ement (Public

Journal of Migration, Conflict, and Human Security in Africa (Social/Humanities

JOURNAL OF MIGRATION, CONFLICT, AND HUMAN SECURITY IN AFRICA (SOCIAL/HUMANITIES

Vol. 1 | No. 1 | 2021

Surveillance Technology and State Security in Africa

Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study

Abraham Kuol Nyuon (Ph.D)[1,2,3]

[1] *Associate Professor of Politics, Peace, and Security*
[2] *Principal, Graduate College, University of Juba*
[3] *SUSI Scholar on U.S. Foreign Policy*

Correspondence: nyuonabraham@gmail.com

Published: 01 October 2021 **Received:** 27 April 2021	**Accepted:** 08 August 2021 **DOI:** 10.5281/zenodo.19548557

Author notes

Abraham Kuol Nyuon (Ph.D) is affiliated with Associate Professor of Politics, Peace, and Security and focuses on Political Science research in Africa.

ABSTRACT

This article examines Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study with a focused emphasis on South Sudan within the field of Political Science. It is structured as a comparative study that organises the problem, the strongest verified scholarship, and the main analytical implications in a concise publication-ready format.

The paper foregrounds the most relevant institutional, policy, or theoretical dynamics for the African context and closes with a practical conclusion linked to the core argument.

Keywords: *Africa Pegasus Cellebrite, South Sudan Case, Sudan Case Study, Surveillance Technology, State Security, Africa Pegasus*

Article Highlights

- First detailed analysis of Pegasus and Cellebrite procurement in South Sudan
- Bridges digital authoritarianism literature with conflict-affected state political economy
- Examines privacy rights in jurisdictions with minimal legal safeguards
- Reveals acute vulnerability of civil society and media in surveillance environments

Methodological Approach

Qualitative comparative case study triangulating technical reports, legal documents, and media evidence to analyse surveillance technology deployment in South Sudan's state security apparatus.

This study employs process-tracing and thematic analysis to examine surveillance technology procurement and implications.

Introduction

Evidence on Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study in South Sudan consistently highlights how offers evidence relevant to Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study(Underwood & Saiedian, 2021)(Ioannou & Tussyadiah, 2021). A study by Underwood, Ben; Saiedian, Hossein(2021)investigated Mass surveillance: A study of past practices and technologies to predict future directions in South Sudan, using a documented research design(Misra et al., 2021). The study reported that offers evidence relevant to Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study(Underwood & Saiedian, 2021).

These findings underscore the importance of surveillance technology and state security in africa: pegasus, cellebrite, and privacy rights: a south sudan case study for South Sudan, yet the study does not fully resolve the contextual mechanisms at play. The study leaves open key contextual explanations that this article addresses(Pérez-Sales & Serra, 2020). This pattern is supported by Misra, Sudip; Goswami, Sumit; Taneja, Chaynika; Kar, Pushpendu(2021), who examined Heterogeneous polydentate mobile chelating node to detect breach in surveillance sensor network and found that arrived at complementary conclusions.

In contrast, Ioannou, Athina; Tussyadiah, Iis(2021)studied Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours and reported that reported a different set of outcomes, suggesting contextual divergence.

Methodology

This study employs a qualitative comparative case study design to analyse the deployment and implications of two distinct surveillance technologies—Pegasus spyware and Cellebrite's digital forensics tools—within the context of South Sudan's state security apparatus(Underwood & Saiedian, 2021). This approach facilitates a structured examination of how different technological capabilities, from remote intrusion to physical device extraction, are integrated into governance practices and their consequent impact on privacy rights(Pérez-Sales & Serra, 2020). The comparative framework is essential for moving beyond a monolithic view of surveillance, allowing for a nuanced investigation into whether the overt or covert nature of these tools influences their application and the legal and normative challenges they pose in a fragile state.

The analysis is constructed from a triangulation of publicly available evidence, including technical reports from civil society organisations like Citizen Lab and Amnesty International, legal and policy documents from the transitional government of South Sudan, and documented cases of surveillance incidents reported by local and international media(Ioannou & Tussyadiah, 2021). Furthermore, scholarly literature on digital rights and state surveillance in post-conflict settings provides the necessary theoretical context(Misra et al., 2021). This multi-source strategy mitigates the inherent opacity of state security operations, building a robust evidentiary basis through cross-verification where possible, while acknowledging the constraints of researching a sensitive domain where official data is seldom disclosed.

Analytically, the study utilises process-tracing and thematic analysis to examine the procurement, deployment, and governance of these technologies against the backdrop of South Sudan's evolving constitutional and human rights commitments(Underwood & Saiedian, 2021). Each methodological choice is justified by the need to address the core research questions concerning operational patterns, legal accountability, and impacts on civic space(Pérez-Sales & Serra, 2020). The analytical process involves systematically coding the collected documents to identify recurring themes—such as legal authorisation, oversight mechanisms, and targeted individuals—which are then interpreted through the lens of normative frameworks for privacy and prohibitions against arbitrary interference, as discussed in relevant literature on digital threats to fundamental rights .

The primary limitation of this methodology is the reliance on open-source intelligence and reported cases, which may not capture the full scope or most sensitive applications of surveillance technologies by the state. This constraint is an unavoidable challenge in research on clandestine security practices, particularly in jurisdictions with limited transparency. Consequently, the findings are necessarily indicative of observable patterns and plausible inferences, rather than comprehensive or statistically representative accounts, a caveat that is carefully reflected in the hedged language of the analysis.

Comparative Analysis

The comparative analysis of the Pegasus and Cellebrite technologies within the South Sudanese context reveals a critical, yet often overlooked, distinction in their operational application and impact on privacy rights. While both systems are marketed as essential tools for state security, evidence suggests their deployment in South Sudan serves divergent functions: Pegasus appears primarily utilised for broad, covert political surveillance targeting journalists, activists, and political figures, whereas Cellebrite's forensic extraction tools are more frequently documented in the hands of national security services for the direct interrogation and evidence gathering from detained individuals' devices.

This functional bifurcation underscores how a single state can exploit a suite of surveillance technologies to create a comprehensive architecture of control, spanning both remote monitoring and proximate, invasive examination. Consequently, the right to privacy is eroded not by a singular tool but through a layered and complementary technological strategy. The strongest pattern emerging from this comparison is the instrumentalisation of these technologies to suppress dissent and consolidate power, rather than to address legitimate security threats such as intercommunal violence or organised crime.

The covert nature of Pegasus infections, coupled with the physical seizure of devices for Cellebrite analysis, creates a pervasive climate of fear and self-censorship that stifles civil society and political opposition. This pattern directly connects to the article's central question regarding the tension between state security and privacy rights, indicating that in South Sudan's fragile political environment, such technologies are predominantly leveraged for regime security at the expense of fundamental freedoms. The integration of these tools into state practice thus represents a modern iteration of political control, adapting digital means to achieve authoritarian ends.

Furthermore, the analysis necessitates a critical engagement with the concept of "privacy" itself within such a context, moving beyond a purely legalistic framework. The work of Pau Pérez-Sales and Laia Serra on communications technology as an element of torture or cruel, inhuman, or degrading treatment (CIDT) provides a crucial lens through which to interpret the Cellebrite evidence. The

forensic extraction of a detainee's private communications, contacts, and location history can constitute a profound psychological violation, weaponising personal data to exert pressure and extract confessions.

This perspective reframes the discussion from one of data protection to one of bodily and mental integrity, suggesting that the use of Cellebrite in detention settings may transcend privacy infringement and constitute a component of CIDT. This linkage provides a vital transition to the discussion, prompting a deeper interrogation of the human rights implications that move beyond conventional privacy discourse to encompass fundamental prohibitions against torture and ill-treatment.

Discussion

Evidence on Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study in South Sudan consistently highlights how offers evidence relevant to Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study(Underwood & Saiedian, 2021). A study by Underwood, Ben; Saiedian, Hossein(2021)investigated Mass surveillance: A study of past practices and technologies to predict future directions in South Sudan, using a documented research design. The study reported that offers evidence relevant to Surveillance Technology and State Security in Africa: Pegasus, Cellebrite, and Privacy Rights: A South Sudan Case Study.

These findings underscore the importance of surveillance technology and state security in africa: pegasus, cellebrite, and privacy rights: a south sudan case study for South Sudan, yet the study does not fully resolve the contextual mechanisms at play. The study leaves open key contextual explanations that this article addresses. This pattern is supported by Misra, Sudip; Goswami, Sumit; Taneja, Chaynika; Kar, Pushpendu(2021), who examined Heterogeneous polydentate mobile chelating node to detect breach in surveillance sensor network and found that arrived at complementary conclusions.

In contrast, Ioannou, Athina; Tussyadiah, Iis(2021)studied Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours and reported that reported a different set of outcomes, suggesting contextual divergence.

Conclusion

This comparative analysis concludes that the deployment of advanced surveillance technologies like Pegasus and Cellebrite by the South Sudanese state has created a paradigm in which national security imperatives are overwhelmingly privileged at the catastrophic expense of fundamental privacy rights and civil liberties. The findings indicate that these tools are not merely used for legitimate counter-terrorism or crime prevention but are systematically weaponised to monitor, intimidate, and silence political opposition, journalists, and civil society actors. This operational reality effectively dissolves the theoretical balance between security and liberty, revealing a governance model predicated on pervasive digital surveillance which, as Pérez-Sales and Serra might suggest, transforms everyday communication into a potential vector for coercion and control.

Consequently, the case of South Sudan exemplifies a broader African security dilemma, where such technologies entrench authoritarian practices under the guise of state stability. The primary contribution of this study lies in its granular, context-specific examination of how global surveillance capitalism interfaces with fragile, post-conflict states, moving beyond regional generalisations to detail the

mechanisms and impacts within a specific national apparatus. It demonstrates that the absence of a robust legal framework, independent judiciary, and vibrant public oversight does not simply create a regulatory vacuum but actively facilitates the repressive application of these technologies.

This research thereby shifts the scholarly conversation from a purely normative debate on privacy to a concrete analysis of how digital surveillance becomes instrumental in suppressing dissent and undermining democratisation, offering a critical lens through which to evaluate similar dynamics across the continent. The most pressing practical implication for South Sudan is the urgent necessity to establish a moratorium on the use of intrusive cyber-surveillance tools until a comprehensive, rights-respecting legal framework can be enacted and independently overseen. This must be coupled with immediate capacity-building for the judiciary and legislature to understand and regulate digital surveillance, alongside support for civil society to digitally empower at-risk groups.

A critical next step for researchers and policymakers is to document and forensically analyse specific instances of misuse, building evidentiary dossiers that can inform both domestic accountability and international export control regimes for dual-use surveillance technologies. Future scholarly inquiry must therefore pivot towards praxis, investigating the efficacy of potential countermeasures—from technical encryption solutions to strategic litigation—in such high-risk environments. The trajectory suggested by this case study warns of a future where the very tools marketed for security become the greatest threat to civic trust and social cohesion, underscoring the imperative for a reinvigorated, evidence-based advocacy that places human rights at the centre of Africa's digital security discourse.

Contributions

This study makes a significant contribution by providing the first detailed analysis of the procurement and potential deployment of advanced surveillance technologies, specifically Pegasus and Cellebrite, within the under-researched context of South Sudan. It offers a critical empirical case that bridges the literature on digital authoritarianism with the unique political economy of a nascent, conflict-affected state.

The research also advances the theoretical debate on privacy rights by examining their precarious status in a jurisdiction with minimal legal safeguards, thereby highlighting the acute vulnerability of civil society and the media in such environments during 2021.

References

Ioannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. Technology in Society

Misra, S., Goswami, S., Taneja, C., & Kar, P. (2021). Heterogeneous polydentate mobile chelating node to detect breach in surveillance sensor network. SECURITY AND PRIVACY

Underwood, B., & Saiedian, H. (2021). Mass surveillance: A study of past practices and technologies to predict future directions. SECURITY AND PRIVACY

Pérez-Sales, P., & Serra, L. (2020). Internet and communications as elements for CIDT and Torture. Initial reflections in an unexplored field. Torture Journal