Digital Colonialism; How U.S.' Big Tech interfere in the Colonization of Palestinians

Paijens, Anne

Digital Colonialism; How U.S.' Big Tech interfere in the Colonization of Palestinians

Bachelor Thesis

Anne Paijens

s3534162

Universiteit Leiden

BSc Political Science: International Relations and Organizations

Supervisor: Dr. Esra Elif Nartok-van der Kist

Submission date: 19-12-2025

Embargo Statement: Public

Wordcount: 7515

Table of contents

Introduction

The Conflict between Palestine and Israel long predates the event of October 7th. However, the scale of deaths and human rights violations witnessed since then is unprecedented in comparison to earlier phases of the conflict. Equally unprecedented is the level of mass surveillance imposed on Palestinians, an escalation enabled by the rapid development of technologies such as big data analytics and artificial intelligence. These technologies have made constant, granular monitoring of an entire population technologically and economically feasible. U.S. Big Tech companies play a central role in this process: they supply digital infrastructure, analytics tools, and data-processing capacities to the Israeli state. Simultaneously, companies such as Meta have been documented to systematically censor Palestinian content online (Human Rights Watch, 21 December 2023). These dynamics raise pressing questions about the role of U.S. Big Tech within the broader system of settler colonialism in Palestine and the ongoing violence inflicted on Palestinians. In the pursuit of profit, these firms materially support and enhance practices of mass surveillance and control.

Since approximately 2019, these has been a surge of academic interest in what is variously termed digital colonialism. techno colonialism, algorithmic colonization, data colonialism and more (Nothias, 2025, p.2). Scholars across diverse disciplines, including international relations (Wright, 2021), law (D'CunhaC, 2021; Mann & Daly, 2019), ICT/development (Young, 2019), sociology (Kwet, 2019), and anthropology (Mouton & Burns, 2021) have adopted these frameworks to interrogate how digital infrastructures reproduce colonial hierarchies of power. For example, in South Africa, private companies increasingly deploy CCTV networks to train AI analytics systems. These systems rely on, and reinforce, long-standing infrastructures of racialised surveillance shaped by apartheid. Across the Global South more broadly, data extraction frequently occurs without meaningful consent, in contexts where legal protections are weak or absent. As Hao and Swart (2022) argue, this extraction. combined with AI systems trained on racialised datasets and designed by Western corporate actors, risks reproducing historical patterns of domination, exploitation, and dispossession. As Nothias (2025) observes, "the perception of Big Tech as an evident force for good has been shattered" (p. 2).

Despite the rapid expansion of this literature, in-depth case studies remain limited (Hao and Swart 2022; Mann, 2019; Peron & Evangelista, 2024; Young, 2019) and none examine

digital colonialism within an active system of settler colonialism and militarised mass surveillance. This thesis seeks to fill that gap by analysing how U.S. Big Tech's digital-colonial practices interact with, the ongoing genocide and colonisation of Palestinians. The following research question is thus;

How does digital-colonialism by US Big Tech interfere in the colonization of Palestinians?

The thesis is structured as follows; Firstly, literature review will describe debates surrounding the political economy of digital infrastructures, drawing on and critically engaging both International Political Economy (IPE) and postcolonial scholarship. The theoretical framework seeks to bridge these fields by applying Haag's (2020) PPE framework, before elaborating the conceptualisation of digital colonialism used in this study. The methodology chapter explains how the concept is operationalised. The analysis examines how U.S. technology companies extract and monetise data from users and publics at large, with particular attention to how these dynamics disproportionately affect marginalised communities in the Global South. The case study of Palestine provides an empirical contextualisation of digital colonialism within a unique and understudied context of settler colonialism and state surveillance. Ultimately, the thesis aims to advance both PPE scholarship and the conceptual development of digital colonialism. In examining Palestine through the lens of digital colonialism, this thesis invites a reconsideration of the political economies underpinning our digital infrastructure, challenging Western narratives of technological neutrality and instead highlighting the forms of domination they obscure.

Literature review

The internet originated as a United States military research project, the decision of the U.S. National Science Foundation (NSF) in the 1990's to privatize its backbone infrastructure enabled commercial internet service providers to interconnect seamlessly with the rapidly expanding network (Naughton, 2016, p.8,9). The internet's shift from a publicly funded research project to a privatized commercialized infrastructure, reflected the ascendancy of neoliberal economic governance. Clinton administration's deregulatory agenda institutionalized a market driven model of digital infrastructure and governance (Radu, 2019, p.84). Perhaps paradoxically so, as it was the exact publicly available hardware and software that had created the communication system's rapid wide diffusion (Schiller, 1999 p. 11). The US' favourable legal environment gave way to the growth of Silicon Valley as the epicentre of digital innovation and U.S. Computer companies and telecommunication carriers allied themselves with transnational enterprises to promote neoliberal approaches to digital infrastructure globally as demands on the infrastructure increased. (Schiller, 1999, p.1). Similarly, liberal IPE scholars advocated a market-led approach to digital infrastructure, arguing that global governance should only be used to facilitate internet development while providing as much freedom as possible for firms and civil society, particularly in terms of freedom of expression (Flonk et al., 2020, p.366, 368).

Within this liberal paradigm, Cowhey (1990, p.169) characterised the multilateral telecommunications regime at the time as a "lucrative international cartel", that defied conventional economic logic. While monopolistic arrangements were long considered 'natural'. economically optimal and even political attractive, in traditional telecommunications, rapid technological innovation rendered such monopolises increasingly unjustifiable (Ibid, pp.183, 184). The emergence of ICT blurred the lines between communication and data processing, transforming these systems into foundational infrastructures for global markets and undermining the rationale for monopolistic control (Ibid, pp.173,187). Cowhey & Klimenko (2005, p.60, 66) further document of telecommunications firms faced major limits in foreign markets, prompting industrialised countries to instrumentalise institutions such as the WTO, IMF and WB to promote market liberation. The authors describe the WTO's 1997 reference paper as a pivotal shift towards pro-competitive regulatory principles and a fundamental transformation of the regime (Ibid, pp.61, 62). Although this libertarian model dominated in the 90's, it was increasingly contested following the collapse of the dot-com bubble, as other states

began to challenge the U.S.-centric internet governance (Flonk et al., 2020, p.367 .369). Nevertheless, liberal approaches persist, warning that politicization of digital infrastructure risks undermining the internet's openness and universality (Kaya & Shahid, 2025, p.220). U.S. policymakers frequently frame regulations of data flows as a threat to economic growth and technological innovation (Brännström et al. 2023, p.2259).

As early as the 70's countries of the Third world critiqued the liberal model and identified the asymmetrical North-South flow of data, databanks and processing capacity as a threat to domestic information and technology services. As Brännström et al (2023, pp.2259-2261) demonstrate, U.S. efforts to secure unrestricted cross-border data flows were underpinned by distinct 'legal imaginaries' that framed free data flows as a human rights issue linked to the freedom of information and as a free-trade imperative. In response, countries of the Global South actively sought to denaturalise U.S. conception of informational freedom by highlighting the entanglement with commercial expansion and American economic power. Additionally, they increasingly called for institutional governance that is not dominated by Western states and firms (Flonk et al, 2020, p.366, 367).

These tensions crystallised in contemporary debates between liberal and sovereigntist approaches to digital governance. While liberal frameworks favour private, multistakeholder governance and expansive freedom of speech, sovereigntist advocate for greater state control and intergovernmental regulation (Flonk et al., 2020, pp.365–367). The concept of digital sovereignty describes the desire to exert control over one's own digital infrastructure and data governance (Kaya & Sahid, 2025, p.220). Importantly, digital sovereignty is not exercised exclusively by nation-states: corporations, communities, and supranational actors such as the European Union also exert significant influence over digital governance arrangements (Jiang, 2023, p.728). Big Tech firms, in particular, wield quasi-legislative, executive, and judicial power through platform architectures and terms of service (Belli & Jiang, 2024). Nonetheless, the past decade has witnessed an intensified trend towards the nationalisation of digital governance (Jiang, 2024, p.728).

China has long been pursuing digital self-sufficiency and now owns a digital ecosystem rivalling that of Silicon Valley's, yet its autonomous digital ecosystem raises concerns regarding censorship and state (Jiang, 2024, p.727). Flonk et al (2020) describe the sovereigntist approaches as associated with authoritarian regimes such as China and Russia, yet this association obscures the diversity of sovereigntist projects. Calls for digital sovereignty also

emerge from democratic states in the Global South and from the European Union, drawing on postcolonial traditions and human rights frameworks respectively (Jiang 2024, p.727).

Postcolonial perspectives on digital governance resonate with historical struggles for independence from colonial metropoles, and several Global South democracies have adopted state-led approaches to developing digital public infrastructure (Ibid,, p.728). Additionally, indigenous communities, such as those in Australia and Aotearoa New Zealand, have articulated claims to digital sovereignty rooted in data governance and self-determination (Kukutai & Taylor, 2016). An important critique by Fischer (2022, p.383) cautions that although digital sovereignty appears promising, dominant actors may instrumentalise digital sovereignty discourses in ways that reinforce imbalanced power relations within the Global South, particularly when models such as China's fail to disrupt underlying structures of dependency.

Despite decades of debate, connectivity remains prohibitively expensive, unreliable, or inaccessible for large parts of the world (Nothias, 2020, p.329). Early attempts to address this "digital divide" led to the normative field of Information and Communication Technologies for Development (ICT4D), which frames digital technologies as tools for addressing poverty and underdevelopment by expanding access to information and services (Heeks, 2008, pp.26,29). Like U.S. free-flow doctrines, ICT4D often conceptualises internet access as a human right. Postcolonial scholars, however, have criticised this framework for reproducing dependency on Western technologies and for deploying a developmentalist vocabulary that closely parallels colonial narratives of progress and modernisation (Kensicki, 2019, p.8).

These critiques extend to corporate-led connectivity initiatives. In 2013, Mark Zuckerberg published a white paper framing internet connectivity as a human right, shortly before Facebook launched Free Basics, a programme offering limited access to selected websites at no cost. By framing infrastructure provision as a moral imperative, Facebook positioned itself as a humanitarian actor (Nothias, 2020, pp.331–332). However, significant corporate investment in promoting such initiatives raised concerns that these projects functioned less as philanthropic interventions than as strategies to capture first-time internet users and dominate emerging markets (Nothias, 2020, p.344). Civil society opposition, particularly in India, highlighted the that free infrastructures provided by transnational corporations would be devastating for local services and start-ups. Additionally, critical infrastructure would be controlled by transnational corporations, leading India to ban Free

Basics and adopt a more sovereigntist, state-led approach to digital development (Jiang, 2024, p.728).

As Jiang (2024, p.728) observes, a central driver of the turn towards digital sovereignty is growing awareness of Silicon Valley's extractive surveillance practices and their neo-colonial implications. Foreign investments in digital infrastructure increasingly function as tools of surveillance, often targeting marginalised populations as experimental sites for data extraction under philanthropic narratives (Latenero & Kift, 2018, p.2; Madianou, 2019). These dynamics remain understudied, as much research on digital platforms prioritises issues such as misinformation and political polarisation rather than the structural conditions shaping digital experiences in the Global South (Nothias, 2020, p.344).

Critical data studies further underscore that the data that is extracted is not an objective capturing of events or conditions. Data descriptions become possible only through the abstraction of life which comprises a variety of richness and complexity. Their meaning can be controlled and manipulated, through this subversion, power relations become visible. (Constantiou & Kallinikos, 2015, pp.50, 54). Similarly Tuzcu (2021, p.514) argues that AI produces information that looks neutral but is artificial in nature. The use of AI is an inaccessible field of computing and knowledge production, this epistemic shift further deepens the geopolitical hierarchies between the Global North and South, rendering their voices unheard. Young (2019, p. 1428) contextualises the ways in which digital technologies privilege certain knowledge system over others. Digital participation is often assumes to be beneficial in instrumental ways, providing economic advances and access to better services and governance. This puts the focus on squarely technocratic questions to access (Ibid, p.1425). However, knowledge politics shape the types of political and economic engagement that is possible digitally, these forms of engagement are largely compatible with the needs and desires of populations in the Global North. Digital engagement and their subtle epistemic biases may actually erase Indigenous knowledges and replace them with Western logics and political goals (Ibid, p.1426). Young (2019) conceptualises this process as digital colonialism, highlighting parallels with colonial educational systems that disrupted local epistemologies.

Definitions of digital colonialism vary, some approaches remain largely metaphorical, describing the digital realm as a new found territory awaiting exploration and exploitation, like colonial territories of the past. Critics argue that such accounts risk obscuring the material and political-economic mechanisms through which digital extraction operates, as data must be actively constructed to acquire economic value (Mouton & Burns, 2021, p.1892; Couldry &

Mejias, 2019, pp.336–339). Postcolonial authors such as Young (2019), Tawil-Souri & Aouragh(2014) and Tuzcu (2021) accurately critique AI and digital infrastructures for developing knowledge production structures that seem neutral yet reinforce structural disparities within the digital space. However, arguments that do not include legal or economic frameworks of historical colonialism weaken the direct link to colonialism. As Couldry and Mejias (2019, 338-9) argue, accounts of digital appropriation must demonstrate how contemporary digital infrastructures function as modern equivalents of colonial mechanisms of control.

Given that the scholarship of digital colonialism has been so recent, much of which emerged after 2019 (Nothias, 2025, p.2), there remains a limited number of empirically grounded studies that examine how digital colonialism operates in specific political and historical contexts (Young, 2019, p.1427). To my knowledge, no academic study has yet examined digital colonialism by U.S. Big Tech in the Palestinian context. While earlier work by Tawil-Souri and Aouragh (2014) addresses the political significance of online spaces for Palestinian resistance, it conceptualizes the internet primarily as a communication system rather than a material infrastructure and does not speak of its material consequences. Similarly, Kensicki's (2019) work on "smart colonialism" and digital divestment focuses on ICT in urban planning and development norms but does not analyse the role of U.S. Big Tech corporations. Existing reports, such as those by 7amleh (2024) and Apoorva PG (2023), provide valuable empirical insights but do not offer a sustained academic conceptualization of digital colonialism.

This thesis therefore seeks to fill a significant gap by providing a theoretically grounded case study of digital colonialism in Palestine. It does so by adopting the Postcolonial Political Economy (PPE) framework advanced by Haag (2020), which integrates postcolonial theory with International Political Economy. By situating digital colonialism within the case of Palestine, this research provides a unique empirical lens through which to analyse how digital domination interacts with, and actively enables, territorial colonisation, thereby extending existing debates on digital colonialism and marginalisation beyond metaphorical and into concrete political-economic realities.

Theory

To address the Research Question - How does digital colonialism by US Big Tech interfere in the colonization of Palestinians? - the thesis adopts the Postcolonial Political Economy (PPE) framework. PPE is grounded in post-structuralist epistemology, which holds that the material world does not exist as a self-evident, objective reality but is instead interpreted and rendered meaningful through discourse (Haag, 2020, p.21). From this perspective, political-economic systems are historically and culturally constituted, rather than universal or neutral. PPE explicitly challenges homogenizing and essentialist assumptions by stating that social, economic and technological practises are embedded within and reproduce unequal global hierarchies. In doing so, this perspective overcomes the material/ideational dichotomy between the two strands of Political Economy and Postcolonial theory.

Central to PPE is a postcolonial conceptualization of power which is understood as not only fluid and intractable but also inherent in specific institutional and historical mechanisms that structure economic relations, technological development, and knowledge production. PPE insists that interrogating the global economy requires more than identifying material inequalities, it also necessitates dismantling the Eurocentric epistemologies that present Western economic norms, such as privatization and proprietary digital systems, as universally valid and politically neutral (Franzki & Aikins, 2010, p.12). As Haag (2020, p.20) argues, PPE enables an analysis of the co-constitution of postcolonial relations and economic practises; postcolonial logics shape political–economic arrangements, while economic simultaneously reproduce and naturalize global inequalities. This approach provides a methodological toolkit for analysing discourse, representation, institutional practices, and material infrastructures as interconnected dimensions of a single global system historically rooted in colonial violence. As such, PPE is particularly well suited to examining power relations within the global digital economy and, for the purposes of this thesis, the relationship between U.S. Big Tech and populations in the Global South.

Recent scholarship have increasingly turned to the concept of digital colonialism as it offers strong explanatory power because it foregrounds the economic, political and epistemic hierarchies embedded in global digital infrastructures. As Couldry and Mejias (2019, p.337) argue, an analysis of Big Data's impact on the Global South first requires recognising contemporary capitalism's growing dependence on new forms of appropriation. Zuboff (2015,

p.75) identifies this reliance as a new phase of "surveillance capitalism," in which corporations seek to predict and modify human behaviour in order to generate profit and market control. Data-driven logistics have expanded across nearly all domains of human activity, incorporating large-scale data processing into areas of work and social life that were previously governed very differently (Couldry & Mejias, 2019, p.341).

Under this system, no form of human activity is too trivial for extraction: all forms of interaction are abstracted, datafied, analysed, and commodified (Zuboff, 2015, p.79). US technology corporations such as Google and Facebook were among the first to adopt this "logic of data accumulation," using platforms, apps, smart devices, and even Street View cars as mechanisms for continuous data harvesting. Couldry & Mejias (2019, p.341) emphasize that his extractive practise is a rationale that had to be normalized to function effectively, requiring data extraction to appear natural, inevitable, or socially beneficial. Personal data are framed as a pre-existing natural resources, simply "there" to be taken. This mirrors the colonial logics that treated newly encountered lands and natural resources as ownerless thus available for extraction without legal interference. However, as Couldry & Meijas (2019, pp.337, 344) argue, such practices invade the very space of the self, undermining human autonomy by enabling surveillance and behavioural manipulation without meaningful consent and within legally ambiguous environments as corporations expand the ways in which humans can exploit each other. These dynamics become especially consequential in contexts marked by intensified surveillance and political repression.

Digital colonialism represents the global consolidation of this logic, as technological infrastructures, data flows, and platform economies reinforce pre-existing economic and geopolitical hierarchies (Yilmaz, 2025, p.322). Yet it is distinctively a new contemporary colonial pattern as it combines colonial domination with the abstract quantification practices of computing (Couldry & Mejias, 2019, p.337). In this context, technology corporations emerge as the new colonial actors (Coleman, 2019, pp.420–425) and unlike classical colonialism it does not require direct territorial conquest. Instead, it operates through control over digital infrastructures, software ecosystems, and algorithmic governance. These corporations, predominantly headquartered in the Global North and especially in the United States, exercise disproportionate authority over these domains, enabling extraction from users in the Global South without redistribution and reinforcing structural dependencies that constrain the development of autonomous digital economies (Yilmaz, 2025, p.322). Couldry & Meijas (2019, p.345) note, that the consequences of this data extraction are profoundly unequal and become

particularly visible in the relationship between Big Tech and in marginalized populations in the Global South.

Kwet (2019, p.4) characterises U.S. Big Tech as an imperial force across the Global South, embedding itself strategically across all layers of the digital ecosystem, software, hardware, and network infrastructures, and thereby concentrating economic and political power in the hands of a small number of U.S.-based firms. In the South African context, this domination has been facilitated by state actors, NGO's, business elites and intellectuals aiming to catch up with the Global North, often by uncritically adopting U.S.-centric models of digital society such as Bit Data analytics, AI, machine learning, centralised Cloud services and more (Ibid, 5). U.S. Corporations reinforce this domination through the proprietary licencing regimes that restrict public access to, and understanding of, underlying source codes. As a result, decisions about data extraction, algorithmic design, and ethical priorities are shaped by a narrow demographic of predominantly white, male engineers in Silicon Valley and imposed globally. In South Africa, these dynamics are particularly evident in sectors such as private security and policing, where predictive analytics and surveillance technologies are layered onto infrastructures historically shaped by apartheid-era racialized control (Hao & Swart, 2022 April 19). This role has intensified as contemporary Big Tech companies now supply advanced products and services to foreign intelligence and security agencies (Kwet, 2019, pp.15–16).

Many accounts continue to frame digital colonialism in terms of Global North-Global South relationships at large (Yilmaz, 2025; Couldry & Mejias, 2019; Nothias, 2025). However, the case of South Africa demonstrates that digital colonialism manifest in highly context-specific ways. Wright's (2019, p.90) analysis of Chinese digital colonialism, for instance, highlights the unique dynamics produced by a state-led economy and authoritarian regime.

This thesis seeks to contributing to the literature through an in-depth case study of Palestine, a context in which digital domination intersects directly with *ongoing* territorial colonization. By examining how U.S. Big Tech infrastructures and data practices operate in collaboration with Israeli state agencies and surveillance systems, this research demonstrates how digital colonialism not only mirrors but actively enables colonial domination and genocidal violence against Palestinians. In doing so, the thesis advances the digital colonialism literature by grounding its analysis in a concrete empirical case, while demonstrating the analytical strength of a PPE framework for understanding the entanglement of digital power, political economy, and colonial domination.

Methodology

This research will analyse how US Big Tech interferes in the colonization of Palestine by the through a qualitative single-case study design. A qualitative approach is particularly appropriate given the study's focus on meanings, power relations and socio-technical processes rather than on quantifiable measurable outcomes. The aim is to develop an in-depth, theoretically informed understanding of how digital infrastructures operate as instruments of colonial domination. Methodologically, the study employs document analysis, drawing on academic literature, NGO and international organization reports, investigative journalism, and leaked corporate materials.

Document analysis enables an in-depth, contextual interpretation of texts by situating them within their historical, cultural, and political conditions of production. Rather than treating documents as neutral sources of information, this approach examines how texts articulate particular worldviews, legitimize power relations, and reproduce dominant ideologies. It is therefore especially well suited to the study of digital infrastructures, not as purely technical artefacts, but as socio-technical systems embedded in political economy and shaped by colonial and geopolitical logics.

The United States is selected as the primary locus of analysis due to its historically entrenched dominance in the global digital economy. Since the early development of the internet as a U.S. public good, information technology investment has remained disproportionately concentrated in the United States throughout the 1980s and 1990s (Schiller, 2019, p.16). This early infrastructural and financial advantage enabled U.S.-based corporations to shape global digital markets and promote a liberal model of internet governance, supported by a state apparatus that actively advanced liberalization and privatization on a global scale. The consolidation of U.S. digital dominance was not linear. Speculative investment and venture capital culminated in the dot-com crash of 2001, leaving extensive telecommunications infrastructures underutilized and unattractive to traditional investors. These conditions created opportunities for a new generation of platform-based corporations, such as Google, Facebook, and Amazon, to repurpose existing network infrastructures for data-driven business models (Naughton, 2016, pp.15, 17). The specific historical, political, legal, and economic configuration of the United States thus provided the foundation for the contemporary dominance of U.S. Big Tech, a dominance that persists today. As Kwet (2019, p.5) argues, these

corporations operate as an imperial force by exporting algorithmic designs, governance models, and ethical priorities developed by engineers and executives in Silicon Valley to contexts across the globe. Their disproportionate structural power therefore necessitates focused and contextualized analysis.

The Case of Palestine has been chosen as it represents one of the most enduring and well-documented examples of territorial occupation in the modern era. This context offers a unique window to the ways in which digital colonization interacts with its territorial form. It also allows for the extension of insights from contexts like South Africa, particularly regarding how digital infrastructures operate within systems of apartheid and racialized control(Hao & Swart, 2022 April 19). The temporal scope of the study will focus on the period from October 7th to 2025**,** a period marked by both the rise of global debates on digital colonialism and the increasing visibility of U.S. corporate involvement in Israeli state surveillance and security infrastructures. This time frame captures the convergence of global debates on digital colonialism with the intensification of digital surveillance practices in Palestine. A short-term, focused temporal scope allows for the detailed analysis of evolving technological deployments, corporate-state partnerships, and their implications for Palestinian life under occupation.

Digital colonialism is operationalised along three analytically connected dimensions: infrastructural integration, extractive surveillance, and its consequential marginalisation. The analysis first established some historical context to the colonization of Palestine and the racialised surveillance infrastructures put in place by Israel. The analysis examines how U.S. Big Tech companies are embedded within Israeli surveillance and security architecture. This includes the provision of cloud services, AI systems, data analytics tools, and platform infrastructures used by Israeli state institutions and military or intelligence agencies. Document analysis will trace formal contracts, partnerships, leaked materials, corporate statements, and investigative reporting to establish how U.S. firms are structurally embedded within Israel's surveillance ecosystem. This step operationalises digital colonialism as control over digital infrastructures, rather than territorial governance. Second, the study operationalises extractive surveillance by analysing how these infrastructures enable large-scale, non-consensual data extraction from Palestinians. Showing how Palestinians are positioned as data subjects without rights, consent, or reciprocal benefit, while extracted data contributes to corporate profit, technological refinement, and market dominance. Moreover, the analysis focuses on the consequential marginalisation of this digital extraction for the Palestinian population by demonstrating how algorithmic systems, data-driven targeting, and AI-assisted decision-

making actively support Israel's settler-colonial project by facilitating population management, repression, and lethal force.

All sources are evaluated critically in terms of authorship, purpose, and potential bias to assess credibility and relevance. Academic sources provide theoretical and analytical grounding for understanding data extraction, platform capitalism, and digital dominance. Reports from international organizations, such as Human Rights Watch (2023), United Nations Human Rights (2025), and the Arab Centre for the Advancement of Social Media (2024), offer detailed documentation of surveillance practices and human rights violations. Investigative journalism further illuminates corporate–state relationships, particularly in contexts where official information is withheld. Notably, leaked Google documents from 2021, as reported by Biddle (2022), provide evidence of contractual and infrastructural ties between Google and Israeli state institutions, forming a critical empirical basis for the analysis.

This brings me to the limitations of this study. Limitations to the study are mostly due to the highly private character of the data, especially that of Israeli Intelligence, making me reliant on second hand sources. Another limitation is that many of the (leaked) sources are in Hebrew, a language I am not familiar with, and thus for those I will also be reliant on second hand translated data, like that of Biddle (2022, 24 July). Finally, the ongoing nature of Israel's military violence against Palestinians means that additional information may emerge after the completion of this study. Despite these limitations, the volume and consistency of existing documentation produced by NGOs, journalists, and scholars provide a sufficient empirical basis for a first academic analysis of this case.

Analysis

Following the 1947 UNGA resolution proposing the partition of Palestine, Zionist militia carried out systematic attacks on Palestinian villages, resulting in the mass displacement of over half of the Palestinian population during the Nakba. Today, Palestinians continue to be dispossessed and displaced by illegal settlements and home demolitions (UN, 'About the Nakba'). As the UN Human Rights Council (2023, March 25, p.3) argues, such practices are inherent to settler-colonialism, where the mere existence of Indigenous people is framed as an existential threat to the settler society, as such the Palestinian existence is incompatible with the formation and preservation of a Jewish state, leading to Israel continuously designating Palestinians as security threats to legitimize its military occupation and violence (UNHRC, 2023, August 28, p. 20).

This ethnic cleansing continued when Israel occupied the West Bank, East Jerusalem and Gaza, transforming Palestinian territories into what the UNHRC describes as open-air prisons in which entire populations experience a multifaceted system of physical barriers, bureaucratic control and digital surveillance (UNHRC, August 28, 2023, pp. 4,17). Since October 7, this system has intensified dramatically, with both the International Court of Justice (24 may, 2024) and the UN Human Rights Council (march 25 2024) identifying credible evidence of genocidal practises. Palestinian digital rights organisation 7amleh (2024, pp.4-5) argue that the intersection of digital rights and genocide is often overlooked and that the role of Big Tech in this genocide has remained largely absent from mainstream human rights analysis.

The collaboration between U.S. Big Tech companies and the Israeli military must be situated within a broader political-economic trajectory in which major technology firms increasingly operate alongside state security agencies. As discussed earlier, Big Tech corporations extract, store, and process vast quantities of data, enabling the collection and monetization of highly sensitive personal information, including political affiliations, social networks, and behavioural patterns (Kwet, 2019, p. 13). Zuboff (2015, pp. 79, 81) conceptualizes this system as *surveillance capitalism*, in which corporations extract behavioural data to predict and modify human behaviour for profit. Social media platforms constitute only one vector of this data extraction. As Couldry and Mejias (2019, p. 341) note, data flows also originate from an expanding network of sensors embedded in smart devices, private and public surveillance cameras, smartphones, drones, and satellites.

Over recent years, Big Tech firms have sought to expand the commercialization of this data beyond advertising markets. Companies have developed extensive facial biometric databases derived from social networks and search engines, which are then used to enhance facial recognition systems for commercial and security purposes (Devlin, 2019, October 5). Meta has emerged as a central actor in generative AI development, while Google has positioned itself increasingly as a machine-learning company rather than merely a search engine provider (Amnesty International, 2025, August 29; Hoijtink & Panqué-van Hardeveld, 2022, pp. 6,7). Since 2017, Google has collaborated with the U.S. Department of Defence through Project Maven, supplying machine-learning tools designed to extract "objects of interest" from military surveillance footage (Hoijtink & Panqué-van Hardeveld, 2022, pp.2,3). Through its TensorFlow platform, Google provided pre-labelled datasets and machine-learning models capable of image recognition, pattern detection, language processing, sentiment analysis, and facial recognition.

These technologies raise significant concerns when deployed in security and military contexts. Facial recognition systems rely on massive biometric databases and operate through cross reference matching. While Facial recognition works well on clear images, their accuracy is often greatly reduced when applied to low-quality or grainy surveillance footage (Devlin, 2019, October 5). Feldstein (2019, p. 16) argues that such databases, search engines, and knowledge systems constitute the backbone of AI-enabled surveillance infrastructures that facilitate a wide range of digital repression tools. Bellanova et al. (2021, p. 121) further link the expansion of these technologies to the growing normalization of digital surveillance over civilian populations in armed conflict. Hoijtink and Panqué-van Hardeveld (2022, p. 4) therefore describe Project Maven as a decisive moment in the broader "platformization" of the military, referring to the deepening integration of civilian digital platforms into military operations. Similar developments can be observed across the industry: Amazon has provided cloud-based computing and AI video-analysis services for security agencies in the United States and South Africa, while Microsoft has developed AI-powered surveillance tools for law enforcement in the United States and South America (Peron & Evangelista, 2024, p. 539).

This bring us to the case study of Palestine. Artificial intelligence and mass data collection are a central feature in Israel's ongoing military aggression and system of control (7amlhe, 2015, p.19). Microsoft, Google and Amazon, have used the war for expanding their involvement as Israel has increasingly relied on U.S. commercial AI models and cloud services (Abraham, 2024, August 4; Biesecker et al., 2025, February 18). In 2021, Israel signed a joint

contract with Google and Amazon called Project Nimbus, which transferred government and military information systems to public cloud servers and granted access to advances AI services (Biddle, 2022, July 24). Since October 7, the procurement of these services has increased significantly (Abraham & Davies, 2025, January 23). Israeli military usage of Microsoft and OpenAI reportedly spiked in March 2024 to levels 200 times higher than prior to October 7 (Biesecker et al., 2025, February 18).

Google, Microsoft Azure, and Amazon Web Services now compete to serve as the Israeli military's primary cloud and AI provider. Israel is considered a "strategic customer," whose adoption of these technologies influences security agencies globally (Abraham, 4 August 2024). Since October 7, Amazon has also signed cloud and AI contracts with Australian intelligence agencies (Cherney, 3 July 2024). Israeli military officials have emphasized that cloud services, particularly those provided by Amazon, offer virtually unlimited storage capacity and rapid scalability, which would have been difficult to construct independently. These companies supply what Israeli officials describe as "the most advanced services" available for the Gaza war (Abraham, 4 August 2024).

An investigation by +972 Magazine and Local Call (Abraham, 2024, August 4) obtained recordings from a 2024 Israeli military computing conference "IT for IDF", in which Colonel Racheli Dembinsky publicly confirmed that the Israeli army would be using Cloud storage and artificial intelligence services from private tech companies civilian tech giants in the Gaza stip. In the video the logo of Amazon Web services (AWS), Google cloud and Microsoft appear (Col. Racheli Dembinsky speaking at a conference titled "IT for IDF", 2024, July 10). The Guardian further reported in January 2025 that Microsoft's provision of cloud technology and AI systems to Israel had deepened significantly since October 7 (Davies & Abraham, 23 January 2025). The companies provide advanced AI capabilities, including speech-to-text systems, image recognition, and machine-learning tools accessible through their cloud platforms, enabling facial recognition, automated image categorization, object tracking, and sentiment analysis (Abraham, 2024, August 4). One concrete application of these services is Google Photos. Israeli soldiers stationed in Gaza and at checkpoints reportedly use cameras linked to the application to photograph Palestinians, whose faces are then uploaded into centralized databases. The application is also used to process surveillance camera footage and drone imagery. Israeli officers have stated that Google's facial recognition capabilities outperform alternative systems (Frenkel, 27 March 2024).

Despite this, Big Tech companies consistently frame themselves as neutral intermediaries providing infrastructure rather than exercising agency over its use (Hoijtink & Panqué-van Hardeveld, 2022, p. 6). Google, Microsoft and Amazon all state that they are commited to responsible uses of AI systems, with Google explicitly states that their design or deploy AI technologies that are likely to cause Harm (Amazon AWS, 'Responsible AI'; Google, 'Our AI Principles'; Microsoft, 'Principles and Approach'). However, Digital rights organizations argue that these corporations supply tools, data, and infrastructure that directly enable technologies facilitating systematic human rights abuses (7amleh, 2024, p. 19). These firms exercise structural power: they shape what forms of surveillance and violence are technologically feasible, economically viable, and politically normalized (Bellanova et al., 2021, p. 121). which is continuous surveillance, predictive targeting, and automated violence of Palestinians. Investigation showed that Amazon and Google certainly anticipated there would be legal challenges over their technology being used in Gaza. Leaked Project Nimbus contracts reveal that Google and Amazon explicitly anticipated legal challenges related to Gaza and prohibited restrictions on Israeli use of their technologies, even in cases of human rights violations. The contracts further oblige the companies to notify Israel if foreign courts demand access to the data (Abraham & Davies, 29 October 2025).

According to the UN Human Rights Council, such circumstances trigger obligations of due diligence and human rights impact assessments (UNHRC, 26 June 2025). The right to privacy and data protection are protected under article 17 of the ICCPR (UNHR, 1966). The violation of these digital rights can impact other rights such as the right to liberty and security and freedoms of assembly and associations (7amleh, 2024, p.7). Amnesty International similarly argues that these data practices are incompatible with the right to privacy and pose disproportionate risks to marginalized populations (Amnesty International, 29 August 2025). Public scrutiny has resulted in limited corporate responses. In May 2025, Microsoft claimed an internal review found no evidence that its products were used to target individuals and that it complied with human rights guidelines (Microsoft, 15 August 2025). However, investigations by *The Guardian* and *+972* revealed that Unit 8200 stored top-secret intelligence material on Microsoft Azure servers located in the Netherlands, with plans to migrate up to 70 percent of its data to Azure. These systems enabled the storage of millions of phone calls and their transcription and translation using AI tools (Biesecker et al., 18 February 2025). Microsoft subsequently acknowledged violations of its terms of service and disabled certain services to the Israeli Ministry of Defence (Berger, 8 October 2025). Israel then shifted parts of its cloud

infrastructure to Amazon (Frenkel, 25 September 2025). Microsoft has proven that Big Tech does have the ability to limit state operated surveillance practises (Berger, October 8 2025).

The analysis thus far demonstrates how U.S. Big Tech companies are structurally embedded within Israeli surveillance and security architectures. The dominance of U.S. software on Palestinian territory is imposed without Palestinian consent and enforced through military occupation. This constitutes an extreme manifestation of digital imperialism. These infrastructures enable non-consensual data extraction, with Palestinian data contributing to corporate profit, technological refinement, and market dominance. The analysis now turns to the concrete consequences of this infrastructural embedding for the Palestinian population. As Kwet, 2019, p.16) states in his case study of South Africa, infrastructures of historical racialised systems of surveillance, AI analytics and racial recognition reproduce the hierarchies and control mechanisms of classical colonial rule and further marginalise these communities.

Israel uses AI-powered target-generating systems named ‘Lavender’, ‘Habsora’ and ‘Where’s daddy?’, these systems process enormous amounts of information collected through the system of mass surveillance in the Gaza strip. They then generate automatic ‘target’ recommendations of people and their private residencies suspected of being Hamas or Islamic Jihad operatives. Israel then carriers out large scale assassinations on these targets. The system ‘Where’s daddy?’ tracks targeted individuals family residences to kill them once they arrived home. An individuals likely hood of being target is numbered between 0 and 100 based on features such as a person’s family relation, social media connections, frequent address and phone number changes and recorded phone calls (Abraham, 2024, April 3; Bielsecker et al, February 18 2025).

Prior to October 7, target approval involved extensive human review, with a team of 20 people to review a single airstrike a day (Bielsecker et al, February 18, 2025. Airstrikes were limited and primarily to high-ranking Hamas operatives and then had to be carefully approved by senior military commander. Senior Israeli intelligence officials continue to state that even when AI is being used, there are still several layers of human oversight and only lawful military targets are targeted (Biesecker et al, February 18 2025). However, since October 7, safe guards have been largely dismantled and hundreds of strikes are now approved weekly (Ibid). Additionally al Hamas operatives are now considered legitimate targets for an airstrike. Officers have no additional requirements to examine the raw intelligence data on which the decision was made, except for checking whether the target is a man (Abraham, 3 April 2024). Intelligence officers describe an emphasis on “quantity over quality,” with limited

time for verification, resulting in the bombing of homes and the killing of entire families (Abraham, 30 November 2023). Israel has relied heavily on *Lavender*, which reportedly generated up to 37,000 suspected militants (Abraham, 3 April 2024). Israel has relied almost completely on the system Lavender that has generated as many as 37000 Palestinians as suspected militants (Abraham, 3 April 2024).

According to the IDF, the use of AI tools improves the accuracy and efficiency of the intelligence material (Biesecker et al. February 18 2025; IDF, 2 November 2023). However, insiders report significant flaws. Training datasets reportedly classified civil defence workers as Hamas operatives, and the system is estimated to produce errors in approximately 10 percent of cases (Abraham, 3 April, 2024). The system has misidentified high school students at potential militants (Biesecker et al, February 18, 2025). It would sometimes flag people whom have identical names to an Hamas operative or use devices that once belonged to an operative. Translation errors from Arabic to Hebrew have further contributed to wrongful targeting. Officers have admitted to striking homes with no confirmed militant presence, resulting in the deaths of entire families (Abraham, 30 November 2023). Even when the target might be accurate, there is a significant gaps between when an officer is alerted that a target arrived home, and the bombing itself, which can result in a family being killed without the target inside (Abraham, 3April 2024). This large scale infliction of indiscriminate assassination is part of Israels genocidal behaviour and settler colonialism against the Palestinians. These surveillance and assassination technologies are actively facilitated by US Big Tech as they provide the digital infrastructure and services to surveilled and target Palestinians.

To answer the research question; *How does digital-colonialism by US Big Tech interfere in the colonization of Palestinians?* U.S.-owned corporate digital infrastructures in occupied Palestinian territory does not merely reproduce historically racialized systems of surveillance and control mechanisms of Israeli settler colonialism. It constitutes a form of colonial domination it itself; Digital colonialism. The domination of digital infrastructures constitutes an asymmetrical power relations between the Global North and South as U.S. Big Tech exercises power over Palestinians through pervasive, non-consensual data extraction in the name of company profit and market dominance. Their innovative technologies shape the ways in which surveillance and violence become technologically feasible. The data of Palestinians are extracted under a system occupation, their consequential deaths are not incidental but foreseeable outcomes of these virtual violations of autonomy and sovereignty. From a Postcolonial Political Economy perspective, this case illustrates the co-constitution of political

and economic power, in which corporate profit depends on colonial violence, and military domination relies on corporate owned technologies and digital infrastructures.

Conclusion

This thesis set out to examine how digital colonialism by U.S. Big Tech companies interferes in the ongoing colonization of Palestinians. By mobilising a Postcolonial Political Economy (PPE) framework and grounding the analysis in an in-depth case study of Palestine, the research has demonstrated that digital infrastructures can be used as politically and economically embedded instruments of domination. The findings show that U.S.-based technology corporations are structurally integrated into Israel's surveillance and military architecture, providing cloud infrastructure, artificial intelligence systems, and data-processing capabilities that enable mass surveillance, population management, and lethal targeting of Palestinians. These practices do not merely reproduce historical forms of colonial surveillance but constitute a form of digital colonialism. Through non-consensual data extraction, proprietary control over digital infrastructures, and the creation of technological dependency, U.S. Big Tech companies exercise asymmetrical power over a colonized population while deriving commercial profit and technological advantage. Palestinian data is extracted under conditions of occupation and fed back into surveillance and targeting systems, from a PPE perspective, this case illustrates how political domination enables corporate profit, while corporate infrastructures actively reinforce settler-colonial control.

This thesis contributes to the literature by offerring an academic analyses of digital colonialism operating within an ongoing settler-colonial and genocidal context. Conceptually, it moves beyond metaphorical uses of digital colonialism by showing how digital infrastructures function as concrete mechanisms of surveillance, control, and dispossession. Still, several limitations should be acknowledged. The analysis relies primarily on secondary sources due to the secrecy surrounding military and intelligence operations, and on translated materials for Hebrew-language sources. Moreover, as the violence in Gaza is ongoing, further evidence may emerge beyond the temporal scope of this study. Nevertheless, the convergence of investigative journalism, NGO reports, and leaked documents provides a strong empirical basis for the conclusions drawn.

The relevance of this research extends beyond Palestine. As U.S. Big Tech companies increasingly operate as global security and infrastructure providers, similar dynamics are likely to appear in other postcolonial and conflict-affected contexts. Understanding digital colonialism is therefore crucial for future debates on global digital governance, human rights, and

international political economy. Yilmaz (2025, p.223) states, resistance to the current global governance regime come in various forms such as national governments building independent digital infrastructures, civic societies that advocate for digital rights and through platform alternatives. However, these are isolated initiatives, real change comes collaboration of (Global South) countries to regulate cross-border data flows and share open-source alternatives that challenge the monopolistic power of U.S. Big Tech. This thesis underscores how confronting digital colonialism requires not only technical regulation but a rethinking of how power and sovereignty are organized withing our digital infrastructures.

Bibliography

Abraham, Y. (2023, November 30). 'A mass assassination factory': Inside Israel's calculated bombing of Gaza, *+972Magazine*. Retrieved from https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

Abraham, Y. (2024, August 4). 'Order from Amazon; How tech giants are storing mass data for Israel's war. *+972magazine*. Retrieved from https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza, *+972Magazine*. Retrieved from https://www.972mag.com/lavender-ai-israeli-army-gaza/

Abraham, Y., Davies, H. (2025, January 23). Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war. *the Guardian*. Retrieved from https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft

Abraham, Y., Davies, H. (2025, August 6). 'A million calls an hour': Israel relying on Microsoft cloud for expansive surveillance of Palestinians. *the Guardian*. Retrieved from https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud

Abraham, Y., Davies, H. (2025, October 29). 'No restrictions' and a secret 'wink'; inside Israel's deal with Google Amazon. *+972Magazine*. Retrieved from https://www.972mag.com/project-nimbus-contract-google-amazon-israel/

Amazon AWS. *Responsible AI: From principles to practice.* Retrieved from https://aws.amazon.com/ai/responsible-ai/

Amnesty International (2025, August 29). *Why are Big Tech companies a threat to Human rights?* Retrieved from https://www.amnesty.org/en/latest/news/2025/08/why-are-big-tech-companies-a-threat-to-human-rights/

Bellanova, R., Irion, K., Lindskov Jacobsen, K., Ragazzi, F. P. S. M., Saugmann, R., & Suchman, L. (2021). Toward a critique of algorithmic violence. *International policy Sociology*, 15(1), 121-150. https://doi.org/10.1093/ips/olab003

Belli, L., Jiang, M. (2024). "Digital Sovereignty From the BRICS: Structuring Self Determination, Cybersecurity, and Control." In Digital Sovereignty in the BRICS Countries: In

How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge, UK: *Cambridge University Press*

Berger, Y. (2025, October 8). Microsoft's Crackdown on Unit 8200 Reveals Tech's Intermediary Role. *Lawfare*. Retrieved from https://www.lawfaremedia.org/article/microsoft-s-crackdown-on-unit-8200-reveals-tech-s-intermediary-role

Biddle, S. (2022, July 24). Documents Reveal Advanced AI Tools Google Is Selling to Israel. *The Intercept*. Retrieved from https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

Biddle, S. (2024, May 1). Israeli Weapons Firms Required to Buy Cloud Services From Google And Amazon, *The Intercept*. Retrieved from https://theintercept.com/2024/05/01/google-amazon-nimbus-israel-weapons-arms-gaza/

Biesecker, M., Mednick, S., Burke, G. (2025, February 18). How US tech giants' AI is changing the face of warfare in Gaza and Lebanon. *AP News*. Retrieved from https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108

Brännström, L., Gunneflo, M., Noll, G., Parsa, A. (2024). Legal imagination and the US project of globalising the free flow of data. *AI & Society*, *39*(5), 2259–2266. https://doi.org/10.1007/s00146-023-01732-y

Burns, R. (2014). Moments of closure in the knowledge politics of digital humanitarianism. *Geoforum*, *53*, 51–62. https://doi.org/10.1016/j.geoforum.2014.02.002

Cherny, M., (2024, July 3). Amazon to build $1.3 Billion Top-Secret Cloud for Australia's Government. *The Wall street Journal*. Retrieved from https://www.wsj.com/tech/amazon-to-build-1-3-billion-top-secret-cloud-for-australias-government-699ec515

Cogburn, D. L. (2003). Governing global information and communications policy: Emergent regime formation and the impact on Africa. *Telecommunications Policy*, *27*(1), 135–153. https://doi.org/10.1016/S0308-5961(02)00088-5

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race and Law, 24*, 417–439. https://doi.org/10.36643/mjrl.24.2.digital

Col. Racheli Dembinsky speaking at a conference titled "IT for IDF" (2024, July 10). [video file] Retrieved from https://www.youtube.com/watch?v=qLBDfnZJrC8

Constantiou, I. D., Kallinikos, J. (2015). New Games, New Rules: Big Data and the Changing Context of Strategy. *Journal of Information Technology*, *30*(1), 44–57. https://doi.org/10.1057/jit.2014.17

Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 20(4), 336–349. https://doi.org/10.1177/1527476418796632

Cowhey, P. F. (1990). The international telecommunications regime: the political roots of regimes for high technology. *International Organization*, *44*(2), 169–199. https://doi.org/10.1017/S0020818300035244

Cowhey, P., Klimenko, M. M. (2004). The New International Trade Regime in Telecommunication Services and Network Modernization in Transition Economies. *Emerging Markets Finance & Trade*, *40*(1), 59–94. https://doi.org/10.1080/1540496X.2004.11052561

D'Cunha, C. (2021). "A State in the disguise of a Merchant": Tech Leviathans and the rule of law. *European Law Journal*, 27, 109–131. https://doi.org/10.1111/eulj.12399

Daniel Schiller. (1999). *Digital Capitalism : Networking the Global Market System*. The MIT Press.

Devlin, H. (2019, October 5). We are hurtling towards a surveillance state: The rise of facial recognition technology. *The Guardian.* Retrieved from https://www.facewatch.co.uk/2019/10/06/guardian-newspaper-reports-on-the-rise-of-facial-recognition-technology/

Feldstein, S. (2019). The global expansion of AI surveillance. *Carnegie Endowment for International Peace*. Retrieved from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Fischer, D. (2022). The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Zeitschrift Für Politikwissenschaft*, *32*(2), 383–402. https://doi.org/10.1007/s41358-022-00316-4

Flonk, D., Jachtenfuchs, M., Obendiek, A. (2020). "Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?" *Global Constitutionalism* 9(2): 364–86. Doi: 10.1017/S2045381720000167.

Frenkel, S. (2024, March 27). Israel Deploys Expansive Facial Recognition Program in Gaza, *New York Times*. Retrieved from https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

Frenkel, S. (2025, September 25). Microsoft Disables Some Services To Israel's Defense Ministry. *The New York Times*. Retrieved from https://www.nytimes.com/2025/09/25/technology/microsoft-israel-defense-ministry.html

Google. (2021, October 14) *Core Infra Nimbus Webinar.* Retrieved from https://www.documentcloud.org/documents/22119705-core-infra-nimbus-webinar/

Google. *Our AI Principles*. Retrieved from https://ai.google/principles/

Halacha. (2021). *Nr 7 The Internet*. Retrieved from https://www.intelligence-research.org.il/userfiles/image/cat7/Halacha_No.7_INTERNET_10.11.2021%20(1).pdf

Hao, K., Swart, H. (2022, April 19). South Africa's private surveillance machine is fuelling a digital apartheid. *MIT Tech Review*. Retrieved from https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/

Heeks, R. (2008). ICT4D 2.0: The Next Phase of Applying ICT for International Development. *Computer (Long Beach, Calif.)*, *41*(6), 26–33. https://doi.org/10.1109/MC.2008.192

Hoijtink, M. & Planqué-van Hardeveld, A. (2022) Machine Learning and the Platformization of the Military: A Study of Google's Machine Learning Platform TensorFlow, *International Political Sociology*, 16(2), https://doi.org/10.1093/ips/olab036

Human Rights Watch. (2023, December 21). *Meta's broken promises*. Retrieved from https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

Grant, N. (2024, April 19). Google Fires 28 Employees Involved in Protest of Israeli Cloud Contract. *The New York Times.* Retrieved from https://www.nytimes.com/2024/04/18/technology/google-firing-israeli-cloud-contract.html

IDF. (2023, November 2) *הצצה למפעל המטרות של צה"ל הפועל מסביב לשעון / A glimpse into the IDF's target operation that operates around the clock*. Retrieved from https;//www.idf.il/%D&

International Court of Justice. (024, May 24), *Order Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel)*. Retrieved from www.icj-cij.org

Jiang, M. (2024). Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. *Policy and Internet*, *16*(4), 727–738. https://doi.org/10.1002/poi3.427

Kaya, M., Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. Interdisciplinary Studies in Society, *Law and Politics*, 4(2), pp.219-233. https://doi.org/10.61838/kman.isslp.4.2.20

Kensicki, A. (2019). "Smart" Colonialism and Digital Divestment: A Case Study. *Journal of Palestine Studies*, *48*(2), 7–25. https://doi.org/10.1525/jps.2019.48.2.7

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3-26. https://doi.org/10.1177/0306396818823172

Kukutai, T., Taylor, J. (2016). *Indigenous Data Sovereignty: Toward an Agenda (CAEPR).* Canberra, Australia: ANU Press.

Latonero, M., Kift, P. (2018). On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control. *Social Media + Society*, *4*(1). 1-11 https://doi.org/10.1177/2056305118764432

Madianou, M. (2019). Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media + Society*, *5*(3). 1-13 https://doi.org/10.1177/2056305119863146

Mann, M., Daly A. (2019). (Big) data and the North-in-South: Australia's informational imperialism and digital colonialism. *Television & New Media, 20*, 379-395. ttps://doi.org/10.1177/1527476418806091

Microsoft. (2025, May 15). *Microsoft statement on the issues relating to technology services in Israel and Gaza.* Retrieved from https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/

Microsoft AI. *Principles and Approach*. Retrieved from https://www.microsoft.com/en-us/ai/principles-and-approach

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mouton, M., Burns, R. (2021). (Digital) neo-colonialism in the smart city. *Regional Studies*, *55*(12), 1890–1901. https://doi.org/10.1080/00343404.2021.1915974

Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, *42*(3), 329–348. https://doi.org/10.1177/0163443719890530

Nothias, T. (2025). An intellectual history of digital colonialism. *Journal of Communication*. 1-13 https://doi.org/10.1093/joc/jqaf003

Peron, A. E. D. R., Evangelista, R. (2024). Beyond Instrumentarianism: Automated Facial Recognition Systems in Brazil and Digital Colonialism's Violence. *Science, Technology & Society (New Delhi, India)*, *29*(4), 535–554. https://doi.org/10.1177/09717218241281819

PG, A. (2025, September 17). Seeing the world like a Palestinian. *Transnational Institute*. Retrieved from https://www.tni.org/en/article/seeing-the-world-like-a-palestinian

Qandeel, M., & Topak, Ö. E. (2025). Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis. *Journal of Genocide Research*. 1–22. https://doi.org/10.1080/14623528.2025.2567372

Radu, R. (2019). 'Privatization and Globalization of the Internet', *Negotiating Internet Governance*, 75-112 https://doi.org/10.1093/oso/9780198833079.003.0004

Scheck, J., McGinty, T., Purnell, N. (2022, January 24). Facebook Promised Poor Countries Free Internet. People Got Charged Anyway. *Wall Street Journal*, Retrieved from https://www.wsj.com/articles/facebook-free-india-data-charges-11643035284.

Tawil-Souri, H., & Aouragh, M. (2014). Intifada 3.0? Cyber Colonialism and Palestinian Resistance. *The Arab Studies Journal*, *22*(1), 102–133. http://www.jstor.org/stable/24877901

Tuzcu, P. (2021). Decoding the cybaltern: cybercolonialism and postcolonial intellectuals in the digital age. *Postcolonial Studies, 24*(4), 514–527. https://doi.org/10.1080/13688790.2021.1985264

United Nations (n.d.). *about the Nakba*. Retrieved from https://www.un.org/unispal/about-the-nakba/

UNHR (1966, December 16). *International Covenant on Civil and Political Rights*. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

UNHR. (2023, August 28). *Arbitrary deprivation of liberty in the occupied Palestinian territory: the Palestinian experience behind and beyond bars, Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967.* Retrieved from https://docs.un.org/en/A/HRC/53/59

UNHR (2024, March 25). Anatomy of a Genocide - Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967". Retrieved from https://www.un.org/unispal/document/anatomy-of-a-genocide-report-of-the-special-rapporteur-on-the-situation-of-human-rights-in-the-palestinian-territory-occupied-since-1967-to-human-rights-council-advance-unedited-version-a-hrc-55/

UHHRC. (2025, June 16). *A/HRC/59/32: Practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies, including activities relating to artificial intelligence - Report of the Office of the United Nations High Commissioner for Human Rights (advance edited version).* Retrieved from

https://www.ohchr.org/en/documents/thematic-reports/ahrc5932-practical-application-guiding-principles-business-and-human

What is Project Nimbus, and why are Google workers protesting Israel deal? (2024, April 23). *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal

Wright, C. (2021). China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road. *SAIS Review of International Affairs.*, *41*(2), 89–113. https://doi.org/10.1353/sais.2021.0020

Yılmaz, Ö. (2025). The Origins of Digital Colonialism, İmgelem, 16, 321-344. https://doi.org/10.53791/imgelem.1636282

Young, J. C. (2019). The new knowledge politics of digital colonialism. Environment and Planning A: *Economy and Space, 51*, 1424–1441. https://doi.org/10.1177/0308518X1985899

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

7amleh, the Arab center for the advancement of social media. (September 2024). *Palestinian Digital rights, genocide, and Big Tech accountability*. Retrieved from https://7amleh.org/storage/genocide/English%20new%20(1).pdf