Channeled Beneath International Law
Vecellio Segate, Riccardo

DOI:
10.1080/10811680.2024.2334081

Publication date:
2024

Licence:
CC BY-NC

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Discovery Research Portal

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in Discovery Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Channeled Beneath International Law: Mapping Infrastructure and Regulatory Capture as Israeli–American Hegemonic Reinforcers in Palestine

Riccardo Vecellio Segate, LLM, PhD

School of Science and Engineering & School of Law, University of Dundee, Scotland, UK; Faculty of Economics and Business, University of Groningen, NL

ABSTRACT

The United States is the most influential actor in the Israeli–Palestinian conflict; its intelligence agencies cooperate with Israel on most “counterterrorism” dossiers impacting Palestinians’ life, with a significant number thereof pertaining to Internet policing in Gaza and the West Bank. Meanwhile, Israel controls some of the key Internet service providers (ISPs) that serve Palestinians, and it is thus endowed with the capability to compel those ISPs to filter information so as to perform as American propaganda reinforcers. Moreover, the United States may unaccountably assert jurisdiction over data from and to Palestine because American cables are where most of the Internet transits through, exercising surveillance without judicial oversight. Verified instances of censorship directed by government-tied U.S. corporations, especially during confrontational seasons, are indeed numerous. Palestinian authorities themselves contribute to creating information clusters and identity bubbles, with infrastructural deficiencies as well as executive and court orders undermining freedom of expression online under arbitrary “public morals” or “security” concerns. The combined effect of technical advantage and regulatory capture supports the convergence of interests between Palestinian and Israeli authorities in restricting Palestinians’ digital rights, and assists the United States in reiterating its “security” hegemony in the region. This warrants a debunking of the limits of the law in constraining private actors and readjusting states’ jurisdiction over Internet infrastructure and data packets transiting through it.

KEYWORDS

Counterterrorism legislation; critical data governance; digital apartheid; digital sovereignty; infrastructure normativity; Internet jurisdiction; legal geographies; public–private regulatory capture

Introduction

Data sovereignty is an infrastructure-intensive terrain of contestation for states and citizens alike. Everywhere in the world, but particularly in contended areas such as Palestine, Internet design and digital policies are regulated well beyond the law, with the latter coping with (or ignoring) infrastructure-level contingencies and related policy


CONTACT Riccardo Vecellio Segate rvecelliosegate001@dundee.ac.uk; r.vecellio.segate@rug.nl School of Science and Engineering, University of Dundee, Dundee, UK

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.
arrangements that make the law redundant or unserviceable for all those who are already targeted with and suffering from discrimination. Hegemons (be they prospective or actual) tend to make the most of this apparent misalignment between the Internet as infrastructure (network) and the Internet as flow of information (content), that is, of the purported insignificance or neutrality of the former for controlling the latter. This article explores this misalignment with reference to Palestine and, more specifically, from the normative, critical third-world perspective of the Palestinians. Nevertheless, prior to delving into the gist of this discussion, a few preliminary remarks are outstanding.

Sovereignty-wise, public Internet governance rests at the confluence of exercising authority over both data transmissions and the “hard structure” enabling them. This calls for two debates that are far too often addressed separately, as if the concerns they raised could be discussed independently. The first debate concerns the Internet as a channeler and propagator of ideas; in this respect, from the viewpoint of democratic societies, public interferences with the free flow of online information are justifiable only in a limited, regulated set of circumstances. There is a Western discourse that emphasizes the appointment of the state as a mere “guarantor” of the public order online, with no supplementary function other than upholding a vaguely defined no-harm approach to online communications. This is ordinarily phrased along the lines of “digital constitutionalism.” Yet because the “geopolitical West” has repeatedly failed to deliver on this premise (and promise) both in-house and abroad, often disguising cyber-surveillance as “security” and “counterterrorism,” governmental agencies at multiple levels have increasingly felt legitimized to overstep their original mandate, up to eventually policing the Internet—overtly or surreptitiously, also depending on the democratic or nondemocratic nature of the state concerned. The second debate concerns the materiality of the Internet, that is, its infrastructural underpinnings; while it is widely ascertained that states may control mentioned infrastructure to filter communications in and out, how infrastructural control shapes the production of online content and the legal and policy stances toward the moderation thereof is severely understudied, especially in context of “borderline statehood”—so to write. In those contexts, infrastructural control and immediate legislative prerogatives over online content may not fall with the same authorities, or even within the same state. There, online and

---


offline authority over the Internet, just like territorial and communication sovereignty, may not perfectly coincide. To make everything more complicated, the asymmetries are exploited by foreign or domestic private parties that de facto or de jure enforce “public authority” of dubious legal standing and fragmented policy mandate. To a largely misappreciated extent, it is the “materiality” of Internet networks that enables or augments the surveillance, censorship, and distortion of online contents.

As for the Internet’s material structure, it may be explained as follows:

It starts at the “bottom” with the physical layer (telephone line, coaxial cable, fibre, wireless, etc.), and then a logical layer consisting of transport protocols (TCP/IP, HTTP) that define how messages are encoded and transported online. Above this is the application layer that defines how the network is used (e.g., search, social networks, websites), and at the top of the stack is the content layer (text, speech, image, video, music, telemetry), which is the actual information that is conveyed by the Internet.

The present work expounds how the first (infrastructure) and second (appliances) layers are controlled to surveil the third (applications) and ultimately fourth (contents) ones. The reader is advised to appreciate that the reasoning provided hereinafter is based on cable-channeled Internet, while the Internet might start being delivered through satellites in the near future—a revolution that would call for a reexamination of some of the key tenets illustrated here. For the time being, a few (private) satellites are already being deployed to foster Internet connectivity (most notoriously over Ukraine and Gaza upon their invasion by Russia and Israel, respectively), but the large-scale, public implementation of these technologies for civilian purposes has a long way to go.

Be they Internet service providers (ISPs), social media, or institutions, all these agents (and several state and nonstate others, as we described in the following) contribute their fair share toward the daily “weaponization”—so to speak—of the Palestinian cyberspace as a public agora, to its occupation and militarization. This is not to say that the present work is concerned with social-media skirmishes conducted for “perception management”; nor is it premised to investigate manifestations of information warfare in Palestine per se. Rather, this article seeks to address the following three—interrelated—research questions: (1) Why can Palestine’s neglected cyber sovereignty be technically characterized as U.S.–Israeli meddling by proxy? (2) In what ways does this protracted impairment affect Palestinians’ life? (3) How do cyber censorship and surveillance become hybrid tools to perpetuate, extend, and legally substantiate more traditional means of political violence? These three questions are not examined one by one;

---

9 Iosifidis and Wheeler, 2016, 71, emphases in the original.
instead, they are answered in a coherent whole as this article progresses, leading to the (admittedly quite tentative) policy suggestions formulated in the final section. The purpose of the present investigation is thus to justify the formulation of just-mentioned policy proposals, as well as to debunk the salience of (captured) infrastructural arrangements for which the policy momentum far outshines regulatory and legislative efforts in the Internet realm.

Prior to delving into Palestine, one more note is due. The reason why this article addresses the three research questions together, as opposed to dealing with each of them in turn, is that the material is deliberately organized in such a manner to coherently lead to overall policy proposals that are centered inter alia around content moderation, despite the article’s originality contribution not resting with content moderation per se. Turning to the three questions one by one would have perhaps reinforced expectations to find policy proposal equally addressing each problem in a silos. Instead, while the proposals are articulated around regulatory issues, especially content moderation, the root of those issues is to be traced to the network–content relationship, which is underproblematized and represents the gist of this article’s contribution. The gist of this article is the role of Internet infrastructure (or “architecture”) and “degrees of sovereignty” thereon in shaping online surveillance, regulatory capture, and ultimately content-moderation regulations and practices. As the article clarifies, the degree of sovereignty on Internet infrastructure could not be more momentous for content moderation, and in contexts where addressing sovereignty would prove merely idealistic, regulating content moderation to account for sovereignty constraints is one of the ways to minimize the violation of users’ rights and promote their online and offline emancipation. When Internet sovereignty is weak, authorities tend to pursue undue ideological alignment and “stance leveling” with the occupying, dominant, and/or hegemonic power, which tends to co-provide Internet services and surveil their operations. This increased scope for surveillance and preventative censorship, as well as for intelligence supply, calls for user mistrust and self-censorship, fostering a “chilling effect” that will have repercussions on their collective identity and communications, and thus emancipation, as an offline community as well. In turn, if users (and citizens) understand that their authorities are not sovereign over their Internet policing and infrastructure, but rather colluded with foreign powers and regulatory capture by their corporate entities, they will not conform to such authorities’ directives and will eventually turn the Internet to a terrain for anonymized contestation, rebellion, and violent rhetoric. These risks, and especially their root causes, must be accounted for when it comes to content moderation, in such a way that the latter is not perceived as “biased” or “one-sided” by the most disadvantaged users who belonging to the most “unsovereign” territories. The focus here, however, is on the root causes; content moderation only features in the policy proposals, right before the Conclusion.

Unneutral Digital Colonialism in Palestine

Since the 1970s, Israel and Palestine have—initially unintentionally—positioned themselves as the natural laboratory for digital cartographers due to their precariously
compenetrating sovereign and unsovereign spaces, “withouts” and “withinss.” Lindtner et al. compellingly observed that “maps can be crucial for survival, not just for finding the nearest Starbucks.” Indeed, digital struggles fall within the portfolio of acts of resistance against “the violence of police power and the criminalization of poverty and protest” that characterize what has been termed “the Anthropocene or the Capitalocene”: the era where the “burdens of solving precarity too often fall on those who are already the most precarious.” In this context, they posit,

Digital infrastructures, from fiber optics to communications platforms, are run on dispossession, genocide, forced relocation, and extraction. Local communities have responded by “bootstrapping” digital infrastructure. Rather than owning the means of production directly, appropriating the means of mediation has become a way to control the lifeblood of commodity circulation.

A parallel can be drawn to more traditional infrastructure policies. Dugard and Reynolds recall that in the West Bank,

The separate road system[ ... ] central to its territorial fragmentation and distinctly evocative of a sense of apartheid despite the absence of an equivalent in the South African context, evolved in the planning and construction realm as a prop for broader segregationist policies without a legislative foundation.

Equally unlegislated about, and yet effective, is the private rule of online mapping services that only show itineraries suitable for the Israelis. An infamous exemplification is the one reported by Al Jazeera five years ago: Not only did Google Maps align to the United States’ nonrecognition of Palestinian statehood (which is manifestly hegemonic, but only of moderate practical significance for the app’s users); more concretely, Google Maps pointed both Palestinians and Israelis to roads that were in fact used by Israelis only, and that for security reasons should not have been traversed by Palestinians. This fact not only contributed to minor incidents; it also reinforced an identity narrative according to which the Israeli viewpoint comes forward, while the other one embodies “the rest,” “the alternative,” the minority one, even where Palestinians represent the overwhelming majority of citizens and users. Most recently, Google Maps and Waze apps reportedly decided to accommodate a request by the Israel Defense Forces to turn off their real-time traffic data feature in order to prevent the disclosure of information that could help track the planning and execution of the Gaza invasion.

The Google Maps saga situates itself on the plane of digital contents, but even before entering such level of analysis, issues of technological segregation in Palestine lie with

---


15 Ibid.


its infrastructure. For instance, checkpoints between Israel and the Occupied Palestinian Territories (OPT) are placed under Israeli military authority and, on the civilian side, under the administration of the Director-General of the Public Administration of the Crossing Points and Borders, who is also endowed with the authority to “define the developmental needs on the level of infrastructure, modern equipment and tools, and the security requirements” as well as to “define the needs required from international parties, especially in the field of technical expertise.” Against this backdrop, the problem does not rest itself solely on the fact that in mobility apps certain roads are privileged over others or certain checkpoints are not displayed, and so forth; rather, it is more about the fact that out of political will, around those very same checkpoints no phone-line coverage for Palestinian telecom operators is allowed. The result is that exactly where most human-rights abuses are committed, power imbalance manifests itself starting at the infrastructural level and propagates therefrom, originating a telling mismatch between political and infrastructural boundaries.

While the Internet is often discussed about as if it were a neutral commons, Cristiano reminds us that

broadband diffusion […] tends to follow profit dynamics, as much as […] infrastructural ownership […] regulate[s] the access to cyberspace (the “square”) and thus compromise[s] the extent [to] which political freedoms online are to be enabled collectively, and for the collectivity.

This struggle is hardly more obvious anywhere else than in the OPT, which is why “strengthen[ing] Palestine’s cyber security and ensur[ing] the [Information and Communication Technology (ICT)] sector’s freedom from external threats and domi-
nation” feature in the Sustainable Development Goals (SDGs) plan of Palestine. One could be tempted to assume that in such a vulnerable, subjugated territory as the OPT, whose issues range from food security to the detention of children, framing ICT within principled and aspirational manifestos such as the SDGs features at the bottom of the agenda. In fact, it is quite the reverse: Supporting international discourses around digital rights, however phrased, is crucial in a territory where Israeli authorities can (and do) suppress opposition and protest by censoring or disconnecting Internet networks. Hence, mentioned inclusion in their SDGs plan cannot come as surprising: “The Palestinian network is in reality nothing but a sub-network of the Israeli network, and

19 Article 4(a)(7–8) of the Presidential Decree No. 16 of 2006 Concerning the Regulation of the Public Administration of the Crossing Points and Borders, enacted on 18 March 2006, officially promulgated in the Gazette of 14 June 2006 no 65, 27, as reported in Roland Friedrich, Arnold Luethold, and Firas Milhem (eds), The Security Sector Legislation of the Palestinian National Authority, 270 (DCAF, 2008).
22 Fabio Cristiano, Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory, in Gabriel Bloum-Genest, Marie-Christine Doran, and Sylvie Paquierot (eds), Human Rights as Battlegrounds: Changing Practices and Contestations 249–268, 253 (Palgrave, 2019).
23 The State of Palestine’s Palestinian National Voluntary Review on the Implementation of the 2030 Agenda (June 2018) at pp. 90–91, with reference to Goal 9 as well as Goal 17 (emphasis added). Freedom from digital domination is so essential to avert cyber-vulnerability that some scholars have gone so far as to propose that cyber blockades by foreign agents are addressed as crimes against humanity; refer eg to https://doi.org/10.34190/iccws.19.1.1948.
Palestinian ISPs are in practice retailers for Israeli ISPs. Market-wise, as illustrated in an infographic released by the Visualizing Palestine project, Palestinians pay more to receive less compared to their Israeli counterparts. Discriminating against Palestinians through what is supposed to be “their own” market and economic infrastructure has long been a constant in technology policing, both before and after the Internet. In fact, alongside the desire to integrate West Bank Palestinians into the Israeli economy, there was a simultaneous desire to exclude these same people in the name of Israeli “security”. It is the tension between these two processes that creates the border regime.

Nonetheless, Internet penetration per se is the least concerning among all technology-related problems for Palestinians, whose access-to-Internet statistics were extremely poor two decades ago but have improved rapidly, up to standing now in line with those of other jurisdictions in the Middle East and North Africa (MENA) region. What may alarm one instead is the overt or hidden control on such Internet, which includes surveillance and subsequent extortion and blackmailing related to digital content, exercised both within and beyond the law. Some of these “law-enforcement” techniques are operated in a legal gray area domestically, meaning that they are neither provided for in (any) domestic law nor ruled out as unlawful under the same regime(s). However, under international law—thus, primarily pursuant to the International Covenant on Civil and Political Rights (ICCPR), to which Israel has been a party since 1991, and related nonbinding yet highly authoritative General Comment by the United Nations (UN) Human Rights Committee (HRCttee)—any gray area privacy-wise verges toward unlawfulness. Scholars reasoned that

ICCPR Article 17 prohibits two forms of interference with privacy: “unlawful” interference and “arbitrary” interference. [...] Absent affirmative authorization by a [S]tate’s legislation, which in turn must comport with the ICCPR, interference with an individual’s right to privacy is therefore prohibited. Additionally, [...] the domestic law authorizing such interference must be both reasonably foreseeable to the person concerned as well as precise and clearly defined. [...] Intelligence surveillance of civilians who are not participating in hostilities [...] is neither reasonable nor proportional and should therefore be deemed arbitrary [...] Assuming, arguendo, the viability of the declared state of public emergency in Israel, these practices would remain violations. While intelligence collection and the infringement of privacy in certain cases may well be protected under Article 4 [ICCPR],

27Zureik et al., op. cit., 32.
29Petros Iospidis and Mark Wheeler, Public Spheres and Mediated Social Networks in the Western Context and Beyond, 184, 262 (Palgrave, 2016); Raja Khalidi et al., Palestinian Innovation System and Digital Economy: Challenges and Opportunities—Annexes, Paper Prepared for the Swiss Development Cooperation, 3, 9 (Palestine Economic Policy Research Institute, Ma’had Abhath As-Syasat Al-Iqtisadiya Al-Filastini, 2018).
even by its own terms, permissible infringement is limited to what is “strictly required.””

These civilians are being targeted simply because they are Palestinians residing in the OPT, without any cause to believe that they are involved in military or terrorist activity. [Importantly], the ICCPR should be found to apply extraterritorially at least insofar as it restricts Israeli action in the OPT.  

Furthermore, it shall be noted that while Israel has attached a reservation to Article 23 ICCPR, it has not expressed any objection to Articles 4, 17, or others.

Along the lines of what the International Court of Justice (ICJ) authoritatively advised in its Wall Advisory Opinion, the preceding demonstrates that unreasonable surveillance conducted by Israel in the OPT is unlawful under international law. Indeed, it has long been recognized, also from the perspective of international human rights law (IHRL), that Internet access alone is meaningless when not complemented by a set of digital rights. Worse even, Internet access per se, which is consistently touted as a self-standing human right due to its supposed merits as an enabler of emancipation, might in fact turn into yet another instrument in autocrats’ (or, in this case, occupiers’) policy toolset aimed at denying individuals their fundamental rights and freedoms of thought, opinion, speech, association, and so forth. This necessary complementarity is mirrored in content-moderation practices, particularly relevant for social-media platforms. After all, the delusion with Palestine is not visibility, but what is being made visible, so that a human-rights approach—underpinned by the principles of legality, legitimacy, and necessity—to said content moderation, despite its foreseeable pitfalls, is warranted. Such an approach would help rebalance the conjecture that “content moderators endeavor to apply the same set [of] rules to [e.g.] Facebook’s 2.3 billion monthly users around the world regardless of social or political context” with more culturally proximate, “indigenous,” and context-sensitive considerations of language and customs informed by historical roots as much as actual on-the-ground, daily-life contingency.

Besides social-media platforms, ISPs are—as mentioned earlier—another agent for potential Internet censorship, contributing to degrading users’ digital rights in Palestine. This follows a global trend whereby “sometimes unknowingly, sometimes reluctantly, sometimes willingly, [private Internet intermediaries] have provided key infrastructure for monitoring and analysing citizens’ communication activities,” a practice that is even graver here as those private actors belong or report to an occupying sovereign entity (Israel). Nonetheless, it shall be emphasized that the trend is Western, too; there

---

33 Cristiano, op. cit., 250–251.
34 Ibid., 252ff.
35 Ibid., 256.
37 Ibid., 968–970.
38 Ibid., 1005.
is indeed little of non-Western in the “colonial ideology that situates Israel as an out-post of the West”\textsuperscript{41}: the “colonial concerns about challenges to settler domination are all filtered through a racial discourse that identifies Palestinians, Arabs, and Muslims as the sources of violence and instability,” and are channeled through the Internet as well. In this sense, the Internet stands as a means by which the crime of apartheid as understood under \textit{public international law} is committed: In the wake of Israeli as well as international doctrinal investigations having already concluded that the stigma of apartheid can be attached to the way Israel exercises its military rule over the non-Israeli Palestinians \textit{as far as international law is concerned},\textsuperscript{42} one can identify with the Israeli management of and control over Palestine’s Internet all the elements that characterize said apartheid more generally, including discrimination, neglect of self-determination, settler colonialism,\textsuperscript{43} and the systematic oppression more and more embedded within institutions as generations take turns.

In Palestine, these tendencies have been worsening rather than relaxing, following—one may suppose—a global trend to the same effect.\textsuperscript{44} While the common imaginary is filled with early-days infrastructure-neutral assumption about online communication, reality is that the Internet architecture has been gradually reconfigured to secure “the prioritization of corporate interests over the interests of end users.”\textsuperscript{45} And wherever (digital) sovereignty is weak, authorities more easily defer to the commercial interests and strategic projections of foreign providers and their states of incorporation. For this reason, while the Internet is charged with a special connotation in Palestine as a much-needed digital replacement for physical mobility and affection\textsuperscript{46} for which the longstanding removal has been normalized and institutionalized, I believe this study may hold wider significance for all other territories that do not enjoy their own sovereign Internet, either because they are militarily occupied or owing to any other technical or socioeconomic reasons. As the regulatory grip on digital infrastructure and content tightens across most world region, and with instances of contested statehood and state–nation asymmetry arguably on the increase, this resonates and holds relevance well beyond Palestine. In fact, at times it is the “state” that finds itself “unsovereign” over the local Internet, and at other times it is the “nation” (intended here as civilization, polity, identity-homogeneous populace) to feel “expropriated,” either because that nation’s “related” state controls the Internet on their behalf, or because the cross-border configuration of such nation\textsuperscript{47} is not backed by an equally cross-border national Internet, which is rather segmented across different state sovereignties. For instance, Aouragh illustrates how


\textsuperscript{46}Elia Zurbik, \textit{Israel’s Colonial Project in Palestine: Brutal Pursuit} 190–191, 205 (Routledge, 2016).

\textsuperscript{47}Ibid., 206.
Palestinians have not only been exiled because of their political engagement or ideological stance, but mainly because they were expelled under a settler-colonialist project and a continuous context of forced land appropriation. This […] strengthens the importance of “return” as an alternative; also of a virtual return to the homeland. The expression of national identity through online encounters is more poignant in the context of the actual loss of land, and in that of being confronted by a colonial other. […] Indeed, not only most exiled Palestinians do not feel less Palestinian because they are not present on Palestinian soil; rather, they share an imagined community with other Palestinians inside and outside the territorial centre, while simultaneously considering historical Palestine a very important point of reference.48

The peculiarity of their situation originates from their condition as “outsiders” being also a perennially potential status that might materialize almost any time, depending for instance on the pace and brutality of the expansion of the illegal-settlements project. Indeed, as is widely known, what remain of Palestine today are microfragments of land scattered across the West Bank (plus a slice of territory in Gaza, currently being evacuated and bombed), rather than a continuous portion of land linking all major Palestinian urban settlements at least.49

And yet, Palestine is a context of constant battling that far exceeds civilian oppression; if the “reorganisation of the global urban terrain, through a series of micro tactical actions, strives to re-imagine the city not only as the site, but also the very medium of warfare,”50 then the quasi-militarized “occupation” of cyber infrastructure is certainly a component of said medium for permanent, low-intensity engagement. When misguidedly deployed and rhetorically misappropriated by power politics, “connectivity” may also symbolise the ultimate hypocrisy of a ruthless engine of necropolitical crushing; this trend only exacerbated with Internet availability, while actually starting with phones.51 Nearly a decade ago, Zureik offered a vivid description of this necropolitics exercise in the Gaza Strip:

As evidence of its attempts to spare Palestinian lives, Israel does not hesitate to mention the recorded messages, or so-called “roof knocks,” that it sends to Palestinians whose homes and neighbourhoods are about to be bombed. These phone numbers are gathered by Israeli intelligence, and although the targeted Palestinians are given five minutes to vacate their homes, it is not clear where they are supposed to vacate to since Gaza’s high-density housing leaves no room for escape.52

This represents the disembodiment of law from technology, the dissociation between what legal frameworks—international humanitarian law (IHL), in this case—prescribe and their most farcical manipulation and cynical distortion, as endorsed by self-legitimizing military lawyering jargon.53

---

48 Miriam Aouragh, Palestine Online: Transnationalism, the Internet and the Construction of Identity 117, 160 (I.B. Tauris, 2011).
50 Ibid., 28.
52 Zureik, op. cit., 206.
When it comes to both Israel’s domestic market and information and communication technologies (ICT)-focused negotiations in international fora, the telecommunications sector has historically been held in high regard by Israeli policymakers as a foundational component of their statecraft, as well as of their projected identity in the Middle Eastern region and the globe. More specifically, Israel invested considerably in cyberdefense, that is, in securitizing its cyberspace, but it is also one of the very first and few states worldwide to maintain a manifestly offensive cyber unit within its regular army. Meanwhile, Israeli companies (including hundreds of startups) specialized in the high-tech surveillance industry, with the NSO Group featuring among the world’s top sellers of spying software for digital warfare and Verint having been turned into a nonsovereign infrastructure.

When it comes to both Israel’s domestic market and information and communication technologies (ICT)-focused negotiations in international fora, the telecommunications sector has historically been held in high regard by Israeli policymakers as a foundational component of their statecraft, as well as of their projected identity in the Middle Eastern region and the globe. More specifically, Israel invested considerably in cyberdefense, that is, in securitizing its cyberspace, but it is also one of the very first and few states worldwide to maintain a manifestly offensive cyber unit within its regular army. Meanwhile, Israeli companies (including hundreds of startups) specialized in the high-tech surveillance industry, with the NSO Group featuring among the world’s top sellers of spying software for digital warfare and Verint having been turned into a nonsovereign infrastructure.

Taking stock from all aforementioned insights, I next attempt to answer the three questions I introduced earlier. To do so, unmissable companionship will be found in a few sources that, among all others, proved to be of the highest significance for the subject of my study. These are first the empirical report by the 7amleh organization, a summary thereof having been provided by Peoples Dispatch. No less importantly, excellent ethnographic work was conducted by Aouragh across several outlets and intellectually salient contributions came from Tawil-Souri; these two scholars also worked proficiently and published together.

Nonsovereign Infrastructure

More than 90 per cent of both groups thought that outsiders monitored information traffic over the Internet, and when asked to name who these outsiders were, 50 per cent of city dwellers cited the Israeli government and its security agencies; 20 per cent cited the United States, including the Central Intelligence Agency (CIA); and 30 per cent mentioned both the [US] and Israel. Among camp dwellers, […] 73 per cent cited the Israeli government, and the responses of the remaining 27 per cent were distributed evenly, at 9 per cent each, among the US, Israel and the [US], and Israel and official Palestinian institutions.

When it comes to both Israel’s domestic market and information and communication technologies (ICT)-focused negotiations in international fora, the telecommunications sector has historically been held in high regard by Israeli policymakers as a foundational component of their statecraft, as well as of their projected identity in the Middle Eastern region and the globe. More specifically, Israel invested considerably in cyberdefense, that is, in securitizing its cyberspace, but it is also one of the very first and few states worldwide to maintain a manifestly offensive cyber unit within its regular army. Meanwhile, Israeli companies (including hundreds of startups) specialized in the high-tech surveillance industry, with the NSO Group featuring among the world’s top sellers of spying software for digital warfare and Verint having been turned into a nonsovereign infrastructure.

57 Tawil-Souri, op. cit.
59 Zureik op. cit., 190.
63 Fabio Cristiano, Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy, in Scott N. Romaniuk and Mary Manjikian (eds), ROUTLEDGE COMPANION TO GLOBAL CYBER-SECURITY STRATEGY (Palgrave, 2020).
U.S. company just for tax-minimization purposes, while remaining essentially subservient to Israel’s political interests. This is far from an isolated incident. Tellingly, Israel has one of the three global clusters of cybersecurity firms (the remaining two clusters being American).

The prioritization of this innovation sector over others, and the revolving doors connecting the Israeli and U.S. cybertech industries, are not a coincidence: They manifest the web of formal and informal Israeli–American ties in the (cyber-)defense field, crafted under the “securitization” manifesto. In 2022, the Israel–US Binational Industrial Research and Development (BIRD) Foundation, funded by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), launched the “BIRD Cyber” initiative in partnership with the Israel National Cyber Directorate (INCD). This is an outstandingly privileged relationship that intends to advance the cybersecurity of American interests and objectives in the Middle East. After all, in October 2023 the U.S. International Trade Administration confirmed it deems “Israel’s telecommunication network [to be] one of the most sophisticated in the world”—also thanks to U.S.-supplied, U.S.-trained, U.S.-funded, and U.S.-overseen cyberdefense, surveillance, censorship, and offense capabilities. Aside from the commercial and military benefits for technology vendors and armies’ cyber units, the U.S.–Israeli cyber ties are potentially aimed at converging around the same approach to global Internet governance, not least at the UN level; they are also supportive of a broader bilateral “High-Level Dialogue” to “manage risks to [their] respective technology ecosystems,” supposedly premised to “promote […] democratic principles, and human rights.” The United States “has been highly impressed by the progress of the Israeli cyber community, learning its path, listening to its cyber leaders, and adhering to their vision,” to such an extent that Israeli scholars frequently propose their country’s cyberdevelopment as a best practice or even a role model for the United States to replicate on a larger scale.

Besides Germany, but still arguably in an attempt to clear their sense of guilt and remedy to their historical wrongs, the most persistent Israeli allies in the geopolitical chessboard are the United Kingdom (UK) and the United States; in this sense, these

---

three jurisdictions (Israel, the UK, and the United States) broadly conform to the canons of an “international clientelistic network” as defined by international relations (IR) scholars. Al-Jazeera, sympathetic to the Palestinian nationalist cause and initially hailed as a beacon of journalistic freedom in the region, was later dismissed as a terrorist-affiliated media outlet by influential American (and Western generally) media tycoons as well as political leaders, so that its Palestinian coverage, too, fell out of the radar in the West through a process of “socialization of value bias.”

From “high politics” to several diplomatic dossiers and, of course, the all-comprehensive and much trendy label of “counterterrorism,” intelligence cooperation has grown steadily between Israel and the United States, showing no signs of abating; the same holds true between their armed forces, police, and law-enforcement agencies generally. If “the US military has widely imitated the experience, technology and doctrine of Israeli forces in tailoring itself to the challenges of urban colonial and counter-insurgency warfare,” it is also salient to explore the way Internet infrastructure has become a component of this urban warfare, and the reason why the U.S. sovereignty over its Internet and indirect de facto control over a major part of the global network matter to Israel in this respect, despite geographical nonproximity.

In fact, provided the “counterterrorist” goals of both the United States and Israel are indeed those “to entrench their sovereign power against a generalized, demonized enemy whose geopolitical claims are radically delegitimized and whose subhuman, monster-like status means that political negotiations will never be necessary,” then those goals can be pursued through the techno-infrastructure (and only later, if needed, legal) control of the Internet, too. This triggers a bundle of choices investing not only bilateral business and politics, but also the crafting of a coherent, almost “coordinated” legal patronage to certain practices that transcend the offline reality to encompass the online “delegitimization” of the Other. On a slightly lighter note, this might also help explain why, differently from the Arab Springs in Tunisia and Egypt, which were supported by Facebook as well as—very explicitly—by the United States, the same support faded with regard to the subsequent uprisings in Palestine, with Israel requesting Facebook to shut down pro-Palestinian pages, and Facebook subserviently complying. That was no

---

76 On this terminology, see further Rainer Ricardo, International Hierarchies Built Upon Gratitude as Political Power, E-INTERNATIONAL RELATIONS (2019), https://www.e-ir.info/2019/12/19/international-hierarchies-built-upon-gratitude-as-political-power/.


80 Clarno, op. cit., 165.


82 Ibid., 136.

83 Former—and still most widely known—denomination of Meta Platforms, Inc. Throughout this article, I keep the original denomination of Facebook even when referring not just to the social-network platform but to its running company, too, which is now called Meta Platforms, Inc. The same goes for Twitter, now X.

surprise though, not even at a more systemic level: “Facebook has allowed major abuses of its platform in poor, small and non-western countries in order to prioritize addressing abuses that attract media attention or affect the US and other wealthy countries.”

Even in the Middle Eastern regional context, Palestine is a special case (in the negative) with reference to exercising control over its Internet policing and infrastructure: Any other polity (or “nation”—think, e.g., of the Kurds) does have a state to rely upon for connectivity matters, and by which it is not proactively discriminated against—they are at worst surveilled, but conditions allow for appreciable degrees of resistance. Indeed, Internet discrimination is far easier when the minority polity, which is “alternative” to the one that forms the majority in the given state, is confined to a certain “space” within the state’s borders and factually segregated there with little to no chance of territorial mobility. The aforementioned ghett奧ization of the Palestinians makes discriminating them fairly viable on the side of Internet infrastructure—of course, jointly with relevant policies that “legalize” such discrimination post factum, often citing “emergency” and “exception” as a legal basis. To compare, the neighboring Jordan enjoys an extensive fibre-optic network as part of an ownership-wise globally interconnected information technology (IT) sector that Palestine could have made recourse to—entering into a bilateral agreement with the managers thereof as well as Jordanian state leaders—had it been fully endowed with statehood (and thus autonomous legal personality) under international law, and especially had it not been cyber-colonized by Israeli technologies (i.e., devices plus infrastructure) and policy restrictions.

Internet infrastructure was once deemed to be a neutral means for communication—so much that it was originally conceived and engineered with an eye to practical arrangements, without much overthinking—and yet it has taken on additional meanings over time, including that of channeling censorship, that is, a new locus of special collaboration between private parties and public authorities. In Palestine, it was once believed that the Internet was not involved in the censorship activities pursued by Israeli authorities; relatedly, it was argued that only offline measures were implemented to surveil Palestinians. Hence, to what do we owe this change of gear? To begin with, it is important to specify that Israel does not pursue censorship against Palestinians in Palestine only, and not even exclusively against Palestinians. In fact, under the customary pretext of “security” or, more precisely, “counterterrorism,” the

---

87 Nataliia Gelvanovska, Michael Roży, and Carlo Maria Rosottò, Broadband Networks in the Middle East and North Africa: Accelerating High-Speed Internet Access 159 (The World Bank, 2014).
88 Michael J. Oghia and Helen Indelicato, Ruling Arab Internet: An Analysis of Internet Ownership Trends of Six Arab Countries, in Aleksandra Wilczura (ed), GLOBAL DILEMMAS OF SECURITY AND DEVELOPMENT IN THE MIDDLE EAST 181–196, 190 (Institute of the Middle and Far East of the Jagiellonian University in Kraków, 2013).
91 Hillel Nossek and Yehiel Limor, Fifty Years in a Marriage of Convenience: News Media and Military Censorship In Israel, 6 COMMUNICATION LAW AND POLICY 1–35 (2010).
Israeli Army has compelled the removal of social-media contents “from within” Israel to Israeli citizens as well, although one may argue that this is still a form of Palestine-related censorship in that it seeks to remove any criticism of military operations, most of which pertain indeed to the OPT.

Most remarkably, however, one shall note that the censorship against Palestinians is not operated by Israel only, but also—or even primarily—by Palestinian authorities themselves (although one may argue that it is the same as to say that Israel operates it both directly and, in the latter case, by institutional proxy). For instance, Palestine ordered the ISPs to block at least twelve websites and Facebook application which had a relationship with the rival group Hamas. This is because the [latter] group controlled the Gaza strip. Also, the authority blocked every website that criticized the Fatah leader such as the ynews.com and the middleeastmonitor.com.

What is more, Palestinian journalists are routinely arrested by the Palestinian Authority (PA), and even Israeli journalists reporting from Gaza and the West Bank face condemnation in Israel when they criticise Israeli authorities, regardless of the fact that they simultaneously criticize the PA even about the same occurrences; although this might surprise some, it actually stands as an accurate representation of the PA being wholly regulatorily captured by Israel.

The considerations just described support the claim that “the Palestinian Authority has moved away from [its original] liberatory model to a neoliberal capitalist governance structure and has become a security subcontractor for the Israeli settler colonial state.” This is echoed by Tawil-Souri and Aouragh, as well as by Rahman; Clarno, too, asserted that

the Israeli military and the PA security forces now work together to suppress Palestinian resistance and enforce order in the West Bank enclaves. [One shall in fact] trace the genealogy of security coordination under Oslo to explain the emergence of an advanced network of security agencies—including forces of the US empire and segments of the colonized Palestinian population—that prioritizes the security of Israel.

Indeed, even the much-emphasized privatization of the telecom sector did not entail actual market competition, let alone people’s empowerment or independence. Quite to the reverse, Aouragh recalls that

---

94 Nick Rahimi and Bidyut Gupta, A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East, 69 EPIC SERIES IN COMPUTING 60–68, 63 (2020).
98 Tawil-Souri and Aouragh, op. cit., 113.
100 Clarno, op. cit., 159.
private investors such as PalNet had set-up [ISPs] and were offering Internet services even before PalTel coordinated the infrastructure. They were licensed by the Israeli civil administration, and tapping from Israeli IT companies. Thus, when the PA was installed after Oslo and PalTel was given telecom/infrastructure monopoly, the status of ISP companies like PalNet with license to roam via Israeli providers into the OT was unclear. [ … I]t soon became clear that ultimately, all providers (including PalTel) buy their Internet lines through Israeli companies like Bezeq. [ … ] The “occupied state” had to tap from its occupier in order to provide connection for what is still referred to as an independent communication infrastructure. It confirms that Palestinians were never offered real independence via Oslo [ … ]. The Palestinian ICT phenomenon confirms that an “artificial” peace sparked the uprising because many of the peaceful agreements led to further lack of Palestinian independence. [ … ] In other words, Palestinians developed a “survival economy.”

In truth, this is a long journey that started with Arafat assigning telecommunication services to multiple foreign companies at once, due to cross-checking paranoia arising from his mistrust for his own fellow Palestinians. Nevertheless, the takeaway point is that with the Oslo accords,

Parts of social and economic life that were formerly common, noncommodified, and largely outside the realm of control and surveillance were turned into private and surveillable possessions under a new property regime limiting free (meaning both sovereign and not paid for) mobility.

Beyond international agreements, the law plays a pivotal role in censoring Palestinians at the domestic level, too, exposing the precarious “sovereignty” of today’s Palestine. A wide array of Israeli laws are relevant to this effect, and while a thorough analyses thereof is unwarranted here, what matters the most for the sake of the present study is to emphasize how dependent those laws are on the constant rhetoric of threat, insecurity, and vulnerability that shaped Israel’s contemporary self-portrait. Surveillance extends far beyond the Internet and entails chilling effects of “self-censorship, including on the Internet, to avoid litigation” as provided in the Boycott Law. Chilling effect are indeed pervasive also offline, although the on/off distinction usually maintained in literature is nuanced by the fact that offline surveillance can trigger immediate reactions after being shared online In real time by the surveiling party with colluded authorities—not rarely in exchange for bribes.

101 Aouragh, op. cit., 55–57.
103 Tawil-Souri, op. cit., 30.
105 Ronald J. Deibert, John Gorham Palfrey, Rafael Rohozinski, and Jonathan L. Zittrain (eds), ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 305 (MIT Press, 2008); Clarno, op. cit., 160.
106 Stevens, op. cit.
It is when one considers Palestinian laws themselves, however, that the perverse legalistic effects of Palestine’s quasi-sovereignty as formalized subservience become strident. For instance, “the Palestinian Cybercrimes Law was referenced by several civil society organisations as the basis for arbitrary restrictions on the freedom of expression”\textsuperscript{109} in the context of the demonstrations that “took place in the West Bank on 13 June 2018 as part of the “Lift the Sanctions” campaign, organized by various Palestinian civil society actors calling for the lifting of the Palestinian Authority’s punitive measures on Gaza.”\textsuperscript{110} Interestingly, the offline tactics employed by the PA proved not dissimilar to—and at times equal to—those routinely resorted to by Israel, including the temporary searching of social media accounts and related extraction and/or removal of audiovisual content.\textsuperscript{111} Israel indeed avails itself of this on-spot “street form” of censorship as a complement to the one—significantly more sophisticated and large-scale, as also recounted by Cristiano\textsuperscript{112}—operated directly on the Internet and its (para-)corporate stakeholders. All in all,

From the controversial Israeli Facebook bill that facilitates the shutdown of Palestinian social media pages to legislation that criminalizes filming Israeli soldiers, the digital sphere is far from being a safe space for Palestinian free expression. With the issue of cybercrime law no. (16), a key concern has been the role it could play in deepening Israeli surveillance considering the PA’s widely controversial commitment to security coordination with Israeli security units. […] Despite amendments[,] several other concerns, highlighted in the original version law no. (16), related to excessive powers, and illegal collection of evidence remained unchanged in the 2018 law. Additionally, Article 40 in law no. (16) granting power to block websites remained as Article 39 in law no. (10).\textsuperscript{113}

The laws are obviously intertangled with—and somehow dependent on—the way the Internet functions from a more technical perspective, with captured policymakers serving exogenous interests by upholding seemingly technology-neutral stances that conceal, in fact, a precise political plan. Their choices pertain to the storage, intermediation, and transfer of data, ultimately questioning the meaning and extent of “data sovereignty” and its neo-colonialities, as investigated by critical-data-studies researchers belonging to, inter alia, the socio-technical systems theory, the critical theory of technology, and as—perhaps most famously—science and technology studies.\textsuperscript{114} Some of these are in fact critical legal scholars,\textsuperscript{115} not least from or focusing on the Middle East.\textsuperscript{116}

Even if one leaves the unaccountability of platforms’ servers situated within the U.S. jurisdiction and the potential complicity of their corporate owners with the U.S.

\textsuperscript{109}UN Human Rights Council, op. cit., para. 651.
\textsuperscript{110}Ibid., para. 646.
\textsuperscript{111}Ibid., para. 648.
\textsuperscript{112}Cristiano, op. cit., 258–260.
\textsuperscript{113}Ayad, op. cit., 4, 6.
\textsuperscript{115}Bertram Turner and Melanie G. Wiber, Legal Pluralism and Science and Technology Studies: Exploring Sources of the Legal Pluriverse, SCIENCE, TECHNOLOGY, & HUMAN VALUES (2022); Rocco Bellanova, Katja Lindskov Jacobsen, and Linda Monses, Taking the Trouble: Science, Technology and Security Studies, 8(2) CRITICAL STUDIES ON SECURITY 87–100 (2020).
government aside, a too-often-overlooked paradigm of neocoloniality lies with the actual functioning of the global Internet, which places them factually under U.S. law, too. While most scholarly literature has focused on the more exterior manifestations of the American influence on Israel’s telecommunications, only few works have examined the repercussions of U.S. hegemony over the global Internet on the narratives it construes about itself amid Palestinians. The United States has been deploying its online supremacy as yet another tool to segregate Palestinian voices and suppress dissent against Israel, not rarely assisted by “unaware” Palestinian authorities in accomplishing its intended results. Most of today’s global Internet communications are still routed through the United States because of the latter’s extensive cable and server infrastructure, which also means that U.S. authorities have enjoyed, over the last two decades, wide discretion in accessing sensitive data pertaining to Palestinians under the rubric of counterterrorism operations or general intelligence cooperation with Israel.

This data oversight was enabled by the technical functioning of the Internet, meaning it reflects not just Internet governance as a policy framework, but the nonhierarchical way the Internet works engineering-wise. The fact that the Internet channels communications through the most efficient route internationally rather than through the shortest or the domestic one, coupled with the quasi-legal intelligence prerogatives of the National Security Agency (NSA) and other Five-Eyes security agencies, makes it highly probable that most Palestinian communications at some point transit through cables the United States can assert jurisdiction over. Granted, data packets travel the Internet mostly encrypted, but this is no safeguard against lawless intrusion for all those world powers that enjoy the technical and political means to assert jurisdiction over Internet cables. In fact, [intelligence] agencies [...] have adopted a battery of methods in their systematic and ongoing assault on what they see as one of the biggest threats to their ability to access huge swathes of internet traffic—“the use of ubiquitous encryption across the internet”.

118 ten Oever, op. cit., 195.
119 The submarine telecom mapping executed by https://www.infrapedia.com/app shows two interesting facts: First, no Israel-departing cable looks eastward—they all traverse the Mediterranean and eventually reach the Atlantic—also through ring connections; second, the two cables owned by Egypt Telecom that could reach Gaza are regrettably truncated at the border. Apparently, British–U.S. surveillance of Palestine’s Internet previously occurred through a National Security Agency’s hotspot located in Cyprus [see Nicky Hager and Stefania Maurizi, Cyprus: The Home of British/American Internet Surveillance in the Middle East, L'ESPRESSO (2013), https://espresso.repubblica.it/inchioste/2013/11/04/news/the-history-of-british-intelligence-operations-in-cyprus-1.139978], which is indeed a convenient intermediary location also cable-wise. This is a credible claim not only because of the technicalities involved, but also as, regretably, such espionage operations would be anything but unprecedented. To exemplify, a GCHQ system code named Tempora provides access to over two hundred international fibre optic cables, intercepted where they come ashore at relay points in Britain and Oman. In 2012, data from up to forty-six cables could be actively processed at once, each providing ten gigabytes of data per second, and plans were in place to grow those figures. Tempora grants GCHQ access to a significant proportion of global internet traffic, automatically analysed and processed into a searchable form. The semantic content of intercepted material is stored for three days, and the metadata—the computer-generated data that enables digital communication to occur—is stored for thirty days. The NSA and other state agencies in the Five-Eyes alliance (comprising the US, UK, Canada, New Zealand, Australia) also conduct this type of upstream data collection at selected sites around the world. Each partner provides access to the data to the others, forming a global network of cable interception points.

Those methods include covert measures to ensure NSA control over setting of international encryption standards, the use of supercomputers to break encryption with “brute force,” and—the most closely guarded secret of all—collaboration with technology companies and internet service providers themselves. Through these covert partnerships, the agencies have inserted secret vulnerabilities—known as backdoors or trapdoors—into commercial encryption software.\(^\text{120}\)

Besides this, the United States operates at a quasi-governmental level, too, when public–private revolving doors and widespread regulatory capture afford governmental agencies the means to direct business decisions by tech giants like Google and, vice versa, the latter to shape the strategies and political priorities of the government.\(^\text{121}\) This sounds like a negligible, indirect process, yet its repercussions on Palestinians’ daily life, collective identity, and digital rights cannot be dismissed.

While the U.S. scrutiny over Palestinian communications as a form of secret diplomacy involving its closest ally in the Middle East (Israel) is mere speculation, the claim I am defending here is not that the scenarios illustrated in the preceding materialize for sure, but that they fall within the realm of the technically possible as well as of the politically plausible—which is problematic enough. Customarily, the enactment of data-localization requirements is employed by autocracies to keep controlling a state’s data “onshore,” but this does not necessarily circumvent the mechanism just described, as it speaks of where the data is ultimately stored, and not necessarily about its journey to get there. Furthermore, data localization is also used by autocratic regimes to spy on their “citizens,”\(^\text{122}\) but also by democracies supposedly to prevent cyber-enabled foreign espionage from occurring.\(^\text{123}\) Yet in this case Israel shows no apparent reluctance in having its Internet data stored in the United States; thus, not only are “the security-industrial complexes of Israel and the United States […] in the process of integrating seamlessly with the military-industrial complexes of those [states],”\(^\text{124}\) but Internet policing is following suit.

Internet governance is also involved in a still very much politicized but somewhat less technical sense, as far as public–private partnerships are concerned.\(^\text{125}\) These partnerships preside over the functioning of the Internet worldwide, with tensions arising from their inherently Western affiliations,\(^\text{126}\) which some may expect to go so far as to make them prone to hidden vetoes by the U.S. administration.

---


\(^\text{123}\) Sargsyan, op. cit., 2228–2229; Deibert and Pauly, op. cit., 84.

\(^\text{124}\) Graham, op. cit., 148–149.


Telecommunications networks and digital infrastructure regimes have become the lifeline of neoliberal globalization enforced by, e.g., the Internet Corporation for Assigned Names and Numbers [ICANN]. Like cyber Gods, these anonymous entities can [...] allocate URL names and addresses to some nations while precluding others, Palestine being a case in point [...] . New ICTs are thus protected through an inherited inequality between North and South.  

On another note, because shutting down only part of the network in times of emergency is technically unfeasible, the whole of the Internet is often characterized as “critical infrastructure,” placing it under regimes of executive exceptionalism even in times of peace—for example, in the United States and of course China. Data flows are, at any rate, impossible to control: The route that every bit of information takes to reach its addressee would be far too much for any administration to keep track of, even via artificial intelligence, which is why administrations prefer to operate at the sending and/or receiving ends, that is, at ISPs level. The latter can cooperate with governments not only in storing log data (metadata) and so on and in preventing access to certain websites (bandwidth capping), but also in downgrading the connection altogether (bandwidth throttling), so much so that forms of intermediary/vicarious liability could be hypothesized. In any case, what cannot be mistaken is that connection speed is always lower across Palestine compared to Israel, especially in Gaza. Filtering, which “typically utilises router-based IP blocking, proxy servers, and DNS redirection,” is also routinely used. Similarly, governments cooperate with messaging apps; this is a concrete problem insofar as these apps are often part of United States-based corporate conglomerates and digital ecosystems, as in the case of WhatsApp—widely used by Palestinians—being owned by Facebook.

Digital rights are also impacted by tangible measures immediately applied onto physical goods, and in this sense, within the context of Palestine generally, the situation in Gaza has been bearing, already prior to the 2023–2024 Hamas–Israel conflict, most of the hardest-to-solve complications. To frame the hurdles, a parallel may be drawn to the phenomena of “overt” and “hidden” hunger in the Palestinian territories, whereby

---


130 Hintz, op. cit., 358.


Palestinians’ segregation features a conjunction of both quantitative and qualitative elements, with the sufficiency of the former being used to dismiss concerns over the insufficiency of the latter. Far more frequently and severely, when compared to the West Bank’s inhabitants, Gaza’s ones are subjected to import/export restrictions and inspections, during which further surveillance hardware can be installed or countersurveillance software can be screened out by the Israeli authorities; additionally, Palestinian houses and workplaces are regularly demolished to free up space and “enhance security” for the illegal Israeli settlers, and in those occasions as well as at the borders, IT equipment easily gets either destroyed or confiscated—hard to tell which option is worse for Palestinians’ development and privacy. Import restrictions are also applied indirectly through taxation, which stands as tantamount to a nonphysical entry barrier due to increased costs disproportionately impacting the poor; fiscal losses to Palestine’s public budget due to Israeli constraints upon the Palestinian ICT sector shall also be noted. The legal argument one may advance is not that Israel—as a matter of IHL, which is the primary legal framework applicable to the OPT—is obliged to supply goods and services or even to allow them to independently thrive. Rather, the argument goes that confronting the specific long-standing circumstances of Palestine, the double applicability of IHR and IHRL is theoretically tenable as much as practically meaningful. As a matter of IHRL,

in certain circumstances corporations should be obligated to supply goods and services, at least when the affected population has no recourse to alternative venues by which to obtain such services or commercial goods. This situation may occur when (1) a corporation enjoys a monopoly over the supply of a certain good, inter alia, due to the home state’s exclusive control of trade with the host state (in the cases discussed in this article this monopoly is created through military and legal restrictions over trade with Gaza), or due to a specific corporation’s exclusive right to supply an essential good; or (2) when a corporation has control over [ … ] essential infrastructure.

The “hard components” of the Internet are, indeed, essential—or “critical,” as explained supra—infrastructure over which Israeli corporations exercise a de facto monopoly, and technological devices should be provided by Israeli companies insofar as it is made impossible for Palestinians to acquire them otherwise.

Interestingly, although the most elementary layers of censorship and surveillance may be circumvented relatively easily through rerouting (VPNs), anonymous communication (Tor), and browsing, as well as third-party-managed encryption services, widespread mistrust remains amid activists toward these forms of concealing, perceived to be

139Zureik 2016, op. cit., 208.
somewhat undignified and anyway “illegal” or untrustworthy, or however not in line with principles of openness, publicness, transparency, open resistance, and inclusivity that certain activist organizations cite as their flagship communication values. Despite the relative ease of access to and proficiency in such anonymizing technologies, the main problem does remain digital literacy. “Literacy,” in this sense, is far more than a technical skillset: It represents the socially encouraged access to a combination of hardware, software, human, and institutional support ultimately depending on the inheritance and perpetuation of politically sanctioned circumstances but also national imaginaries. Having said that, the activists’ attitude just described seems to stand in contradiction to another tendency that often manifests itself in contexts of privacy–power imbalance, namely, the so-called “privacy self-efficacy,” whereby

Obtaining desired results is more important than fully comprehending the underlying technical or legal contexts. While practical, this view also highlights a major constraint on users’ agency, as “doing without understanding” may reify existing power structures, likely reinforcing the relatively powerless status of already marginalized groups.

The mentioned view might also deepen a sense of fear and insecurity arising from the fact that one is not comfortable with being immersed in a reality for which the mechanisms are increasingly complex and technical, and for which the management is more and more outsourced to “experts” also identifiable as techno-extensions of politically motivated bureaucracies, whose “intimate desires” are ostensibly charged upon choices of otherness sold as specialist and thus techno-necessary and foundationally, uncontestably “true.” At other times, it is exactly the consummate understanding of technology, instead, that leads to suspicion, no matter how rumor-based it sounds; for instance, an allegation was circulated that “an Israeli company [wa]s lowering the price of navigation systems (GPS) in order to sell it to Palestinians and thereby increase their surveillance.”

Regulatory Implications for Social Media

While the Internet broadly understood is not the only technological or “mass media” device subjected to Israeli censorship (with TVs and radios regularly adhering to the same fate), social media are certainly more pervasive and impactful nowadays: “A qualitative difference between internet and other media forms are the participative elements provided to its consumers/users.” This helps explain why high degrees of actual or expected social-media censorship generate a subconscious sense of intellectual dependence on and complacency with the (actual or semi-imagined) censors. Although these

143 Cristiano, op. cit., 254–255.
144 Zureik, op. cit., 183.
147 Dmitry Epstein and Kelly Quinn, Markers of Online Privacy Marginalization: Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior, 6(2) Social Media + Society 1–13, 9 (2020).
148 Shalhoub-Kevorkian, op. cit., 66.
149 Aouragh, op. cit., 20.
dynamics are at play globally as “attention economy” and “surveillance capitalism.” What differs from other areas of the world is that Palestinians have to please multiple corporate and public actors at once, while managing to survive the intricacies of their daily struggle, also thanks to these very same platforms and devices. It seems increasingly obvious that America’s “woke capitalism” and Israel’s surveillance brutally coalesce in Palestine into a sinister market–security tandem.

The structural violence of this system is modeled, once again, on the apartheid precedent, whereby “the inferior” shall implore “the dominant” to be afforded a new technology or be granted their permission before installing or using their own. Curiously, some states in the region act upon offline but reportedly not online censoring policies, meaning for instance that Jordani citizens were operating online by a sort of self-restraint a couple of decades ago, and this unwritten social equilibrium might have consolidated over the years—a similar tacit pact seems to be alive and well complied with in Saudi Arabia and elsewhere in the Gulf. Conversely, others in the region, like Iran, have adopted a traditional censorship scheme at the major ISPs level.

Because real street-protests are consistently repressed with brutality in Palestine (not only by Israeli soldiers), social media have acquired the role of sites for popular contestation and for organizing and staging protests at least virtually, channeling the expression of political concerns both individually and collectively and aiding the recruiting of (often only virtual) fighters as well as the dissemination of political idea(l)s. Tawil-Souri and Aouragh famously termed this “Intifada 3.0,” as a follow-up to the two intifadas that had unfolded offline. More moderately, social media also serve the function of re-policing memory and of supporting pathos with logos, that is, narration as reasoned information without preset emotional overloading. Needless to remark, “undisciplining memory” is of poignant significance in Israel, and the law plays a pivotal role in delineating what falls within and outside the perimeter of the memory discipline. The Nakba Law offers a paradigmatic legislative instance to this effect:

It fines state-supported institutions that mark “Independence Day or the day of the establishment of the state as a day of mourning”. It is the Palestinians, who account for approximately 20 percent of the population, who mourn on Israeli Independence Day. When Israelis celebrate the War of Independence as a miraculous victory against all odds

---


156 Tawil-Souri and Aouragh, op. cit.


158 See Hitchcock, op. cit., 7.
that resulted in many casualties (1 percent of the population), Palestinians mark their loss in the 1948 war, which resulted in their massive displacement and dispossession, also known as al-Nakba. This is why the law intended to fine Palestinian commemoration is commonly known as “the Nakba Law.” Israelis and Palestinians commemorate the war through opposite national narratives. In the dominant Zionist narrative, it is similar to David’s miraculous victory over Goliath, who represents the Arab countries who fought alongside the Palestinians. However, the Palestinian national narrative construes the events of 1948 as a tragedy inflicted on unequipped and unprepared peasants who were betrayed by both Britain and the Arab countries and subjected to an organized campaign of ethnic cleansing by Israeli military forces.\(^{159}\)

The beneficial effect of digital rights as the enablers of repositories of memory seldom concretize, though. One reason for this is that Palestinians’ social-media resistance is increasingly concentrated onto a few platforms and, within them, a limited number of channels, which are thus easily monopolizable and manipulatable by infiltrated outsiders.\(^{160}\) This worsens with the curation of digital geographies\(^ {161}\) being pursued by content creators (platform users) only initially, while being subsequently influenced by “algorithmic allocation” (e.g., on what contents get more exposure to and thus higher engagement by and/or interaction with similar/uneven groups of users), which—even assuming algorithms have been coded “neutrally”—will take into account the strategies and preferences of the data colonizer, too.\(^ {162}\) Some strategies will “enter the code” by means of the data it is fed with, while others result from very basic marketing such as targeted advertising and search-result optimization. Some expressions of digital resistance elaborated by Palestinian young artists showcase artistic proficiency, but platforms are so rigged to favor the powerful and disfavor intellectual debate online that it should surprise no one if the “post-Oslo generation […] is disillusioned with existing political frameworks, in particular with that of post-Oslo state building, but also, to a certain extent, with a confined narrow conceptualization of resistance art.”\(^ {163}\)

All considered, social media in Palestine have functioned as a centralized echo chamber for Palestinian municipalities to spread the word around their “success stories,”\(^ {164}\) as much as a distracting tool crafted around addicting self-gratification, diversion, and escapism, particularly for the younger generations. Addiction arises from the precluded access to political engagement rather than to the availability of online channels for political expression, and findings to the reverse are contradictory as much as unpersuasive.\(^ {165}\) This sort of circensem


\(^{160}\)Halewa, op. cit., 9–10, 14.


\(^{164}\)Khalidi et al., op. cit., 49.

\(^{165}\)For the sake of exemplification, Tang et al. postulated two mutually exclusive conclusions. First, they found that people with more online exposure to movement-related information are more likely to have Internet addiction. The latter is positively related to depression. Then, stronger depression prompts stronger support for radical actions. Immediately after, they stated that online exposure to movement-related information relates positively to support for peaceful protests, but it has no relationship with support for radical actions. Gary Tang et al., *Politically Motivated Internet Addiction: Relationships among Online Information Exposure, Internet Addiction, FOMO, Psychological Well-Being, and Radicalism in Massive Political Turbulence*, 17(2) INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH 633, 11 (2020).
sine panem is alienatingly exemplified by “TEDxRamallah,” which was rightly identified as a meaningful act of United States-sponsored “hallucination of normalcy” in the West Bank. Not by accident, the political strategy pursued by the United States itself has been that of “removing” or “siding” the experience of alienation and frustration endured by young Palestinians in order to create a future cohort of more individualistic and Israel-friendly (or at least Israel-neutral) Arabs, leveraging on those younger generations’ biographical distance from the Israeli forced expropriation of their lands and, ultimately, of their culture as well as collective future. And yet this is the very strategy adopted by Palestinians leaders, too, who “sponsored ‘resistance culture’, on the one hand, and ‘normalized’ the very occupying power that was being resisted, on the other.” As social-media artistic creations can be equated to more traditional, “offline” forms of cultural resistance—or help circulate them—this normalization bears momentous implications for the Palestinians’ use of and trust in the Internet for said purposes. Content censorship implies that a potentially “dual-use” technology such as social-media platforms is only left with facetious cosmetics, and brought to Palestinian youth as politically disengaged, reflection-spared gaming. This feeds and worsens a spiral of betrayal, humiliation, and hopelessness both in the older generations—whose fight has ignited more violently because of their closer living proximation to the twentieth century’s forced displacement events—and in the younger ones as they mature and acknowledge the gamble that is being played on them. Indeed, automated news-making looks prima facie less biased than traditional centralized media, yet when the spell fades and young Palestinians realize the politically driven automation feeding their social-media profiles, and that such newsmaking can be manipulated and manipulative, their resentment and frustration erupt even more violently.

In asymmetric economies and societies, especially where fractions thereof are not premised upon the rule of law, the Internet becomes ipso facto a propaganda reinforcer. This is optimal for Israel in that the Israeli state, since its inception, has already been polishing up its propaganda channels through the so-called Hasbara (Hebrew: חסברה), in a systematic and systemic fashion, including by contracting copywriters dedicated to editing Wikipedia entries as to make Israel shine therein. Most recently, Twitter and Telegram have been inundated with propaganda by the Israeli government, which has been tolerated in its sharing of extremely violent and hateful content—content that, when coming from other governments or organizations, would have arguably been ex ante banned or ex post removed. And U.S. newspapers have been (or “felt”) encouraged to “disproportionately [emphasize] Israeli deaths in the conflict [and deploy] emotive language to describe the killings of Israelis, but not Palestinians.”

166 El-Khairy, op. cit., 154.
167 Ibid., 70.
Tellingly enough, it reads as if it was not violence comprehensively that needed to be countered online, but “incitement to hatred” only on the side of Palestinians: contrariwise, Israeli online violence is tolerated, as clarified by the way Facebook has handled both sides of the claim differently.¹⁷⁴ “Frustrated that Facebook was not cooperating satisfactorily, [Israeli] Public Security Minister Gilad Erdan appeared on television calling Facebook a ‘monster’ and said ‘some of the victims’ blood is on Zuckerberg’s hands’”¹⁷⁵—but according to him, that only worked for (the comparably very few) Israeli victims of “terrorist” attacks! All Palestinian civilians (including hundreds of children) who have perished out of clashes with Israeli settlers, occupiers, and soldiers as a follow-up to social-media incitement by Hebrew Israeli citizens matter nothing to their ill-intentioned minds.¹⁷⁶ Resultantly, I am unsure social media platforms are being mistrusted for “adopting content standards that are deemed either too restrictive or too permissive”¹⁷⁷ generally; it occurs to me they are rather criticized due to their double standards in enforcing whatever policy they adopt, not only when it comes to verifiable yet potentially dangerous and hatred-fueling information (like “incitement to violence” or “hate speech”¹⁷⁸), but also vis-à-vis the so-called “fake news”—which is almost never completely true or completely false, nor fully real or fully fake¹⁷⁹—and its legal consequences.

One party’s martyrs are the other party’s terrorists, but only the second narrative survives “moderation.” In this sense, even though the Internet is “simultaneously oppressive and progressive, enabling both domination and resistance,”¹⁸⁰ power asymmetry coupled with the specific infrastructural configuration of Palestine make it biased toward oppression. In fact, moderation biases trigger “feelings of alienation, frustration, and moral outrage within individuals and communities whose content is erroneously removed or restricted.”¹⁸¹ Differently from other states in the region, Israel does not consistently or proactively filter out Facebook et similia for Palestinians at the ISPs level¹⁸²; this is because rather than blocking these platforms per se (and being probably aware that these blockings can be circumvented with relative ease, as described earlier), it is resolute to turn them to its own propagandistic and selectively censorial advantage—this is a much smarter solution, indeed.

For Palestinians, social-media use often turns to a manifestation of their “home nostalgia,”¹⁸³ but on the negative, it is also felt as part of the Israeli project of “violently dismantling the urban, civil, and infrastructural foundation of the proto-Palestinian

¹⁷⁵Koslov, op. cit., 185, internal citations omitted.
¹⁷⁷Sander, op. cit., 956.
¹⁷⁸Ibid., 957.
¹⁸⁰Shalhoub-Kevorkian, op. cit., 56.
¹⁸¹Sander, op. cit., 958.
state”\textsuperscript{184}, indeed, large digital infrastructures play a semiotic function in the city and for democracy,\textsuperscript{185} just like nondigital ones with their presence in the urban texture. Poignantly, Israel is reiterating vis-à-vis “its” digital infrastructure in Palestine the same policies it applies to offline urban management there, starting with territorial balkanization and the consequent segregations of communities living thereupon, not to mention abusive colonial settlements, in what one might trace a parallelism between of\textit{life} and on\textit{life} planning of the social. “Palestine, as a nation in its abstract sense and as a territory more concretely, faces a form of colonial subjugation motivated by emptying the land of its inhabitants rather than ‘civilizing’ the people,”\textsuperscript{186} with predilection for the latter’s objective only when the first proves unattainable, or where Palestinians are vili\textit{fied} and dehumanized.\textsuperscript{187} The Internet plays a role toward both objectives, which reinforces the salience of conceiving the cyberspace as a territorially anchored dimension of the living, rather than as “ateritoriality” or anyway “else” from the physical territory.

In fact, far from being a borderless space, the “cyberspace” is bounded by technological infrastructure and the extractive dominion thereover.\textsuperscript{188} And the same fragmentation one can spot in the Palestinian territory—the infamous “archipelago of isolated enclosures”\textsuperscript{189}—is generated at the societal level, too, by means of extreme individualization. Does this choice owe to the most classic \textit{divide et impera},\textsuperscript{190} or does it also symbolize the will on the part of Palestinian authorities to attempt a less collective route toward emancipation? Encouraging individualization seems closer to a coherent project of subjugation, that is, to a politics of \textit{spacio-cide} that goes beyond \textit{urbicide} in that it systematically denies room (“space”) for demographic growth.\textsuperscript{191} Technology fits the mentioned project insofar as Internet (and ICT more generally) infrastructure is tied to a certain capacity preset by law that is never subsequently updated (e.g., through more bandwidth or frequency spectrum) in relation to the upscaling demographic needs of the local population.

Hereby the distinction between expressive and consequentialist law-acts gains momentum: The first are meant to express certain values at the time of drafting/enforcement, while the second might express those values in the future by originating a certain set of behaviors that were foreseen by the legislator. Consequentialist law-acts are also aimed at widespread receptions on the part of the targets, who will, in turn, express such values through their actions\textsuperscript{192}; these laws as perlocutionary acts easily end up bringing about humiliating objectification.\textsuperscript{193} Palestinians’ decolonial resistance against surveillance cannot be accurately understood through Western lawyering eyes, in that it is not (yet) based on an individual legal recourse whereby “reading the laws”

\textsuperscript{184}Stevens, op. cit., 14.
\textsuperscript{185}Bregje van Veelen et al., \textit{Intervention: Democratising Infrastructure}, 87 \textit{Political Geography} 102378, 2 (2021).
\textsuperscript{186}Tawil-Souri and Aouragh, op. cit., 104.
\textsuperscript{187}Cook, op. cit.
\textsuperscript{189}Clarno, op. cit., 163.
\textsuperscript{190}Graham, op. cit., 139–140.
\textsuperscript{193}Ibid., 396–397.
is a means for “knowing one’s privacy rights” in detail; instead, it has to be channeled through general change collectively and wider emancipation and awareness within society. Indeed, a nonnegligible percentage of Palestinians themselves prefer to connect their devices to the networks (unlawfully) made available by Israel to its settlers in the West Bank; this choice is performed to double detriment, to the market development of their own operators and to fellow Palestinians’ freedoms. This implies that higher awareness and collective ethics are warranted on the side of Palestinians, too, although younger generations seem more inclined to pay attention to these “conflicts of interests”; Hitchcock reports the interesting example of a schoolkid who charged Motorola for breaching their privacy by selling their personal data to Israeli authorities arguably in exchange for money or business favors and other facilitations.

The “Westernization” of the Palestinian ICT discourse is not warranted linguistically, either, although again, it is Palestinians themselves who lay the foundations for this to happen; as briefly touched upon by Shalhoub-Kevorkian, English is preferred as an idiom of emancipation and “transnationalist appeal,” even though not only Arabic texts are often machine-translated into English, feeding misunderstanding, but also English is the average language programmers of spying software are proficient in, so that the algorithms they code are primarily fed with English terminology. Last but truly not least in light of our discussion taken as a whole, English is the U.S. language, and most communications are routed through the United States and/or surveilled in cooperation with the Americans. In all probability, this is not the smartest way for sensitive topics to be discussed online in Palestine.

**Tentative Policy Proposals**

By way of assuming a minimal degree of good faith on the part of Israeli and Palestinian authorities alike, and keeping the former’s (more or less justified) ontological security anxieties in mind, one may formulate a number of suggestions. To begin with, what about turning Israeli cybersecurity assessments for new infrastructure into participatory projects including—to a certain extent, at least—Palestinians?

When it comes to social media, Facebook and similar corporations usually feel cornered also due to threatened or actual lawsuits from Global North firms, like those representing Israeli families claiming that Palestinians use Facebook to incite violence resulting in Israeli injuries; what about shielding Facebook et similia from these lawsuits, which resemble a paradoxical reversal of human-rights lawyers’ “impact litigation” strategy? As social media become a battleground for competing narratives, it seems necessary to ensure that preemptory silencing is not confined to litigation routes only available to the wealthy and dominant. Either litigation becomes affordable and practicable for all parties involved (which is unlikely, especially with reference to the burden

---

197 Shalhoub-Kevorkian, op. cit., 65.
of evidence gathering), or the law should abstain from restraining platform neutrality. This means shielding social-media platforms from frivolous lawsuits, but also ensuring that organizations are not themselves targeted for what they write therein via overbroad communication clauses of “security” statutes. For instance, in the United States,

One of the world’s oldest Zionist organisations with close ties to the Israeli government, the Jewish National Fund (JNF), is using American anti-terrorism laws to sue [ … ] the US Campaign for Palestinian Rights, a coalition of groups seeking to end the decades-long occupation of East Jerusalem and the West Bank.189

Corporations’ positioning is a complex balancing affair. With regard to the most recent atrocities in the 2023 Israel–Hamas war, it was noted that “Some companies have been criticised for ‘picking a side’; others condemned for their silence.”200 One solution could be to ensure that on the one hand, social-media and content-sharing platforms like Facebook, Instagram, Twitter, YouTube, and TikTok actually enforce their proclaimed neutrality201 (including by preventing algorithmic “shadowbanning”202), while on the other, “silencing lawsuits” are by-default dismissed. Ultimately, it would be on the courts to establish where the threshold lies for characterizing a lawsuit as “silencing”; while specific content shared by and against specific individuals might prove more open to contestation,203 an immediate connection to extremely recent events involving large fractions of systematically abused populations and long-standing group political claims should definitely be a warning sign that the lawsuit displays a preemptive character.

On a related note, this essay has described a tangled situation where a public actor (the state of Israel, primarily) is interfacing with private ones like Facebook. It seems unreasonable, or at least premature, to expect Facebook to hold itself publicly accountable on the contents it removes; also, it can hardly be compelled to endure such accountability. However, while Facebook acts discretionally to remove whatever it pleases (also confidentially), the counterpart (removal-requesting party) is public, and therefore one way forward could be that most—if not all—requests forwarded to Facebook be published on institutional websites; this could be done perhaps without specifying any motivation (which might include sensitive security data or state secrets, classified information, etc.) but still showing the name, date, and content of the posts for which removal is sought. Other scholars advised on publishing any agreement between private platforms and Israel,204 which unfortunately seems unlikely to happen anytime soon because even assuming such agreements can be produced as formal documents, Israel would never agree to publish them out of reasonable fears of (further) major blows to its international reputation. Despite exceptional contrary examples

204Taha, op. cit., 9.
retrievable from the United States, it is also unreasonable to expect companies themselves to publish governmental requests to access data—that might even be unlawful if they are covered by executive privilege. Eventually, governments should publish, if not requests to access data, at least those to eliminate posts that are not under criminal investigation. Alternatively, requests to social media should be submitted under judicial oversight—according to the U.S. Department of State and Sander, currently they often are not—or perhaps even a bipartisan Israeli–Palestinian committee—no matter how unrealistic this might sound at this turn of history. This is not the same as to suggest—as the International Bank for Reconstruction and Development inexplicably did—any strengthening of shared or jointly operated networks between the two sides.

One more policy proposal is that content moderation should be grounded on actual content as opposed to who is it that posts or shares it; this solution will prove algorithmically harder to encode, but also fairer and neutral to all parties involved. In other words, social-media and content-sharing platforms are advised against removing contents or users based on state-backed listing of organizations as “terrorist” and alike, and states should refrain from legislating in such a way to force them to do so. Indeed, as difficult as it might prove for some of us to accept, “terrorism” probably stands as the most controversial term of contemporary times in policy and adjudication, and those who are labeled as “terrorists” by one state might legitimately be considered “freedom fighters” by another, so that content moderation should never turn into organization moderation. Hateful and violence-inciting content could still be removed, but not depending on whether those who are posting it are legitimized or blacklisted by the public authorities of a specific state (or group of states). Unsurprisingly, this issue has gained momentum during the latest “digital confrontations” accompanying the Israel–Hamas war, where Facebook, YouTube and TikTok have banned Hamas content altogether, Twitter has largely “failed” to enforce its own ban, and Telegram has generally allowed Hamas-produced or Hamas-distributed content to circulate. Curiously enough, in an unprecedented move, the European Commission zealously probed (and stopped advertising on) Twitter under the EU’s Digital Services Act for the sharing of “misleading” (understood as Israel-critical) information on the conflict, as if Twitter had never allowed the sharing of equally “misleading” information against Palestinians over the previous months and years. It is not for this article to decide whether Hamas or any other organization should be listed as “terrorist” while others are not, but it

208International Bank for Reconstruction and Development, op. cit., 44.
seems fair to advise that in this context, certain Hamas contents could be removed based on the content itself, rather than due to the organization being listed as “terrorist” by specific states. Indeed, the very same organization, including Hamas, could be considered “terrorist” or “freedom-fighting” not just by different populations, but by different states, too. It is precisely in light of sovereignty on infrastructure issues that we should tie content moderation to the content itself, as opposed to the public “affiliation,” “recognition,” or “accreditation” of those creating, posting, and sharing such content; the risk in doing otherwise would be to tie content moderation to (contented) sovereignty as opposed to message merit. Put differently, the risk is that territories and populations relying on “less sovereign” Internet infrastructure will need to concede more to the content-moderation preferences of third parties, that is, “more sovereign” states on whose infrastructure their own infrastructure partly depends—and on their most influential technology and “security” providers. Although content moderation policies based on organizations’ public status inevitably promote inter-state conflict about who is censored and who is not, status-neutral moderation would arguably help attenuate (justification for) Internet fragmentation along regional, sociocultural, sectarian, and ideological lines—especially between “the West” and “the Rest.”

One more content-moderation related policy observation, as a partial caveat to the preceding, is due. Upon invading Gaza in October 2023, the Israel Defense Forces (IDF) and even some Israeli ministries were allowed to freely post and “tweet” videos of and written/oral commentaries to alleged war crimes, in order to steer internal political propaganda. This is widely documented, most comprehensively within South Africa’s submission to the ICJ. Platforms generally acquiesced to it under the argument that those acts were committed (and narrated) by the “official” representatives of a

---


---


“regular” army of a “legitimate” state actor. Some of these contents would have plausibly not survived the scrutiny of a merit-based content-moderation policy. Yet a potential “conflict of interests” shall be acknowledged with evidence-gathering and fact-finding: To complement the risky fieldwork of journalists and grassroot human-rights movements, it is precisely thanks to such a “generous” IDF posting that the international community could gather verifiable evidence of Israeli alleged crimes. This “open-source” evidence can be later tendered to the International Criminal Court and similar criminal tribunals, or even reported, as it happened indeed, within submissions to the ICJ. This is to say that, in some way, content moderation on Israel would have restrained the world’s ability to take cognizance of the extremely questionable modes (if perhaps not rules) of engagement operated by the IDF. An inherent tension exists between moderating content for preventative purposes and obtaining potential evidence of war crimes, and while “merit-based” moderation can help soothe the resentment, hatred, and violence, as well as prevent emulation acts and radicalization on all sides, it could also hinder the acquisition of open-source evidence of state-backed crimes (including their most invaluable “intent” component, as in the case of genocide allegations). The balance to be sought is a difficult (and probably context-sensitive) one, and can only be addressed in another article.

Alongside content moderation, statecraft, traditional and business diplomacy, technology transfer, development cooperation, and humanitarian assistance also cover essential functions. “E-infrastructure” diversification thanks to development cooperation with other geopolitical players is praiseworthy, although one should be reminded that mentioned e-infrastructure usually refers to web portals and so on, rather than to the Internet’s “hard infrastructure” built on cables, access points, and servers. Other actions in the field manifest in the form of institutional “study visits” to, for example, the European Union (EU), which can do fairly little to help Palestinians in loco, although is admittedly valuable as far as academic collegiality and, to an extent, e-government are concerned. One closing comment is perhaps of convenience. The EU noted that in Palestine,


216 For instance, the European Commission’s Proposal for a Council [of the EU’s] Decision on the Union position within the Joint Committee established by the Euro-Mediterranean Interim Association Agreement on Trade and Co-operation between the European Community, of the one part, and the Palestine Liberation Organisation (PLO) for the benefit of the Palestinian Authority (PA) of the West Bank and the Gaza Strip, of the other part, with regard to the adoption of a Recommendation on the implementation of the EU-PA ENP Action Plan, COM(2012) 748 final, 2012/0346 (NLE), paras. 119–120 (12 December 2012).


neither the Basic Law\textsuperscript{219} nor other laws establish the process through which policies are formulated and laws are prepared within the government and sent for approval either through the regular procedure or the extraordinary one. Thus, laws tend to be drafted without a specific guiding policy and in the context of institutional competition. In the absence of a set legislative procedure within the government, regulatory impact assessments are not conducted, legislative policy memoranda are scarce, while inter-institutional consultations are inadequate and are not part of a general development vision regulated through annual legislative plans. [...] As a result, ad hoc committees are regularly set up to work on legislation, whether focusing on specific laws (e.g. committees for the amendments of the Judicial Authority Law and the cyber-crime law) or on the harmonisation with international human rights treaties.\textsuperscript{220}

Because most needs and emotions of the population are canalized through the Internet today, this is too important a policy area for being left to faceless committees with no accountability to the citizenry, which also remove from impact assessments—even if they were transparently conducted—any political bearing. This implies, inter alia, that any serious commitment to lasting peace, being it through a one-state or two-states solution, will need to account for either a shared Internet infrastructure that works alike for all parties, or a separate infrastructure for each state where none of the two technically depends on the other.

**Conclusion**

The United States retains its role as the by far most powerful and controversial international player in the Israeli–Palestinian chessboard. In most recent years, its influence extended from altering Palestinian priorities in response to the Arab Spring(s), to mediating normalization processes between Israel and Sunni regional actors with no reference to Palestine. Furthermore, its intelligence agencies cooperate with Israel on regional cyberdeterrence\textsuperscript{221} and on all major “counterterrorism” dossiers impacting Palestinians’ life, a significant number thereof pertaining to the policing of the Internet across Gaza and the West Bank. As if these regulatory and technological exchanges did not suffice, Israel controls some of the key ISPs that serve(d) Palestinians, especially in Gaza; hence, it can easily compel those ISPs to filter information as to perform as propaganda reinforcers to the U.S. benefit.

Moreover, the United States is where most Internet data from and to Palestine transits and can thus be asserted jurisdiction over and surveiled with scant judicial or even political accountability. Far from being speculative, this argument stands as politically reasonable and technically attainable because of the several verified instances of information censorship operated upon instructions by government-tied U.S. corporations, especially during confrontational seasons. Worryingly, Palestinian authorities themselves contribute to creating information clusters and

\textsuperscript{219} That is, a sort of Constitution for the State of Palestine, just like those in force in the People’s Republic of China’s two Special Administrative Regions (SARs) of Hong Kong and Macao.


\textsuperscript{221} Beatrice Gori, From Kinetic to Cyber Attacks and Back: The Israeli Approach to Deterrence in Cyberspace and the Multi-Dimensional Threat of Hamas, Research Paper, Center for Cyber Security and International Relations Studies at the University of Florence, 12–13 (2022).
identity bubbles, with infrastructural deficiencies as well as executive and court orders undermining freedom of expression online and prohibiting access to certain websites under the usual vague, meaningless aegis of “public morals” or “security” concerns.

The combined effect of these deliberate and casual informational biases, supported by an unanticipated convergence of interests between West Bank and Israeli authorities in restricting online access and freedom of expression, is aiding the United States to maintain its tech-savvy hegemony in the region not simply through diplomatic and military means, but equally rhetoric-wise, on the more normative side. This interrogates the current trends of capitalism-powered regulatory capture that, far from standing as an exclusively Western problem, influence Palestinians’ rights on an everyday basis. The policy proposals outlined in the preceding might embody a first step toward Palestinians’ emancipation from Israeli–U.S. surveillance and censorship online. However, their success is contingent on scholarly and policymaking communities realizing that unless the infrastructure is uncaptured from foreign jurisdictional assertions and the primacy of unaccountable corporations, any efforts on the legal side will be frustrated by the current technical design of Internet networks—in Palestine and beyond.

While this research has situated its research questions within the specific complexity of Palestine, their broader significance warrants further research in multiple directions. The most obvious is the effect of military occupation, techno-enabled neocolonial regimes, and power asymmetries in contexts of “borderline statehood” onto the governance of Internet infrastructure and, as a reflection thereof, online content, information flows, and perception management. Relatedly, studies are called for with respect to the relationship between online and offline “networked élites,” insofar as the Internet reshapes the functioning of networks of clientelism and capture without, however, fundamentally altering the inequality divides that characterize structural subalternity at the group and national level, that is, the ability to capture lawmaking processes and exercise hegemony. Finally, the perennial regulatory question of how to properly embed these transformations within “fairer” legal regimes “by design” is probably worth continued asking. The law’s ineptitude toward abandoning old-fashioned dichotomies (starting with the public/private dichotomy) shall be overcome if people are to preserve the conviction (or perhaps the illusion) that the complexity of technologically enabled framings of social reality can find in the law a source of order as safety and emancipation, as opposed to order as stagnation and oppression.

Acknowledgments

An earlier draft of the present work was presented at the Workshop on “Algorithmic and Technological Modes of In-/Exclusion – International Legal Method and Critique” organised at Utrecht University Law School by the ESIL Interest Group on International Law and Technology on 31 August 2022, during the ESIL Annual Conference 2022. The author would like to acknowledge insights from the workshop panelists and attendees, and in particular from the paper discussant Dr. Roxana Vatanparast.
Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Riccardo Vecellio Segate [ ] http://orcid.org/0000-0001-5385-4948