ongoing innovation and creativity in this scenario of personalized control, a balance needs to be struck.

Switching over to the idea of democratic governance, a user-centric internet aligns with democratic principles, where users collectively contribute to the shaping of policies and platforms. Online communities and participatory platforms, such as Reddit or platforms using blockchain technology, exemplify this approach. Because it promotes a more inclusive and participatory style of decision-making, individual internet control has the potential to improve democratic governance. Users might actively participate in the creation of guidelines, policies,

and platform rules in an individual-centric model, reflecting a democratic consensus. It is essential to implement transparent governance structures where user input is valued, and decisions are made collectively. Protection of users' rights should be given top priority in policies to make sure platforms continue to be responsible and receptive to community needs. A more democratic and user-focused approach to internet governance would include mechanisms for impartial dispute resolution, user-driven content moderation, and frequent feedback loops. It takes the implementation of transparent, easily understandable policies that advance democratic values to strike a balance between the values of inclusivity and openness while reducing potential risks.

The main issues brought up in opposition to an individualistic control over the internet are disinformation, privacy, and security. An individual-centric internet could become a digital echo chamber, where people are only exposed to information that confirms their preexisting beliefs, and disinformation could proliferate due to its open nature. As a result, there are problems for social cohesiveness since opposing ideas are being ignored more and more. Furthermore, a personal preference-driven internet might not follow standardized security procedures across all platforms, which could lead to security holes that could be exploited by cybercriminals. The absence of strict regulations and oversight exposes users to identity theft, data breaches, and other privacy violations, giving rise to privacy concerns. Furthermore, a decentralized environment increases the possibility of abuse by bad actors, such as malicious actors disseminating false information or carrying out cyberattacks. Thus, the effect of individualistic control on the development of the internet is complex. A purely individualistic approach could lead to a fragmented digital landscape, impeding efforts to combat misinformation and ensure a secure, cohesive online environment, even though user

empowerment and freedom of expression are essential. A future internet that blends freedom and security will depend on finding a balance between individual empowerment and collective governance through thoughtful legislation and digital literacy programs.

Taking a different approach to this idea, a proposition for states and society to come together and control this thing as on unit, a partnership if you will. This would need careful planning and open minds in order to make it work. Fostering a digital environment that prioritizes both security and individual freedoms requires striking a careful balance between state and individual control over the internet. Policies and regulations could be shaped by states, industry stakeholders, and users working together in collaborative governance models that may be part of the future partnership. Governments would play a role in developing a legal framework that ensures national security, protects citizens from cyber threats, and upholds the rule of law. Individuals would retain autonomy over their online activities and content creation at the same time, contributing to a vibrant and diverse digital space. It would take open and honest policies, efficient channels for user feedback, and a dedication to privacy rights protection to strike this balance. This symbiotic relationship could benefit both parties; governments would ensure a secure digital environment, while individuals would have the freedom to express themselves and shape the online world. With some adjustments, such a model could serve as a model for other countries seeking a harmonious partnership between state control and individual empowerment on the internet. This well-rounded strategy may help create a global internet environment that respects cultural diversity, protects human rights, and promotes innovation by encouraging international cooperation and the sharing of best practices.

To summarize, the debate over internet control has highlighted the importance of a nuanced and balanced approach that navigates the complexities of state authority and individual

empowerment. Future prospects and inherent difficulties for the internet are revealed by the tension between the two. It seems possible that states and people will come together to form a collaborative governance model in the future. According to this model, people contribute to a varied, creative, and open digital environment while governments provide the legal framework that protects citizen interests and national security. Because of these factors working together, it is necessary to establish open policies, strong cybersecurity defenses, and user feedback channels to guarantee inclusive and democratic decision-making. A collaboration of this kind can serve as a spark for advancement, promoting safe and lawful virtual environments while upholding democratic principles of creativity and freedom of speech. As long as issues like privacy and misuse are present, the best course of action is to take a moderate approach that avoids going too far in favor of authoritarian control or unbridled chaos. This collaboration blueprint, which is adaptable to different cultural contexts, has the potential to set a global standard for internet governance, promoting a future in which states and individuals share responsibility for cultivating a digital landscape that reflects the diverse needs, values, and aspirations of users worldwide.

Works Cited

Blitz, Matt. “What Will the Future of the Internet Look Like?” *Https://Www.Popularmechanics.Com*, 30 Sept. 2021, www.popularmechanics.com/technology/infrastructure/a29666802/future-of-the-internet/.

Edell, Jeffrey. “Who Should Control the Internet?” *Rolling Stone*, Rolling Stone, 29 Nov. 2022, www.rollingstone.com/culture-council/articles/who-should-control-internet-1234638427/.

Gjelten, Tom. “Who - If Anyone - Should Control the Internet?” *NPR*, NPR, 12 Jan. 2012, www.npr.org/2012/01/12/145125429/who-should-control-the-internet-some-say-the-u-n.

Hsieh, Ying-Ying, and Jean-Philippe Vergne. “The future of the web? the coordination and early-stage growth of decentralized platforms.” *Strategic Management Journal*, vol. 44, no. 3, 26 Aug. 2022, pp. 829–857, https://doi.org/10.1002/smj.3455.

Kim, Geun-Hyung. “How will blockchain technology affect the future of the internet?” *Advances in Computer Science and Ubiquitous Computing*, Jan. 2021, pp. 289–294, https://doi.org/10.1007/978-981-15-9343-7_40.

Maity, Pallab, et al. “The future of the internet of things (IOT) and Iot Authentication.” *2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON)*, 10 Feb. 2023, https://doi.org/10.1109/iemecon56962.2023.10092285.

Marr, Bernard. “Here’s What the Future of the Internet Will Look Like.” *Forbes*, Forbes Magazine, 12 Sept. 2023, www.forbes.com/sites/bernardmarr/2023/05/09/heres-what-the-future-of-the-internet-will-look-like/?sh=5eff0fa82f68.

McDowell, Robert. “This Is Why the Government Should Never Control the Internet.” *Https://Www.Washingtonpost.Com*, July 2014, www.washingtonpost.com/posteverything/wp/2014/07/14/this-is-why-the-government-should-never-control-the-internet/.

Murray, Alex, et al. “The promise of a decentralized internet: What is WEB3 and how can firms prepare?” *Business Horizons*, vol. 66, no. 2, 2023, pp. 191–202, https://doi.org/10.1016/j.bushor.2022.06.002.

Rejeb, Abderahman, et al. “Unleashing the power of internet of things and Blockchain: A comprehensive analysis and Future Directions.” *Internet of Things and Cyber-Physical Systems*, vol. 4, 2024, pp. 1–18, https://doi.org/10.1016/j.iotcps.2023.06.003.

Sovacool, Benjamin K., et al. “Making the internet globally sustainable: Technical and policy options for improved energy management, governance and community acceptance of Nordic Datacenters.” *Renewable and Sustainable Energy Reviews*, vol. 154, Feb. 2022, p. 111793, https://doi.org/10.1016/j.rser.2021.111793.

Watney, Murdoch. “Governmental control of the internet in addressing law enforcement and national security.” *ISSE 2008 Securing Electronic Business Processes*, 2009, pp. 108–118, https://doi.org/10.1007/978-3-8348-9283-6_11.

Yin, Hao, et al. “Big Data: Transforming the design philosophy of future internet.” *IEEE Network*, vol. 28, no. 4, July 2014, pp. 14–19, https://doi.org/10.1109/mnet.2014.6863126.