SCHOOL OF PUBLIC POLICY
CHIANG MAI UNIVERSITY

Policy Brief

Navigating Coup Dynamics in Myanmar's Digital Era: The Responsibilities of Private Companies in Managing State Digital Assets

HNIN NU NU NAING, YATANAR HTUN

Introduction

The relationship between nation-states and private technology companies has become increasingly complex in today's digital age. As governments embrace digital tools for governance and public services, they rely heavily on private companies to host and manage essential digital infrastructure and assets. From government websites to social media accounts and data repositories, core functions of the modern state now often reside on servers owned by private corporations. When a coup d'état occurs, critical questions arise regarding the control of state digital assets and the responsibilities of hosting companies in ensuring service continuity, protecting human rights and upholding democratic norms. Private technology platform companies' decisions can legitimize and delegitimize governments during power transitions, with major implications for rights, democracy and stability. Despite the gravity of these issues, there is minimal guidance on appropriate actions to undertake and navigate these intricate situations effectively. This study examines the challenges faced by private companies hosting state digital assets during coups and political upheavals by exploring the rising trend of coups worldwide and increasing state reliance on private digital infrastructure. Through analysis of technology platform's responses to recent coup, particularly the 2021 Myanmar case study, this study provides policy recommendations for companies to maintain essential services as well as to protect digital rights of the users while navigating political instability.

Core Problem

Control of Digital assets becomes particularly critical under authoritarian regimes, who often weaponize digital infrastructure to suppress opposition. These regimes employ various tactics, from internet shutdowns and content censorship to surveillance and biometric tracking of activists (Strub, 2023). The 2022 freedom house report highlights numerous cases where coups and elections have significantly impacted internet freedom, including Myanmar, Sudan, Nicaragua and Hungary (Shabaze et al.2022). Private companies hosting state-link digital assets face complex challenges in navigating political instability during coups and regime changes. These companies must make critical decisions regarding access control and preservation of digital assets while balancing competing interests of free speech promotion and government compliance requirements, particularly with "hostage" policy mandating local presence for their operation. The absence of clear guidelines leaves companies ill-equipped to handle complex ethical dilemmas surrounding legitimacy recognition, takedown demands, and account access restrictions. Their decisions carry significant implications for human rights, democratic stability, and social welfare, yet there is minimal guidance on appropriate actions and strategies for effectively managing these situations.

The role of private technology companies in political crisis

The influence of private technology companies on political and social domains traditionally controlled by governments has garnered scholarly attention. Cronin (2023) describes these entities as geopolitical actors with resources rivaling nation-states, while concepts like "digital feudalism", "neo-medievalism" and "intermediary liability" highlight their quasi-governmental roles (Jensen, 2019). Despite extensive research on topics such as technology's role in social movements (Carty & Reynoso Barron, 2019) and corporate complicity in state abuses (Hamilton, 2022), limited focus exists on the ethical challenges companies face while hosting state digital assets during coups.

Studies have criticized platforms for inconsistent moderation, particularly in non-Western countries, highlighting the need for greater investment in governance (Pírková & Fatafta, 2022). Pantti and Pohjonen (2023) argue that the Russian invasion of Ukraine marked a shift, as platforms aligned with EU policies against Russian disinformation, showcasing a new geopolitical dynamic. However, concerns about government pressure on platforms, such as in the U.S. Supreme Court case *Murthy v. Missouri*, underscore the tension between government influence and free speech (Quinn, 2024).

The Myanmar coup exemplifies these dilemmas, as social media platforms and telecom companies faced pressure to comply with the military junta's demands, raising privacy and rights concerns (Rio & Oo, 2022; Mi-Kun, 2023). Similarly, the Taliban's access to biometric systems in Afghanistan highlighted the risks of companies managing sensitive data during political instability (Human Rights Watch, 2022). This study addresses gaps by examining Myanmar as a case study to explore private companies' ethical dilemmas during coups, aiming to inform global policy on managing digital assets responsibly amid political crises.

The Evolution of Digital Infrastructure and the Role of Private Companies Before 2021 military Coup

Myanmar's digital transformation accelerated through domestic initiatives, private sector involvement, and external influences. Early reforms, like the 1999 e-government project and ICT master plans, aimed to enhance online services and modernize infrastructure but faced tight government control. The 2013 liberalization of telecommunications marked a turning point, allowing international companies like Telenor and Ooredoo to expand internet access, making digital technologies affordable. By 2021, over half the population accessed the internet, and mobile penetration reached 127% (Kemp, 2021). The democratically elected NLD government advanced digital initiatives through e-Governance master plan and smart cities projects in Yangon, Mandalay and Nay Pyi Taw (Fernando, 2019).

Private Sector involvement became integral to Myanmar's Digital Ecosystem with companies providing various services through cloud services, biometric systems and digital payment platforms. Digital payment platforms, including bank-led, telecom-led, and independent applications, became vital to Myanmar's financial infrastructure, storing citizen data and enabling transactions. Their growth was driven by government efforts to promote financial inclusion and digital payment adoption (Kyaw, 2022). Facebook emerged as a crucial platform for government-citizen communication, while YouTube gained popularity for news and entertainment. Companies managed sensitive government data, including biometric information and personal records, while facilitating digital services and transactions.

External influences, particularly China's Digital Silk Road initiative, shaped Myanmar's technological advancement. Huawei's involvement since 2013 included both infrastructure development and surveillance technologies (Chan & Rawat, 2019). Concerns arose regarding surveillance capabilities, exemplified by Huawei's intermediary role in providing in lawful interception gateway stems to Telenor (Justice for Myanmar, 2022) and Cognyte's provision of interception equipment to state-own operators (Justice for Myanmar, 2023). The 2021 military coup disrupted this progress, regressing Myanmar's digital ecosystem under authoritarian control. This transition underscores ethical dilemmas for private companies in safeguarding citizen data and rights while navigating the complexities of hosting state digital assets under repressive regimes.

The role of Role Private companies in Post-Coup

Following the 2021 military coup, Myanmar's Digital landscape transformed dramatically as the junta exploited pre-existing digital infrastructure for surveillance and repression. Technologies such as traffic cameras and facial recognition CCTVs, originally intended to enhance public safety, were repurposed to track and target dissidents (Amnesty International, 2022; Mathieson 2023). Local businesses were coerced into installing surveillance equipment under threat of license revocation (Ni, 2023). The junta has also leveraged extensive telecommunication infrastructure developed by private companies to surveil citizens, resulting in arrests and violence. It also forced telecom firms to impose internet and mobile network shutdowns, disrupting connectivity and silencing dissent.

Digital Platforms, however, became tools of resistance. Activists and elected lawmakers conducted utilized platforms like Zoom to organize, while platforms like X (formerly Twitter) amplified global awareness through the hashtag like #WhatIsHappeningInMyanmar (Phattharathanasut, 2024). Facebook remained the primary platform for organizing protests and documenting human rights abuses, though it also became a battleground for military propaganda (Rio, 2023). YouTube was used for fundraising and activism but similarly faced issues with disinformation. Telegram, valued for its privacy features and anonymity, emerged as a key platform for secure communication and coordination. However, its weak moderation also allowed pro-military groups to spread propaganda and intimidation.

Despite military suppression, digital tools empowered civil society. Citizen journalists and activists documented abuses, while interim education and healthcare initiatives thrived online amidst widespread disruptions. However, the junta's intensified digital crackdown resulted in severe deterioration of internet freedoms, with Myanmar scoring just 12/100 on Freedom House's 2022 index and being among the countries with the most internet shutdowns as reported by Access Now and #keepitOn Coalition (Rosson et al., 2023). The previous NLD government faced post-coup criticism for lacking transparency in deploying dual-use technologies. Telecom companies, in particular, were scrutinized for complying with military demands or exiting the country. These technologies have become tools for both military control and citizen resistance, shaping Myanmar's fight for democracy.

Myanmar Military's Digital Repression Strategy During Coup

Since the military coup on February 1, 2021, Myanmar military junta has employed a multi-faceted digital repression strategy to consolidate power, suppress dissent, and maintain control over the flow of information. Leveraging technological, legal, and coercive measures, it targets opposition movements and civil society. Their key tactics encompass systematic internet shutdowns, forced exit of foreign telecom operators, enhanced surveillance systems, and strict financial monitoring. The junta has also weaponized legal mechanisms through amended penal codes and proposed cyber laws, while conducting extensive censorship and information operation campaigns. These coordinated efforts have resulted in widespread arrests, digital rights violations, and the creation of a pervasive climate of fear, effectively undermining opposition movements and civil society resistance.

Analysis and Discussion of Responses by Companies

The following case studies examine how various companies, both domestic and international, responded highlighting key lessons for corporate responsibility in political crises.

Norwegian telecom Telenor entered Myanmar in 2014, prioritizing transparency and human rights. It publicized government internet shutdown directives during the Rohingya crisis, earning trust from activists, journalists and human rights defenders. However, after the 2021 military coup, Telenor faced pressure to comply with military directives. Concerns over employee safety led to reduced transparency, followed by orders to activate intercept equipment, which were in violation of EU sanctions. Subsequently, the company decided to sell its operations to the M1 Group, in partnership with Shwe Byine Phyu Group, a company with military ties. This decision was not driven by financial or strategic objectives but was guided by the company's commitment to its values and standards, as well as the absence of a legal framework to safeguard customer rights. The case has raised significant concerns about potential user data misuse. Civil society organizations criticized Telenor for insufficient human rights safeguards, emphasizing the risks of user data falling into military hands. Following the Telenor Exit case, Qatari telecommunication Ooredoo also exited Myanmar, selling its operation to Nine Communication Pte.Ltd. Civil society raised similar concerns about data privacy and human rights implications, criticizing Ooredoo’s lack of transparency and engagement with stakeholders during the sale.

Meta, Facebook’s parent company, took unprecedented action against Myanmar’s military following the 2021 coup, introducing the Tatmadaw Ban Policy to restrict military-controlled assets on its platforms. The policy expanded restrictions based on their 2018 actions against military actors during the Rohingya genocide. Meta also implemented measures to combat misinformation, protect users, and prevent violence, setting a precedent for corporate responses to illegitimate state actions. Alphabet Inc., Google and YouTube's parent company, faced criticism for its reactive and inconsistent approach to Myanmar's military coup (Potkin, 2020). Unlike Facebook's targeted measures, Alphabet relied on global guidelines, removing military-linked channels, apps, and accounts only after public pressure. Civil society groups emphasized the need for proactive, country-specific strategies to address misinformation, propaganda, and the military's use of tech platforms for psychological warfare. Telegram became a battleground where military supporters conducted doxxing campaigns and harassment, particularly targeting female activists, while the platform's response remained limited (Frontier, 2022; Myanmar Witness, 2023). Apple faced criticism for hosting military-affiliated apps and restricting VPN updates.

Local financial service providers, particularly banks like KBZ, struggled between military pressure and protecting customers. They were required to comply with Central Bank directives for account monitoring and suspension, often resulting in customers losing access to their accounts or facing arrest for suspected resistance support. This period highlighted the complex balance between corporate responsibility and operating under an authoritarian regime.

The Myanmar case study and the analysis of private companies’ response to the military coup reveal a complex web of tensions and trade-offs that technology companies must navigate when hosting state digital assets during times of political upheavals. Location significantly influenced the company's responses. Local companies, constrained by physical presence and potential retaliation, focused on service continuity and employee safety, Local companies, constrained by their physical presence and potential repercussions like arrests or nationalization, prioritized maintaining essential services and protecting employees, even if it meant enabling digital repression. In contrast, international companies, with more operational flexibility, focused on balancing user security, privacy, and freedom of expression while addressing offline harms. However, the lack of proactive, context-specific strategies hindered their ability to effectively manage these challenges.

Facebook's response to the Myanmar coup illustrates the potential benefits of learning from past crises. After facing criticism during the Rohingya genocide, Facebook adopted a proactive stance during the coup, implementing the Tatmadaw Ban Policy, restricting military-controlled entities, and collaborating with civil society to better understand local dynamics. This stands in contrast to the more reactive approaches of other companies, particularly Alphabet's largely passive response, underscoring the importance of meaningful consultation and engagement with stakeholders to develop effective strategies.

While international guidelines like the UN Guiding Principles on Business and Human Rights provided theoretical frameworks, practical implementation often fell short. Companies frequently responded to criticism rather than proactively developing comprehensive strategies. The experience highlighted the need for context-specific approaches and stronger engagement with local stakeholders. The most successful responses came from companies that prioritized the consent of the governed and maintained active dialogue with civil society organizations. These experiences underscore the importance of developing proactive strategies for managing state digital assets during political crises, while recognizing the practical constraints faced by companies operating in unstable political environments.

Recommendations

Based on the analysis of private company's actions during the Myanmar coup and theoretical frameworks on legitimacy in governance, stakeholder and corporate social responsibility, and ethical decision-making, this section presents recommendations to help companies anticipate, prevent and mitigate risks in managing state digital assets and political instability.

For Companies operating inside the Country:

1. **Conduct thorough risk assessments and human rights impact assessments for the local context.** Companies should perform thorough risk and human rights impact assessments, engaging local stakeholders to understand challenges. Prioritize safeguarding individual rights and safety over corporate risks or reputational concerns.
2. **Keep safety of employees and prioritize the protection of user data and privacy.** Companies must prioritize employee safety through secure communication channels, emergency support, and relocation assistance when needed. Additionally, companies must implement strong data protection measures to safeguard user day and privacy, resist illegitimate data demands, and review government requests for compliance with international human rights standards.
3. **Maintain transparency and open communication with relevant stakeholders.** Companies must maintain transparency and open dialogue with stakeholders, including activists, civil society groups, and international communities. They should regularly disclose policies, government demands, and responses while engaging in continuous consultation to enhance their practices.
4. **Advocate the protection of human rights.** Companies should leverage their influence to protect human rights, collaborate with others to resist military regime unethical demands, and support local civil society through technical assistance and knowledge sharing. Joint initiatives between tech companies, like coordinated implementation of policies restricting military access, can amplify impact and effectiveness in coup situations.

5. **When deciding to withdraw from the market as the last resort, establish a responsible disengagement plan.** When Withdrawal becomes necessary, companies must develop a responsible disengagement plan prioritizing user data protection, employee safety, and essential service continuity. Consult stakeholders, minimize data left behind, and mitigate impacts on users and society.

For Companies operating outside the Country:

1. **Take a clear stance against the military coup and its associated human rights abuses.** Companies should condemn the military coup through clear statements backed by concrete actions like refusing services to military-controlled entities and supporting independent media and civil society organizations.
2. **Conduct enhanced due diligence on state-linked assets and partnerships.** Companies must rigorously assess state-linked digital assets and partnerships in Myanmar, investigating affiliations and setting criteria to restrict ties with entities violating human rights. Collaboration with organizations tracking military connections can aid this process.
3. **Prioritize the protection of user rights (Freedom of expression, safety and security) by siding with citizens.** Companies must safeguard users' freedom of expression, safety, and security by implementing context-specific moderation policies and providing privacy tools like encryption, two factor authentication and profile locking. Prioritize citizens' needs while preventing military exploitation of platforms and resources.
4. **Collaborate with local and international stakeholders to develop policies and guidelines.** Companies must actively and continuously engage and collaborate with local and international stakeholders, including civil society organizations, human rights groups, and industry peers to develop context-specific policies tailored to Myanmar’s unique need through multi-stakeholder dialogues and collective action initiatives.
5. **Develop clear policies for responding to illegitimate regime changes.** Companies should develop clear policies to assess regime legitimacy and manage state-linked digital assets under illegitimate control. These policies should align with international human rights standards and be communicated transparently to relevant stakeholders
6. **Consider avoiding /minimizing physical presence in markets with complicated political histories.** Companies without physical presence requirements should reconsider entering politically unstable markets like Myanmar to avoid dealing with authoritarian regimes, safeguarding employee safety and reducing compliance risks with oppressive demands. Operating remotely, as social media platforms often do, can minimize risks to employees and avoid direct confrontation with such regimes.

Conclusion

The findings and insights from the Myanmar case study have broader implications for other contexts of political instability and unconstitutional regime changes. As the world continues to grapple with the challenges posed by coups and political turmoil, the lessons learned from Myanmar serve as a valuable guide for private companies operating in similar situations. By applying these lessons globally, particularly in volatile contexts, businesses can help build a stable and rights-respecting digital ecosystem. As private companies continue to play an increasingly influential role in the digital age, it is crucial that they recognize their responsibilities and take proactive steps to align their actions with the interests of the people they serve. By doing so, they can help to foster a more just and equitable digital future, even in the face of political instability and uncertainty.

References

- Amnesty International. (2022, April 22). *Myanmar: International community must do more to protect brave protesters*. Amnesty International. https://www.amnesty.org/en/latest/news/2022/04/myanmar-coup-peaceful-protest/
- Carty, V., & Reynoso Barron, F. G. (2019). *Social movements and new technology: The dynamics of cyber activism in the digital age*. In H. B. Demetriou, C. Papadakis, & G. Tsobanoglou (Eds.), *The Palgrave handbook of social movements, revolution, and social transformation* (pp. 373-397). Palgrave Macmillan.
- Chan, J. H., & Rawat, D. (2019, April 29). *China's digital silk road: The integration of Myanmar – RSIS*. RSIS Commentary. https://www.rsis.edu.sg/rsis-publication/rsis/chinas-digital-silk-road-the-integration-of-myanmar/
- Cronin, A. K. (2023, August 21). *How private tech companies are reshaping great power competition*. Johns Hopkins SAIS. https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition
- Fernando, F. (2019, September 23). *Smart city in Myanmar: Opportunities and challenges*. LinkedIn. https://www.linkedin.com/pulse/smart-city-myanmar-opportunities-challenges-felix-fernando
- Frontier. (2022, June 2). *Pro-military death squad rallies openly on social media*. Frontier Myanmar (blog). https://www.frontiermyanmar.net/en/pro-military-death-squad-rallies-openly-on-social-media/
- Hamilton, R. J. (2022). *Platform-enabled crimes: Pluralizing accountability when social media companies enable perpetrators to commit atrocities*. *Boston College Law Review, 63*(1349).
- Human Rights Watch. (2022, March 30). *New evidence that biometric data systems imperil Afghans*. Human Rights Watch. https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans
- Jensen, J. L. (2019). *The return of medieval society – control, surveillance and neo-feudalism in the age of the internet*. *AoIR Selected Papers of Internet Research 2019 (October)*. https://doi.org/10.5210/spir.v2019i0.10986
- Justice for Myanmar. (2022, March 2). *Telenor Group violating sanctions through installation and imminent transfer of German lawful intercept gateway*. Justice for Myanmar. https://www.justiceformyanmar.org/press-releases/telenor-group-violating-sanctions-through-installation-and-imminent-transfer-of-german-lawful-intercept-gateway
- Justice for Myanmar. (2023, January 15). *Israeli surveillance firm Cognyte's business in Myanmar exposed*. Justice for Myanmar. https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed

- Kemp, S. (2021, February 12). *Digital in Myanmar: All the statistics you need in 2021*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-myanmar
- Kyaw, E. N. (2022, June 3). *The revolution of Myanmar fintech: Mobile payment applications*. MYANMORE (blog). https://www.myanmore.com/2022/06/the-future-of-myanmars-fintech/
- Mathieson, D. S. (2023, August 3). *The age of urban insurgency in Myanmar?* Myanmar Now. https://myanmar-now.org/en/news/the-age-of-urban-insurgency-in-myanmar/
- Mi-Kun. (2023, July 31). *In post-coup Myanmar, telco operators act as the military's eyes and ears*. EngageMedia (blog). https://engagemedia.org/2023/myanmar-telecommunications/
- Myanmar Witness. (2023, January 25). *Digital battlegrounds*. Myanmar Witness. https://www.myanmarwitness.org/reports/digital-battlegrounds
- Ni, N. M. (2023, September 2). *Junta pressures Mandalay street vendors to install surveillance cameras*. Myanmar Now. https://myanmar-now.org/en/news/junta-pressures-mandalay-street-vendors-to-install-surveillance-cameras/
- Pantti, M., & Pohjonen, M. (2023). *Social media platforms responding to the invasion of Ukraine*. In *Media and the War in Ukraine* (pp. 57-75). Peter Lang.
- Phattharathanasut, T. (2024). *#WhatsHappeningInMyanmar: The evolution of the digital fight against authoritarian state repression*. *International Journal of Communication, 18*(0), 21.
- Pírková, E., & Fatafta, M. (2022, November 29). *Content governance declaration in times of crisis: How platforms can protect human rights*. Access Now (blog). https://www.accessnow.org/publication/new-content-governance-in-crises-declaration/
- Quinn, M. (2024, March 17). *Supreme Court to hear free speech case over government pressure on social media sites to remove content*. CBS News. https://www.cbsnews.com/news/supreme-court-social-media-sites-government-content-misinformation-censorship/
- Rio, V. (2022, November 16). *The battle for control over Myanmar's digital state apparatus*. Myanmar Internet. https://www.myanmarinternet.info/post/blog_002
- Rio, V. (2023, January 24). *Facebook's Tatmadaw ban policy*. Myanmar Internet. https://www.myanmarinternet.info/post/blog_004
- Rosson, Z., Anthonio, F., Cheng, S., Tackett, C., & Skok. (2023, February 28). *Internet shutdowns in 2022: The #KeepItOn report*. Access Now (blog). https://www.accessnow.org/internet-shutdowns-2022/
- Shahbaz, A., Funk, A., Vesteinsson, K., Friedrich, P., Baker, G., Grothe, C., Masinsin, M., Vepa, M., & Weal, T. (2022). *Countering the authoritarian overhaul of the Internet*. *Freedom on the Net 2022*. Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet
- Strub, D. (2023, April 8). *Confronting the rise of digital authoritarianism*. *NBR Congressional Briefing Series*. The National Bureau of Asian Research. https://www.nbr.org/publication/confronting-the-rise-of-digital-authoritarianism/