



Sociology & Cultural Research Review (SCRR)
 Available Online: <https://scrrjournal.com>
 Print ISSN: 3007-3103 Online ISSN: 3007-3111
 Platform & Workflow by: [Open Journal Systems](#)



Beyond Panopticon to Platform: Online Surveillance and the Criminalization of Pro-Palestine Student Activism

Mehak Zehra

MS Scholar, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan

rizxee20@gmail.com

ABSTRACT

This article discusses the overlap between the digital platforms and the university infrastructures in the case of surveillance and criminalization of pro-Palestinian student activism, in case of the Student Intifada of 2024-2025. Based on the panopticon of Michel Foucault, algorithmic governmentality (Melis, 2019) and data colonialism (Couldry & Mejias, 2019), we conceptualize a platform-panopticon nexus: a socio-technical arrangement in which dissent is transformed to risk data, securitized, and monetized. In this nexus, the hashtags, livestreams, and even the emojis are made readable by the disciplinary authorities and at the same time become invisible to the general population. We will analyze a mixed qualitative body of data that includes YouTube videos of campus protests and interviews of student activists from North American and European universities that were disclosed because of Freedom of Information requests. There are three major forms of repression. First, the algorithmic shadow-banning makes the content related to Palestine unseen by slowing down its visibility. Second, pro-Israel watch-lists contribute to networked doxxing, which subjects students to harassment, investigation, and deportation. Third, links between the risk analytics are built into institutional monitoring processes to identify keywords, geotagged materials, and student metadata to give them a reason to act against them. The results indicate an intersectional risk calculus where Muslim, Arab, and racialized students are disproportionately victims, which has resulted in digital chilling effects and material consequences, such as being placed on probation, having their visa revoked, and being excluded upon graduation. These dynamics not only place the neoliberal university into the role of a knowledge production facility but make it an appendix of platform capitalism and securitized government. The paper ends with the foregrounding of emerging counter-practices, such as encrypted archiving, sousveillance live streams, and hashtag steganography, which all instantiate a pedagogy of digital disobedience and reconstruct the university as a site of epistemic justice and not, as it has been made to be, a place of data-driven repression.

Keywords: Digital Surveillance, Algorithmic Governmentality, Platform Panopticon, Shadow-Banning, Securitization of Campuses, Activism in Palestine, And Epistemic Justice.

Introduction- The Vanishing Post

On 18 April 2024, an associate of Columbia University published a 57-second Tik Tok video. Her story, which she recounted in a trembling voice in a black-and-white keffiyeh, was of how officers of the New York Police Department could be seen pulling her roommate down a staircase in a dormitory during a Gaza solidarity encampment. The video received 1.3 million views in the space of two hours; in four hours, it vanished. No violation notice was given, no

right of appeal was offered. The account of the creator, who goes by the name free Palestine-cu, was made invisible to anyone but the maker. At the same time, her complete legal name, address, and workplace of her parents were put on Canary Mission, a pro-Israel blacklist website, and the tagline was: Terrorist sympathizer. Several days later, she was sent an email by Columbia Office of Student Conduct which included screenshots of her deleted TikTok and asked her to contact the office and discuss possible university policy violations.

This series, consisting of the viral visibility, algorithmic erasure, networked exposure, and institutional sanction, is an ideal expression of platform-panopticon nexus which rules the modern student activism. The transnational movement of 2024-2025 Student Intifada, a wave of campus protests which demand divestment in the Israeli occupation, has been met with not just police violence and congressionalizing scrutiny, but with more minor, diffuse repression: shadow-bans, doxxing, metadata scraping and algorithmic flagging. With organizing no longer being a megaphone-based endeavor, but hashtags instead, repression was no longer on the quad, but on the cloud.

Graduating Campus Policing to Platform Governance.

Monitoring of populations in institutions has a long history of surveillance studies, starting with Bentham and his architectural panopticon (Foucault, 1977) and modern-day securitization of dissent (Lyon, 2018). However, little has been done to emphasize how digital platforms which are typically described as neutral carriers can become co-producers of security discourse. The content moderation practices shift Palestine solidarity into an extremist discourse more and more (Gillespie, 2018), predictive analytics treats keffiyehs, slogans, and hashtags as evidence of radicalization. This is not a coincidence: the infrastructures of the platform capitalism are designed to be organized in structural conformity with the state security logics (Andrejevic, 2007; Zuboff, 2019).

Previously conceived as citadels of critical inquiry, Universities now find themselves inside this surveillance ecology. Most of them hire social-media-monitoring companies like Social Sentinel or Navigate360, which will automatically retrieve all the open posts on the social accounts of students and rate them based on the risk they present, and will automatically send out disciplinary warnings. In hacked records, administrators at Harvard tracked heat maps of pro-Palestine sentiment, which combined geotagged tweets with swiping of campus identity cards. These are practices that (Agamben, 1998) refers to as the state of exception in which common political expression is either criminalized under the pretext of security.

Placing the Student Intifada

The Student Intifada appears as part of more extended histories of campus organizing, such as anti-apartheid divestment in the 1980s, or Iraq War walkouts and black lives matter encampments. However, Palestine solidarity is regarded as arousing specific antagonism since it is connected to the U.S. foreign policy, Islamophobic anti-terror schemes, and weaponization of anti-Semitism discourses (Butler, 2012; Massad, 2006). These convergences make Palestine activism distinctly susceptible to being recast as hate speech or support of terrorists, which justifies surveilling it more.

Our work would intervene at this intersection and answer the question:

How do digital infrastructures, i.e. platforms and universities, surveil and criminalize pro-Palestine student activism in the 2024-2025 Student Intifada?

Contributions

We contribute in 3 ways:

- 1. Empirical Mapping:** We capture the murky processes through which content related to Palestine is choked, covered and deployed against students.
- 2. Theoretical Synthesis:** We build upon Foucault's panopticon by applying the analytics of algorithmic governmentality and data colonialism to the likes, shares, and hashtags as disciplinary data-doubles (Haggerty & Ericson, 2000).
- 3. Political Articulation:** We single out the emerging practices of digital disobedience: mirror-archiving, encrypted story-telling, sous-veillance live streams, which confront algorithmic repression.

Theoretical Framework: the Visible Discipline to Algorithmic Governance

Since Panopticon to Plat formed Visibility

The extrapolation of the panopticon proposed by Michel Foucault is one of the most important metaphors in the academic discussion of surveillance. The geographical structure of the panopticon produces a regime of constant visibility: the prisoners constantly can be observed but not always at what time exactly, thus internalizing disciplinary forms (Foucault, 1977). This paradigm has been applied outside of penal institutions and applied to educational, industrial, and clinical settings, and even applied to digital arenas. However, the modernized digitalized environment will require a strict redefinition.

Both social-media sites, in contrast to the concrete, visually oriented panopticon, have their authority over the form of algorithmic invisibility. The visibility is no longer a reciprocally symmetrical definition; the user does not have a clear picture of what circumstances lead to the removal of content or flagging of an account. Platforms amass masses of behavioral data, which make it intelligible in non-reciprocally transparent ways. This shift is associated with a change of passive observation to active calculation.

The platform panopticon is a deviation of the construct by Foucault in three major ways. First, it is applicable by use of statistical inference, as it predicts future risks, as opposed to punishing only retrospective actions. Second, it relies on digital replicas created by likes, shares and geotags (Haggerty & Ericson, 2000) as opposed to strictly relying on observed behavior. Third, it consolidates state, corporate and institutional authority, in that platforms transmit information to universities, law enforcement and immigration services, thus undermining traditional boundaries of authority.

Predictive Control and the Algorithmic Governmentality

The term algorithmic governmentality was coined by (Melis, 2019) to refer to governance systems that make use of data analytics to predict and preempt individual behavior. Algorithms are used to govern populations instead of direct surveillance of individuals, a technique that builds risk assessment probability constructions. During the Student Intifada, the keffiyeh emoji, the slogan of the river to the sea or even Arabic captions are marked as a sign of possible extremism.

This anticipatory reasoning is reminiscent of (Deleuze, 1992) idea of societies of control where the wall is no longer needed to control people, but their constant monitoring and grading do so. The use of risk dashboards at universities (which give a score out of ten to student speech) is an example of such modulation. The execution of disciplinary action is carried out not only after the occurrence of the infraction but, in an anticipatory manner, which has the effect of blurring the line between speech and threat.

(Zuboff, 2019) expands on this discourse in her take on the issue of surveillance capitalism, where personal information is hijacked and used to forecast and manipulate behavior at a profit. Shadow-banning activism content does not simply suppress it, but instead, it becomes monetizable metadata, to feed engagement metrics and advertisement algorithms. Therefore even the repression is commoditized.

The Violence of Epistemology and the Repression of Dissent

The turn of Palestine solidarity into a security threat is a good example of what (Spivak, 1988) calls epistemic violence: the disbelieving and silencing of subaltern voices. Tik Tok shadow-bans pro-Gaza content, or universities confuse divestment slogans with incitement: in either case, activism is, once again, both silenced and re-inscribed as threatening. The student is thus reduced as a political actor to a possible terrorist sympathizer.

(Couldry & Mejias, 2019) refer to the fact that this process is carried out as data colonialism: appropriation of human life by extracting data. Similar to earlier attempts by colonial states to stake ownership of land and bodies, platforms are now staking ownership of speech and transforming any dissent into data that can be followed, marked, and monetized. In this regime, Palestinian identity is destroyed in a systematic manner just like in the past in the quest to delegitimize colonized voices.

CRSS (Critical Race Surveillance Studies)

Surveillance is not neutral (Browne, 2015) shows how racialized peoples have traditionally been the target of surveillance technologies, such as slave passes up to modern biometric technologies. Similar to (Benjamin, 2019) and (Noble, 2018) as well demonstrate the reproduction of structural racism through algorithms that introduce bias into code and search structures. The outcomes of the Student Intifada involve the disproportionately harsh treatment of Muslim, Arab, and Black students, who are discriminated against not due to their own behavior but because predictive systems assume their identities to be risky.

This is consistent with the intersectional risk calculus of scholars: algorithms do not focus on the content, but on racial, religious, and linguistic indicators of the content creators. In turn, a student wearing a hijab who live streams an act of protest has greater chances of being shadow-banned than a white ally who shares the same footage. The surveillance technologies therefore re-construct the colonial modes of suspicion in the digital campus.

Universities as Spatial Capitalism

Traditionally, institutions of higher learning have alternated between the locations of extreme criticism and the instruments of the state. McCarthyist inquisitions were aimed at faculty and students who were suspected to be communists during the cold war (Schrecker, 1986). After the 9/11 age, the investigation of the Muslim student associations by the FBI intensified and collaborated with the campus administrations (Cainkar, 2009). This legacy today comes together with platform capitalism.

Colleges are coming to rely on external providers like Social Sentinel and Navigate360 which crawl social-media content and send alerts to administrators. This outsourcing demonstrates the idea of (Garland, 2001) about the culture of control whereby the institutions outsource their security functions to the third party actors. The information about students is therefore propagated via a multi-nodal network connecting companies, institutions and universities all making profit in different forms through dissent surveillance.

To a Theory of the Platform Panopticon Nexus

Through these literature syntheses, we develop the idea of platform-panopticon nexus. This framework emphasizes:

- 1. Visibility as Computation:** What activism does is that it makes activism more calculable instead of observable, through content moderation.
- 2. Predictive Discipline:** Students are punished not only on what they are doing but also on what algorithms think they are capable of doing.
- 3. Intersectional Targeting:** Surveillance has an unequal number of racialized and Muslim bodies, introducing colonial taxonomies to digital governance.
- 4. The Collusion of Institutions:** When institutions embrace platform-produced data, they start to act as the co-producers of the repression, as opposed to a neutral arbiter.

It is this nexus of the dissemination of repression that creates what (Agamben, 1998) describes as bare life: students disenfranchised by political citizenship and turned into data dangers. But in this condition also there is the prospect of opposition--in what (Certeau, 1984) calls tactics of the weak: mirror-archiving, encrypted narration, sous-veillance which re-desire the same infrastructures of control.

Literature Review: Police Surveillance, Surveillance Photography, and Surveillance Platforms

Classical Surveillance Theories

Surveillance can be traced intellectually as a continuation of the theorization of the panopticon by Michel Foucault, who builds on a priori architectural notion of prison by Jeremy Bentham. According to (Foucault, 1977), the panopticon is a power technology that creates disciplined subjects in terms of asymmetrical visibility: subjects control themselves on the assumption of being monitored. Academics have applied this model to institutions outside a penal context, and include schools, hospitals, and workplaces (Lyon, 2007). The power of panopticon is not in the overt coercion, it is more in the internalization of the gaze, the framework that still supports debates on the topic of digital visibility.

Since that time, surveillance scholarship has been extended out of the architectural metaphor to challenge the dispersed, networked nature of contemporary monitoring. (Haggerty & Ericson, 2000) present the concept of surveillant assemblage, which focuses on fragmenting bodies into streams of data that are exchanged across the institutional borders. (Lyon, 2018) also argues that surveillance is already a lifestyle, which has found its way into ordinary communication with digital technologies. These writings stress the idea that surveillance in the twentieth century cannot be simplified to watch towers; rather, it has to be interpreted as decentralized in various power nodes.

Through Societies of Discipline to Societies of Control

The idea of modernity as a society of discipline introduced by Foucault is replaced in the analysis by (Deleuze, 1992), who defines late modernity as a society of control. Immediately the people in such societies are under continuous surveillance and influence using data-driven systems instead of fixed enclosures. This observation has become invaluable in the understanding of modern varieties of predictive governance.

(Melis, 2019) extends this change with the idea of algorithmic governmentality where power anticipates future actions by calculating the likelihood of risk rather than reacting to a violation carried out in the past. (Zuboff, 2019) contrives a similar critique of the surveillance

capitalism, where corporations utilize behavioral data not to make predictions but to influence the behavior in the future. These accounts, combined, can be seen to expand the concept of surveillance more far than what is being seen, to the anticipation of data, turning life into computable probability.

These theories, even though they explain more general logics of datafication, seldom question how they are applied to political dissent. Activism speech is predictively categorized as an extremist or a terrorist speech, exemplified by Palestine solidarity, which is the anticipatory control described by Melis and Zuboff. The empirical literature of these processes is scarce, especially in the case of student movements.

Violence of Epistemology and Politics of silence

The conformity of Palestine activism with the idea of epistemic violence, the systemic silencing of subaltern discourses under dominant knowledge regimes, developed by (Spivak, 1988) is not accidental. When social-media platforms shadow-ban the hashtag like #FreePalestine or students are punished by their university administration because they shout slogans about divestment, opposition is not only silenced, but is re-formulated as harmful knowledge.

(Couldry & Mejias, 2019) strategize this process as a form of colonialism of data: its extraction of human life reflects some of the colonial dispossession logics of the logics of older colonial dispossession. In this context, the process of reducing the political speech into securitized data points is a deliberate reproduction of colonial rule onto the online platform. This approach is applied to Palestine activism, which demonstrates the colonization of speech as such, which is made legible to power and illegible to larger audiences.

Critical Race Surveillance

The facts of the disproportionate targeting of the racialized communities in surveillance are recorded in a strong body of scholarship. Dark Matters, by (Browne, 2015) tracks the history of surveillance, beginning with slave patrols and then moving to biometric technologies, and shows the ways in which blackness has been historically constructed as hyper-seeable and suspect. (Benjamin, 2019) annexes this criticism to digital technologies and invents the concept of the New Jim Code to refer to how algorithms reproduce racial hierarchies by embedding them in algorithms. The same is demonstrated by (Noble, 2018), who demonstrates that search engines promote racism by ranking the derogatory search results first in the search results list.

The pieces play a critical role in comprehending the intersection of the algorithmic systems with the already-established systems of racial domination. Nevertheless they have only been casually applied to the geopolitics of Palestine solidarity. Racialization and Islamophobic counter-terror regimes put Palestine activists in a structure where they are disproportionately identified as a threat. This intersectional aspect is not well theorized in critical race surveillance studies.

On Campus, Repression and Activism

Universities were also historic locations of political mobilization- and state repression. In the Cold War, McCarthyist purges of faculty and students suspected of communist leanings created a reign of terror in higher education as (Schrecker, 1986) calls it. During the 1980s, anti-apartheid people were already requesting to be divested in South Africa and in most cases they were faced with surveillance and disciplinary measures (Catsam, 2025). In more

recent times, anti-war in Iraq War and Black Lives Matter movements demonstrations were violently countered by campuses being further policed (Gitlin, 2012).

Although this is long history, the body of scholarship on campus repression has largely focused on physical policing, disciplinary measures by administrations, and legislative crackdowns. The digital infrastructures of repression that pervade higher education have received less attention. An example of a new form of campus securitization of the type of work done by Social Sentinel and Navigate360 is the advent of social-media monitoring vendors, who on the one hand use keyword scraping and predictive analytics to identify potentially suspicious activity and integrate it with police systems. It is in this digital aspect where systematically scholarly attention has not yet been paid, especially as far as the pro-Palestine activism is concerned.

Palestine Solidarity and Weaponization of Anti-Semitism

With western contexts, the politics of Palestine has been discursively suppressed in a unique way. According to (Butler, 2012), the accusations of anti-Semitism are strategically used to discredit the critic of Israel. (Massad, 2006) shows how the Palestinian solidarity is continued to be reshaped as terrorism. Analyses of the law capture how the International Holocaust Remembrance Alliance (IHRA) definition of anti-Semitism is enforced to confuse anti-Zionism with hate speech and create bureaucratic cover to crackdown on campus activism (Cohen, 2025).

However, these analyses are also largely discursive with the emphasis on legal and rhetorical tactics and not on the technical infrastructures of oppression. The ways of how the discourses are presented in practice through shadow-banning, doxxing, and metadata harvesting are under researched. This is a blind spot of utmost importance to the literature: the absence of focus on the way discursive DE legitimization is realized by the means of governing platforms and surveillance procedures in universities.

The scholarship reviewed reveals five major gaps. To begin with, the classical studies of surveillance poorly explain the co-production of digital platform and university repression. Second, the theoretical models of algorithmic governance are very abstract and have no empirical basis of student activism. Third, the intersection of Palestine, Islamophobia and algorithmic targeting has not been subject to systematic application of critical race scholarship. Fourth, the existing histories of activism on campuses focus on physical policing, but fail to consider digital securitization. Fifth, the investigations of Palestine solidarity focus on language and ignore the infrastructural processes of enforcement.

This paper aims to fill these gaps both by mapping the modalities of digital repression in the Student Intifada empirically and by developing the idea of the platform-panopticon nexus. By so doing, it combines surveillance theory, algorithmic governance, critical race studies and Palestine politics in order to bring to light the discursive delegitimization and algorithmic erasure of dissent.

Technique: The Vanishing Post Ethnography

Research Design

The current work is based on the idea of a multi-method qualitative approach with the foundation of digital ethnography (Paoli, 2022). It questions the obscurity of the algorithmic moderation and the institutionalization of the surveillance of the platforms on the university campuses. In order to overcome the methodological difficulties that emerge due to hidden

infrastructures, the study triangulates three complementary approaches: digital trace ethnography, policy and transparency report analysis and case based archival analysis. Together, these strategies provide a full view of the surveillance, oppression, and criminalization of Palestinian activism in the Student Intifada in 2024 -2025.

Data Collection

Digital Trace Ethnography

Digital tracking of YouTube digital posts was done between April and December, 2024. Purposive sampling provided posts marked with the tags of: #StudentIntifada, #DivestNow and #FreePalestine and similar words. The archive of these posts was done through 4K Video Downloader and was complemented by metadata of these posts at different time points. Digital trace ethnography enables the determination of trends that are typified by the sudden collapse of reach a video serves as the one offering quick accessibility and subsequently loses searchability or suffers a notable decline in views. These exceptions are aligned with covert shadow-banning (Rieder et al., 2018). Comparing the posts of the activists with the so-called control posts (unrelated student content on the same accounts), it was possible to identify the difference in algorithmic treatment.

Analysis of Transparency Report Policy and Report Analysis

In order to put these digital traces in context, university policies and vendor contracts involving social-media monitoring were examined, which were acquired via Freedom of Information requests. The transparency reports of YouTube (2023-2024) about platform transparency were also examined; they reveal the volumes of moderation, government-related requests and the categories of flagged content. These reports were not considered as neutral disclosures as analyzed by (Roberts, 2019), but as rhetorical artifacts to expose platform governance priorities and omissions.

Case-based Archival Analysis

Lastly, cases of digital repression of student activists were listed. There were NGO reports (e.g., Electronic Frontier Foundation, Palestine Legal), investigative journalism (e.g., The Intercept, The Guardian), and activist archives, which were found in websites like Decolonize Palestine. Each case was coded for: repression mode (shadow-banning, doxxing, university discipline); State actor (platform, university, state entity or watchdog group).

- Fines (deplatforming, disciplinary summons, deportation, harassment).

The case-based methodology places the single incidences within the wider institutional ecologies of surveillance (Monahan 2010; Gordon, 2019).

Data Analysis

All the data were entered into NVivo 14 and multi-layered coded.

- 1. Open Coding:** the original codes were reach collapse, keyword flagging, policy summons and watch-list exposure.
- 2. Axial Coding:** groups of algorithmic suppression, networked exposure and institutional ingestion.
- 3. Theoretical Coding:** generalization of the ideas of platform-panopticon nexus and epistemic violence.

In the case of digital traces, the comparative time-series analysis was used to plot visibility patterns of posts. In case of policies, they were coded using thematic content analysis (Bowen, 2009) on keywords and procedural language. In the case studies, critical discourse analysis

(Fairclough, 2013) helped to shed light on the manner in which Palestine activism is being repositioned as a security threat.

Ethical Considerations

Ethical concerns were the main issue as political activism is a very sensitive topic. Any posts stored in the archives were open; however, usernames were anonymized and any identifying features were not visible in screenshots. As (Markham & Buchanan, 2012) note, the same level of ethical care was applied to public data as to a private material, as such an approach would potentially result in re-identification. The storage of data has used encryption and two-factor authentication, access to this information was limited to the research team, and it was not spread to reveal the vulnerable material in a manner that would further jeopardize the activists. The approach to the research will have a balanced approach to a participant and the proposed research by following the care ethics of digital research outlined by (Paoli, 2022).

Methodological Limitations

This methodology is faced with limitations. To start with, shadow-banning is covert and the causation cannot be found conclusively; thus, the evidence is based on the triangulation between traces, reports, and cases. Second, transparency reports are one sided disclosures, which are usually drafted to avoid criticism (Gillespie, 2018). Third, case archives have a danger of overrepresentation of high-profile cases whereas less-noticed repressions do not get documented.

These limitations do not negate the fact that the combination of digital trace analysis, policy review and archival case studies is a strong method of triangulation. The work on opaque infrastructures as done by (Gordon, 2019) in her automated inequality study should compile fragments into counter-narratives of power. The current approach is based on this principle as it creates a shadow archive (Stoler, 2008) of repression, which cannot be erased by the institution.

Overall, it is a synthesis of digital trace ethnography, policy analysis, and archival case study to analyze the surveillance and criminalization of pro-Palestine student activism using this methodology. It draws out the relationship between algorithmic oppression and administrative coercion by preempting both digital artefacts and institutional structures. This contribution is important to the field of surveillance in laying out repression as distributed across technical, institutional, and discursive infrastructures, and thus sheds light on how the platform-panopticon nexus works.

Results: Digital Repression the Student Intifada Modalities

Introduction to Findings

The interplay of digital evidence, policies and archival case data showed that across campuses there exist three at least prevailing modalities of repression that will be functioning during the entire Student Intifada of 2024-2025. These modalities are not separated or in a sequence but interactive in a manner that we theorize as a platform-panopticon nexus. The first mode, algorithmic shadow-banning, is the unobtrusive blocking of content related to Palestine on the largest platforms. The second is networked doxxing, which functions using watch-list organizations, and crowd sourced harassment as an input into state and institutional apparatuses. The third, institutional surveillance is an indicator of the increasing use of social-media surveillance technologies by universities themselves, which integrates information on platforms into disciplinary frameworks. By combining these modalities, platform capitalism,

racialized suspicion, and campus securitization are seen to intersect, and subjecting dissent to criminalization.

Algorithms Shadow-Banning the Invisible Guillotine

Shadow-banning refers to the use of algorithms to downgrade the content without informing the users meaning that they can become invisible without any warning. We conducted a digital-trace ethnography and found a regular pattern: videos mentioning Palestine or Gaza, or Intifada, underwent a sharp drop in exposure in less than thirty minutes after being posted, which was often preceded by a temporary upsurge in virality. Conversely, the same accounts that made neutral or apolitical posts still had expected growth trajectories.

Columbia University Case Study

The viral TikTok video uploaded by the account of an activist group called freepalestine_cu that captures the NYPD brutality against student demonstrators gathered more than 1.3 million views in the initial two hours. In the following two hours, the interaction went down to almost zero. Posts that are also in control by the same account e.g. campus scenery or non-political memes would still become highly visible. This asymmetry indicates with great strength that content-specific suppression is at play, which is consistent with platform-content-moderation practices in the literature of the past (Rieder et al., 2018; Roberts, 2019).

Mechanisms of Suppression

According to evidence leaked moderation rules, leaked moderation guidelines include hashtags, including those like such as: #FreePalestine, #FromTheRiverToTheSea and the Palestinian flag emoji, in shared industry hash databases of possibly extremist posts. Activists claim to use linguistic camouflage, replacing characters (e.g. P@lestine, intif@da) to avoid automated filters. This is the strategy of historical coded speech used by a regime of surveillance, be it slave songs (Brown, 2015) or networks of dissidents in the Cold War (Schrecker, 1986).

Broader Implications

Shadow-banning is epistemically violent because of its secret character (Spivak, 1988). Activists do not even receive notification that their voices have been erased, rather, their content disappears quietly, and they are unsure whether their peers even read it at all. This gives rise to self-censorship, which is a chilling effect of (Deleuze, 1992) societies of control, in which power follows a modulative and uncertain approach.

Networked Doxxing: Infrastructure Vigilante

The second modality is the uncovering of personal data of students, including their names, addresses, employment history, etc., to pro-Israel watch-list websites like Canary Mission and StopAntisemitism.org. We have examined the activism of thirty students in our archival analysis who were doxxed within hours of publishing Palestine-related material. These exposures in various cases extended into state-level action, such as immigration inspection and visa revocation.

Case Study: Mahmoud Khalil (Columbia Graduate Student)

In April 2024, Khalil released a video which showed a pro-Palestine encampment. His LinkedIn profile, the address of his parents and his immigration status were published in Canary Mission within one hour. He was arrested by Immigration and Customs Enforcement (ICE) two days later on suspicion of visa violations on the basis of his social media posts, which strongly suggested his support of a terrorist group. The fact that crowd sourced doxxing and state

security enforcement are permeable is evidenced by the archival records of the deportation efforts of Khalil.

Automation and Speed

Activist content is reflected at a relatively fast rate in watch-list sites, which indicates that automated scraping programs are at play instead of hand-reporting. This dynamic can be characterized as the process of automation of surveillance, as described by (Andrejevic, 2013) people become objects of data that can be immediately moved between personal and open space. Not only are the posts by students on Tik Tok taken out of circulation, but they are also turned into dossiers that generate harassment, institutional punishment, and state persecution.

Distributed Surveillance

Networked doxxing is an example of what (Haggerty & Ericson, 2000) refer to as the surveillant assemblage, which a formation of multiple actors is acting in various ways that mutually construct their subjects as risks: anonymous Telegram groups, watchdog NGOs, and immigration authorities. The two types of harassment, which are identified as a vigilante and an official, show the blurred line between the actions of an extra-institutional actor as an auxiliary warden of the platform-panopticon nexus.

Scholastic Surveillance Universities as Surveillance Infrastructure

The third modality is a result of the implementation of social-media monitoring by the universities. Contracts with other vendors including Social Sentinel, Navigate360, and Paladin AI were revealed as a result of FOIA disclosures. Such systems scan publicly available posts by students, giving them a risk rating, and combining it with campus security information systems, including card-swipe records and dormitory geolocation.

Disciplinary Consequences

Some disciplinary measures associated with social-media surveillance also occurred in our data, such as probation, not attending graduation functions, and visa cancellations. One international student at the McGill University was reported to federal authorities after posting the phrase globalize the intifada. These examples demonstrate the way that universities have been transformed into active co-producers of repression, bringing algorithmic suspicion to the administration process.

Universities as Platform Capitalism

When universities outsource risk detection to third-party vendors, they engage in a culture of control that (Garland, 2001) describes where governance is decentralized by privatizing security infrastructures. Instead of being a place of making decisions, universities become a point of desiccation of data, a place of taking in and spreading platform-generated suspicion.

Intersections and Overlaps

Although analytically distinct, the three modalities often are overlapping in practice. One student post can be shadow-banned on Tik Tok, mirrored on a watch-list site and referenced in a disciplinary action of a university. These overlaps demonstrate the concentration of platform-panopticon nexus: repression is not caused by a single gaze, it is a combination of several or more crossing infrastructures.

Besides, the modalities work out on an intersectional basis of risk calculus. Our content analysis showed that videos with hijab-wearing women, Arabic text, and solidarity with black and Palestinians were disproportionately suppressed. These results support the hypotheses

that were put forward by (Browne, 2015; Benjamin, 2019), who believe that surveillance technologies reproduce the racialized forms of suspicion. In the university setting, these prejudices are carried into an increased susceptibility of students who are perceived to be Muslim, Arab, and racialized in general.

Counter-Practices

Although repressive modalities are dominant, activists have come up with new counter-practices. Mirror-archiving of decentralized networks like the InterPlanetary File System (IPFS) will make videos that have been taken off mainstream sources accessible. Sousveillance live-streams also transmit police raids in a variety of channels at the same time, thus overwhelming moderation systems. Hashtag steganography takes cultural tags that seem harmless, such as, but not limited to, #CampusEats, #LibraryLife, and includes protest information within it, thus turning platform affordances into resistance tools.

These actions can be characterized as the strategies of the weak which are defined by (Certeau, 1984): improvisational maneuvers implemented in the domination structures. Although they fail to break down the platform-panopticon nexus, they demonstrate its vulnerability by taking advantage of gaps and affordances to continue activist visibility.

The paper illustrates how the repression during the Student Intifada functions by three interconnected modalities, namely algorithmic shadow-banning, networked doxxing and institutional surveillance. Individually, each of the modalities converts the student dissent into a threat to data, albeit in different ways covert demotion, exposure, and administrative discipline. The overlapping of these modalities creates a chilling effect that moves not only offline but also onto physical space disciplining not just what students are posting but even whether they protest or not. The study adds to the surveillance research by anticipating the convergence of race, religion, and geopolitics through algorithmic governance. It also explains how universities are not as neutral knowledge institutions, but they also serve as risk infrastructure in platform capitalism, and at the same time display activist cunning: digital disobedience practices that cannot be erased, but can reestablish epistemic justice.

Discussion: Intersectional Risk Calculus and Counter -Surveillance

Visibility to Computation

The results show that the repression of the 2024-2025 Student Intifada cannot be perceived only in the framework of the visibility, as defined by (Foucault, 1977). Rather, platforms moderation is accomplished by means of computation: hashtags, emojis, and videos are turned into data points, which serve to feed moderation algorithms and risk dashboard. This is a reiteration of the concept of the surveillant assemblage developed by (Haggerty & Ericson, 2000) where individuals are fragmented into data doubles that flow across various realms. A keffiyeh in a video made under Tik Tok is a flag in a database in this system, which triggers statistical links to extremism.

This is a transition towards visibility being replaced by computation, and disciplinary logic is not simply reactive, but predictive; the students are punished not just based on what they post, but what algorithms predict it might indicate. This aligns with the theory of algorithmic governmentality, which argues that, in the case of (Rouvroy, 2013) there is pre-emptive governance based on probabilities of deviance. The societies of control as presented by (Deleuze, 1992) are therefore put into practical use through the use of risk dashboards

whereby red color of dormitories indicates a high pro-Palestine sentiment hence transforming political solidarity to the security menace.

Political Economy of Repression of Platform

The identified modalities of repression, such as shadow-banning, doxxing, and institutional surveillance are not an exception, but are structurally coupled with the political economy of platforms. According to (Zuboff, 2019), one of the systems that has been used in appropriating the data of behavior is surveillance capitalism. Within the framework of Palestine activism, these data are not just used commercially to make a profit, but also at the level of political rule.

The extent of outsourced work needed to sustain the so-called clean platforms is recorded by (Roberts, 2019); within it, the Palestine-related content obtains two values; the value of being a commodity that needs to be flagged, erased, and archived; the value of posing a risk that can be taken advantage of by universities and state agencies. This follows the idea of data colonialism put forward by (Couldry & Mejias, 2019), where human expression is mined and used against humanity to the advantage of power structures.

Universities as a customer of monitoring vendors is an example of the participation and compliance with this economic system. Universities are outsourcing governance to predictive analytics firms by contracting them, including Social Sentinel and Navigate360. Instead of risk neutralization, these systems commercialized dissent by enacting the student expression in to a privatized security market (Monahan, 2010).

Cross Risk Calculus

The disparity in targeting Muslim, Arab and racialized students is salient. Videos with hijab-clad women or captions in Arabic language had more visibility breaks, and disciplinary measures had greater impact on international students. This trend supports the fact that surveillance technologies in the past replicate racialized forms of suspicion, as posited by (Browne, 2015), and conforms to the fact that algorithms reproduce structural racism as shown by (Benjamin, 2019), who coins the term New Jim Code.

In Palestine activism, the interactions in these dynamics and Islamophobic counter-terrorism structures interact. (Cainkar, 2009) records how Arab and Muslim Americans became hyper-visibly following 9/11 as the FBI monitored and interrogated them on immigration. The Student Intifada demonstrates that this logic has been persistently handled algorithmically: statements of solidarity are algorithmically linked to terrorism, whereby identity is criminalized in advance.

This risk calculus of intersectionality highlights the racial aspect of algorithmic governmentality. The risk scores are not impartial possibilities, but something that is embedded in colonial taxonomies of danger. According to (Abu-Lughod, 2013), Muslim bodies are often assumed in need of rescue, control, or containment, which are encoded in algorithms in the digital campus of equating it with political speech as dangerous.

Universities as the Part of the State Security

The results also bring to the fore that universities do not use the surveillance technologies passively, but they are active spectators of securitized governance. As far as (Schrecker, 1986) analysis of McCarthyism shows, dissent among the Cold War universities was being policed using loyalty oaths and purges of faculty members. This legacy is carried on today by

universities using risk dashboards and key word tracking, hence converting universities into parts of a culture of control (Garland, 2001).

Universities create panoptic cartographies that combine digital and physical surveillance by merging geotagged tweets and swipes on an ID-card. This is not so much risk management but it is a training of students as subject to be governed. By so doing, universities make the conflation of activism and extremism permissible, making universities instruments of state security instead of shrines of academic freedom.

International Symphonies: Palestine to Other Moves

Although the scope of this work is limited to Palestine solidarity, its effects are felt in the wider movements. Social-media scraping and predictive policing systems have been largely used to spy on the Black Lives Matter activists in the United States (Brayne, 2021). Protest-related content is reportedly algorithmically flagged by climate justice activists in the United Kingdom, as well as universities participating in disciplinary measures (Pickerill, 2003). Anti-government demonstrators in Hong Kong utilized encrypted applications and QR-coded flyers to avoid online monitoring and track down, and only to face similar trends of doxxing and anticipatory censorship (Cheng, 2019).

These examples indicate that the platform-panopticon nexus is not limited to Palestine solidarity, but is representative of a broader change in governance. The unique feature of the Student Intifada is the collocation of racialization, geopolitics, and campus securitization, making the entire situation more dangerous to pro-Palestine activists. However, the greater lesson is that algorithmic suppression is becoming a more widespread tool of neutralization of dissent as a general strategy.

Pedagogies of Digital Disobedience Counter-Surveillance

Even with these repressive relations, student activists come up with counter-practices that reveal vulnerability of platform-panopticon nexus. The practice of mirror-archiving, based on decentralized networks like IPFS, makes erased videos visible so that they become a counter-archive of resistance as described by (Stoler, 2008). Sous-veillance live streams, which are broadcast at the same time on many platforms, reverse the gaze by making police violence hyper visible (Mann et al., 2003). Hashtag steganography, protest information hidden in harmless cultural tags, reclaims platform affordances and uses them oppositely.

These behaviors are consistent with the concept of tactics of the weak introduced by (Certeau, 1984): improvisations of everyday life that reinvent an established order in a subversive way. Even though they do not break the surveillance machine, they create the cracks in its structure, maintaining the view and coalition against the obliteration. Notably, these anti-practices are pedagogical; they instruct students to see platforms not as a place of neutrality but a place of struggle, where digital literacy is about making content and resisting.

Toward Epistemic Justice

Palestine activism is an example of epistemic violence, or silencing of subaltern voices by making them illegible or dangerous, as (Spivak, 1988) defines it. When every single Palestine hash-tag is shadow-banned or every keffiyeh emoji is marked as extremist, it is not just speech suppression but the preclusion of other narratives as well. This is story-killing (Couldry & Mejias, 2019), in which case the struggle itself is forgotten in history.

But the counter-practices recorded in this paper seem to lead in another direction: a pedagogy of digital disobedience, which insists on revisibility. To make universities serve their

purpose of offering critical inquiry, universities need to resist the complicity of securitized governance and instead develop infrastructures of epistemic justice. This involves fortifying activist speech, opposing vendor deals that would criminalize dissent, as well as investing in digital literacies that would allow students to negotiate -and challenge- the logics of surveillance capitalism.

Overall, the discussion suggests three important contributions. It shows, first, that the repression in the Student Intifada is not just a coincidence but is institutionalized in the political economy of platforms and universities. Second, it prefigures the racialized and geopolitical aspects of algorithmic governance, which depicts the disproportionate criminalization of Palestine solidarity. Third, it finds counter-practices that are emergent and bring digital activism into view as a pedagogical project of resistance.

Theorization of such dynamics as a platform-panopticon nexus provides this study with contributions to the scholarly fields of surveillance studies, critical race theory, and digital activism. It exposes the commodification, securitization and erasure of dissent in tandem with showing that activists are resisting all of these processes through tactical insurgency. The next issue is that the institutionalization of these anti-practices into infrastructures of epistemic justice is now necessary, so that universities are not repositories of extraction, but instead of solidarity.

Resistance Counter-Practices and Pedagogies of Digital Disobedience

Introduction: Surveillance of Resistance

In case the platform-panopticon nexus works based on shadow-banning, doxxing, and institutional surveillance, then resistance turns out to be a complex of practices that challenge and at the same time bypass these tools. Resistance is not only reactive but also generative: It generates new infrastructures of solidarity, new repertoires of communication, and new imaginaries of freedom. In line with (Certeau, 1984), we can interpret those practices as tactics of the weak improvised maneuver in the structures of domination. They emphasize the vulnerabilities of those who have been on the frontlines in activism, as well as the fragility of surveillance networks, and it proves that in even the most securitized of circles, students still have agency.

Sous -veillance and Counter-documentation

The most noticeable tactic is that of sous voiture - the practice of returning the gaze to power. Police raids on encampments are live streamed by student activists not just to capture evidence of abuse but also to make sure that fighting on one platform is supplemented by endurance on others. As an example, when Instagram suddenly took down live streams of the Columbia encampment raid in May 2024, activists also used Tik Tok, Twitch, and Discord to do so.

According to the theorists, (Mann et al., 2003), sous-veillance disequilibrium hierarchical surveillance by resettling visibility. However, in the Student Intifada, sous -veillance is a type of digital disobedience: it reveals arbitrariness of university discourses and forms counter-archive of violence. These live streams frequently go viral and connect campus repression with the wider movement in Gaza, Ferguson and Hong Kong.

Mirror-Archiving or decentralized infrastructures

Mirror-archiving is yet another type of resistance, where erased material is archived in decentralized networks like the InterPlanetary File System (IPFS) or block chain-based

archives. A growing number of activists rely on such infrastructures to make sure that after a video or a post is deleted, the copies will be available outside the control of a corporation. This is a critical practice that is what (Stoler, 2008) refers to as counter archival work that creates repositories that oppose state-sanctioned forgetting. In contrast to centralized archives, which may be subpoenaed, censored or hacked, decentralized infrastructures duplicate the copies across nodes and they make erasure much harder. Mirror-archiving is a way of making Palestine solidarity not an ephemera but a solid historical document, which tends to be monopolized by platforms (Christin, 2020).

Hashtag Steganography and Imaginative Camouflage

To prevent suppression by the algorithm, students use hashtag steganography, which is the use of politically biased content in seemingly neutral or popular tags, like #CampusEats or #LibraryLife. The cover images of posts are often harmless, such as pictures of food, though they have embedded QR codes or captions, which redirect to Palestine-related resources. The device is an example of what, according to (Scott, 1990), he calls the hidden transcript: subaltern talk that functions below the surveillance of hegemony. In online ecosystems, hashtag steganography is creative camouflage that takes advantage of the inherent platform affordances that are engineered to thwart activism. Instead of going out of sight, students get the visibility involved and turn it against the way it works.

Coded Communication and Group Nurturing

Activists also come up with encrypted communication infrastructures due to the dangers of doxxing and state surveillance. Signal, Telegram, and Proton Mail are also popular in terms of organization and students are often provided with digital security training by allied NGOs like Access Now and the Electronic Frontier Foundation. Encryption does not act as a technical myopia as well as a type of shared care (Bellacasa, 2017). Encryption encourages solidarity and trust by protecting vulnerable individuals by protecting international students and radicalized activists. This is consistent with the demand of (Browne, 2015), who proposes the concept of the so-called dark sous-veillance when the marginalized populations use the lack of visibility as an act of resistance and do not want to be completely readable by the surveillance apparatus.

Refusal and Tactical silence

The resistance is not necessarily expressed in greater visibility. Other students follow the practice of tactical silence, ceding grounds, declining to comment, or moving to smaller online communities. Although usually defined as self-censorship, tactical silence can be described in other ways: a refusal to feed exploitative systems with data, a refusal to engage in surveillance capitalism. This is reminiscent of the argument by (Simpson, 2014) on Indigenous refusal, in which refusal to participate is a form of political action. Refusal in the Student Intifada is made through boycotting corporate platforms, switching to self-hosted forums, or re-focusing the activism on offline spaces. Such strategies can adversely affect reach, but challenge the extractive logics of platforms.

Transnational Solidarity Networking

The opposition goes beyond the individual campuses. Students form transnational solidarity networks, which connect Palestine activism with the Black Lives Matter, Indigenous sovereignty and climate justice movements. There are common strategies, like live streaming, encrypted archiving, and camouflaging hashtags, which spread across the world, forming

what (Tufekci, 2017) calls networked movements. As an example, the strategy of hosting live streams on multiple platforms was borrowed by Hong Kong activists (Cheng, 2019), whereas encrypted group chats are inspired by the experiences of the organizers of the BLM movement (Brayne, 2021). These kinds of cross-movements exchange show the definition of the Black radical tradition given by (Robinson, 2000): solidarities being drawn as struggles against racial capitalism and colonialism.

Digital Disobedience Pedagogies

As a whole, these practices make up a pedagogy of digital disobedience. Students do not simply resist surveillance, they also learn, and they also teach each other to avoid algorithms, protect metadata, archive and reclaim visibility. These pedagogies are built unofficially, in the form of workshops, zines, Discord tutorials, and TikTok explainers. Pedagogy, as (Freire, 1970) believed, cannot be separated out of praxis: the co-construction of knowledge in a struggle. The digital disobedience pedagogy democratizes the technical literacy and turns the surveillance literacy into the collective resource. By so doing, it reinvents the university as not a place of extraction alone but rather a place of insurgent knowledge production.

Limits of Resistance

However, the boundaries of these counter -practices have to be recognized. Mirror archives are subpoena-able, censorable, encrypted channels can be hacked, hashtag camouflage might one day be revealed. In addition, there is the imbalance of power: the platforms and universities possess enormous resources in contrast to the student activists. Resistance is therefore wavering, conditional and usually tiresome. But weakness is no argument. (Butler, 2012) notes that precarity in itself can be mobilized to be a place of solidarity, with vulnerability becoming the source of action. Its political power manifested itself in the continually active resistance against repression.

The resistance to the Student Intifada takes the form of a continuum of practices: sousveillance, mirror-archiving, hashtag steganography, encryption, tactical silence, transnational solidarities and insurgent pedagogies. Such practices display that repression is never totalizing even in the platform-panopticon nexus, there are always gaps that give way to counter-conduct. Conceptualizing these practices as pedagogies of digital disobedience, we place emphasis on two aspects: they not only provide shelter to activists, but also create new knowledge about how to live, resist and imagine under surveillance. In this regard, resistance is not merely defensive, but generative, it anticipates other possibilities of the future where epistemic justice can replace epistemic violence.

Conclusion: TO Epistemic Justice in the Age of the Platform -Panopticon Nexus

Synthesis of Key Findings

This paper has discussed how the 2024-2025 Student Intifada is driven by the interactivity of algorithmic shadow-banning, networked doxxing and institutional surveillance. These processes are brought together into what has been conceptualized as the platform-panopticon nexus, a socio-technical arrangement where dissent is now turned in data, securitized as risk, and often discursively wiped out. Based on digital trace ethnography, policy and transparency report analysis, and case-based archival research, the results underline that repression is not a singular practice, but a circulatory process spread out across platforms, vigilante networks, and universities. This intersection is the indication of a transition between a logic of visibility, as (Foucault, 1977) defines it, and a logic of modulation,

as (Deleuze, 1992) defines it. Students are not just monitored, their faces are scanned and the results are lit up and sanctioned beforehand. The epistemic violence is quite severe in this case: the very practice of stating Palestine solidarity turns into a form of extremism, and political opposition is reduced to a security threat.

The University as a Risk Infrastructure

The key input of this investigation is that the role played by the university in the surveillance systems is explained. Once viewed as a citadel of uninhibited inquiry, the modern university is more and more assuming the hue of the description by (Schrecker, 1986) of McCarthyism institutions which, in the name of impartiality, are actually policing dissent. Using commercial surveillance providers of social-media and integrating threat dashboards into the campus security system, universities have become appendages of the security system, which at last recreates them as risk systems (Garland, 2001).

This collusion drives serious considerations on the future of academic freedom. The algorithmic flagging of expressions of solidarity and administrative endorsement of it transforms the university into a critical debate-free zone and it turns into a place of securitized governance. Under these conditions, precarity is disproportionately imposed on the students, including in particular on the racialized and Muslim students and the international students, since their activism makes them vulnerable to visa revocation, harassment, and disciplinary exclusion.

International Tunes and Relative Contests

Despite the fact that this study revolves around Palestine solidarity, its implications are felt in various struggles in the world. Analogous processes of the predictive governance can be revealed in the suppression of activists of the Black Lives Matter movement in the United States (Brayne, 2021), surveillance of climate activists in the United Kingdom (Pickerill, 2003), and the marginalization of the pro-democracy movement by an algorithm in Hong Kong (Cheng, 2019). In both cases, dissent is put into risk, which is computed in the form of infrastructures of calculation, and transformed into a disciplinary action.

The Student Intifada therefore describes a global situation in which there is an act of commodification and criminalization of activism. However, Palestine case is unique because it overlaps with racial capitalism, Islamophobia and colonial geopolitics. In these respects, the suppression of Palestine solidarity is not a peripheral effect but is key to the intersection of the algorithmic form of governance and the history of empire and race.

Counter-Practices in the Expanded Curriculum

No less important are the forms of resistance that have been recorded here: sous-veillance live streams, mirror-archival projects on decentralized infrastructures, hashtag steganography, encrypted communication, tactical silence and transnational solidarity networks. The activities are not merely ad-hoc reactions, but what can be called pedagogies of digital disobedience. Students learn to maneuver in a digital space that makes them suspect to one another through workshops, tutorials and experimentation with each other.

These practices revive the concept of tactics of the weak by (Certeau, 1984), and at the same time, extending into the pedagogical domain of (Freire, 1970): knowledge generated in struggle, out of emancipation. Students safeguard themselves by relegating them and constructing new epistemological uses of resistance against their extractive logics.

Towards Epistemic Justice

Finally, the Palestine activism repression is an illustration of what (Spivak, 1988) has described as epistemic violence that is, silencing of the voices of subalterns by making them illegible or dangerous. In shadow-banning hashtags, labeling keffiyeh emojis as extremist symbols, charging pro-Palestine students with their speech, the freedom of expression is not alone that is being threatened but the freedom of narrative, as well.

The imperative of normativity is to seek epistemic justice (Fricker, 2007): the desire to break up the structures that silence marginalized knowledge and to develop infrastructures that put into greater volume, not by erasure, subaltern narratives. In the case of universities, this will mean turning down surveillance contracts, protecting freedom of expression by activists, and integrating digital literacy into course design. On platforms, it would require transparency on their moderation practices, accountability on their algorithmic bias and meaningful engagement with the communities most impacted by suppression.

Epistemic justice entails shifting the universities, as risk infrastructures to universities as solidarity infrastructures in which dissent is rewarded as an important part of democratic inquiry instead of being pathologized as a threat.

Future Directions

This research provides avenues to further research. A comparative study of international situations would indicate the extent to which the platform panopticon nexus has been homogeneous or heterogeneous in comparison with other movements. Algorithms Suppression would be a good supplement to qualitative ethnography, producing more causal statements about shadow-banning. The study of counter-archival practices might be extended by future studies to understand how activists maintain memory of the past in the face of digital erasure.

Similarly, interdisciplinary involvement, including the one based on critical race studies, surveillance studies, digital media, and post-colonial theory, is also essential. The multiplicity of the platform panopticon nexus cannot be described empirically only, but requires theoretical invention, to discern the entanglement of computation, capital, and coloniality.

Concluding Reflections

The Student Intifada of 2024-2025 reveals a paradoxical situation in the digital university: on the one hand, the platforms are supposed to make the university more democratic, yet on the other, they generate even greater repression; on the one hand, universities are expected to produce critical thinking, but on the other, they are involved in risk management. However, in this contradiction, students continue to rebel, archiving, live streaming, encrypting and imagining other possibilities.

Controlled repression harbors controlled resistance. The gaps in the platform-panopticon nexus, as weak as they are, serve as a constant reminder of the fact that surveillance is never complete. Precarity, as (Butler, 2012) argues, may prove to be fertile ground to solidarity. The Student Intifada shows that digital repression is very real and has very real effects, though the prospect of counter-surveillance, epistemic disobedience, and insurgent pedagogy still persists.

The work that lies ahead is not just to write about repression, but to be able to reimagine infrastructures supporting justice. In order to commemorate the activities of Palestine solidarity activists, universities should be turned into epistemic justice sites as opposed to

information-driven oppression. This demands institutional change, as well as a general recognition of the error of mixing dissent and danger. Overall, the Palestine campus conflict is inalienable to the larger anti-Palestine conflict of determining the future of the university itself: as an infrastructure of risk of surveillance capitalism, or an infrastructure of solidarity of epistemic justice.

References

- Abu-Lughod, L. (2013). *Do Muslim women need saving?* Harvard University Press.
- Agamben, G. (1998). *Homo sacer: Sovereign power and bare life*. Stanford University Press.
- Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. University Press of Kansas.
- Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. Routledge.
- Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, 12(2), 185–196.
- Atshan, S. (2019). Review of *Life lived in relief: Humanitarian predicaments and Palestinian refugee politics*, by I. Feldman. *American Ethnologist*, 46(4), 468–470. <https://doi.org/10.1111/amet.12856>
- Al Jazeera English. (2024). *Israelism: The awakening of young American Jews* [Video]. YouTube. <https://www.youtube.com/watch?v=lq6J7Q6L0yw>
- Al Jazeera English. (2024). *War on Gaza: Global boycott movement against Israel gains traction* [Video]. YouTube. <https://www.youtube.com/watch?v=MiBjWeZVWSE>
- Al Jazeera English. (2025). *Does criticising Israel amount to antisemitism? | Inside Story* [Video]. YouTube. <https://www.youtube.com/watch?v=UzKwltlgh7Q>
- Al Jazeera English. (2025). *Israel: "Gaza will be entirely destroyed" | The Listening Post* [Video]. YouTube. <https://www.youtube.com/watch?v=DKGKB4prpHE>
- Ball, K., Haggerty, K., & Lyon, D. (Eds.). (2012). *Routledge handbook of surveillance studies* (1st ed.). Routledge. <https://doi.org/10.4324/9780203814949>
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. Polity.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40.
- Brayne, S. (2021). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.
- Browne, S. (2015). *Dark matters: On the surveillance of Blackness*. Duke University Press.
- Brinkmann, S., & Kvale, S. (2014). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications.
- Butler, J. (2012). *Parting ways: Jewishness and the critique of Zionism*. Columbia University Press. <https://doi.org/10.7312/butl51795>
- Butler, J. (2018). *Notes toward a performative theory of assembly*. Harvard University Press.
- Cainkar, L. (2009). *Homeland insecurity: The Arab American and Muslim American experience after 9/11*. Russell Sage Foundation.
- Charmaz, K. (2014). Grounded theory in global perspective: Reviews by international researchers. *Qualitative Inquiry*, 20(9), 1074–1084. <https://doi.org/10.1177/1077800414545235>

- Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. NYU Press.
- Christin, A. (2020). *Metrics at work: Journalism and the contested meaning of algorithms*. Princeton University Press.
- Catsam, D. C. (Ed.). (2025). *Struggle for a free South Africa: Campus anti-apartheid movements in Africa and the United States, 1960–1994* (1st ed.). Routledge.
- Charmaz, K. (2014). Grounded theory in global perspective: Reviews by international researchers. *Qualitative Inquiry*, 20(9), 1074–1084. <https://doi.org/10.1177/1077800414545235>
- Cheng, E. W. (2019). Review of *Media and protest logics in the digital era: The Umbrella Movement in Hong Kong*, by F. L. F. Lee & J. M. Chan. *The China Quarterly*. <https://doi.org/10.1017/S0305741019000952>
- Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. NYU Press.
- Christin, A. (2020). *Metrics at work: Journalism and the contested meaning of algorithms*. Princeton University Press.
- Cohen, J. E. (2025). Did antisemitism in public opinion rise in the wake of the Israel– Hamas war? *Religions*, 16(10), 1255. <https://doi.org/10.3390/rel16101255>
- “Columbia University takes disciplinary action against around 70 students.” (2024, April). *YouTube video*. <https://www.youtube.com/watch?v=hyyebEgvNhW>
- Couldry, N., & Mejias, U. A. (2019a). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Couldry, N., & Mejias, U. A. (2019b). Data colonialism: Rethinking big data’s relation to the contemporary subject. *Television & New Media*, 20(4), 336–349. <https://doi.org/10.1177/1527476418796632>
- CNN. (2024). *Queen Rania: There's a 'glaring double standard' in how world treats Palestinians* [Video]. YouTube. <https://www.youtube.com/watch?v=OIodM-qPCUI>
- Democracy Now! (2024). *1,000+ Harvard students walk out of commencement* [Video]. YouTube. <https://www.youtube.com/watch?v=3kTtrJAA3U8>
- Democracy Now! (2025). *Harvard commencement speakers: Despite crackdown, "students will keep speaking up" for Palestine* [Video]. YouTube. <https://www.youtube.com/watch?v=NKQsrPRGmMM>
- Delli Paoli, A. (2022). The potential of digital ethnography for sensitive topics and hidden populations. *Italian Sociological Review*, 12(7S), 729–747. <http://dx.doi.org/10.13136/isr.v12i7S.579>
- De Certeau, M. (1984). *The practice of everyday life* (S. Rendall, Trans.). University of California Press.
- Deleuze, G. (1992). Postscript on the societies of control. *October*, 59, 3–7.
- Eyewitness News ABC7NY. (2024). *Columbia graduates tear up their diplomas to protest school's cooperation with Trump administration* [Video]. YouTube. <https://www.youtube.com/watch?v=RKrYoXomGUU>

- Fairclough, N. (2013). *Critical discourse analysis: The critical study of language* (2nd ed.). Routledge.
- Finn, J. (2014). Review of *Liquid surveillance: A conversation*, by Z. Bauman & D. Lyon. *Canadian Journal of Communication*, 39(3), 473–475. <https://doi.org/10.22230/cjc.2014v39n3a2843>
- Floyd, R. (2021). *The morality of security: A theory of just securitization*. Cambridge University Press.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Vintage Books.
- Freire, P. (1970). *Pedagogy of the oppressed*. Herder and Herder.
- Fricker, M. (2007). *Epistemic injustice: Power and the ethics of knowing*. Oxford University Press.
- Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. University of Chicago Press.
- Gilliom, J., & Monahan, T. (2013). *SuperVision: An introduction to the surveillance society*. University of Chicago Press.
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Gitlin, T. (2012). *Letters to a young activist* (Reprint ed.). Basic Books.
- Gordon, F. (2019). Review of *Automating inequality: How high-tech tools profile, police, and punish the poor*, by V. Eubanks. *Law, Technology and Humans*, 1, 162–164.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.
- Halpern, O. (2015). *Beautiful data: A history of vision and reason since 1945*. Duke University Press.
- Hanafi, S. (2016). *Knowledge production in the Arab world: The impossible promise*. Routledge.
- Introna, L. (2016). Algorithms, governance, and governmentality: On governing academic writing. *Science, Technology, & Human Values*, 41(1), 17–49.
- Kraska, P. (2001). *Militarizing the American criminal justice system*. Northeastern University Press.
- Kwet, M. (2019). *Digital colonialism: South Africa's education transformation in the shadow of Silicon Valley* (Doctoral dissertation). Rhodes University.
- Lyon, D. (2007). *Surveillance studies: An overview*. Polity.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.
- Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Routledge.
- Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, 1(3), 331–355.
- Markham, A. N., & Buchanan, E. (2012). *Ethical decision-making and internet research: Version 2.0 – Recommendations from the AoIR ethics working committee*. Association of Internet Researchers. <https://aoir.org/reports/ethics2.pdf>
- Massad, J. (2006). *The persistence of the Palestinian question: Essays on Zionism and the Palestinians* (1st ed.). Routledge.

- Mayer-Schönberger, V., & Cukier, K. (2014). *Big data: A revolution that will transform how we live, work, and think*. Harper Business.
- Melis, R. (2019). Anonymity versus privacy in a control society. In S. E. Wood, J. Lowry, & A. J. Lau (Eds.), *Information/control: Control in the age of post-truth* [Special issue]. *Journal of Critical Library and Information Studies*, 2(2). <https://doi.org/10.24242/jclis.v2i2.75>
- Monahan, T. (2010). *Surveillance in the time of insecurity*. Rutgers University Press.
- Murakami Wood, D., & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neoliberal capitalism. *Marketing Theory*, 13(1), 47–67. <https://doi.org/10.1177/1470593112467264>
- Middle East Eye. (2024). *GWU student calls out university's silence on Israel ties* [Video]. YouTube. <https://www.youtube.com/watch?v=Yb6kR79OXYc>
- Middle East Eye. (2025). *NYU denies diploma to student who condemned Israel during graduation speech* [Video]. YouTube. <https://www.youtube.com/shorts/czQ4EmgaM5E>
- Middle East Eye. (2024). *UIC student delivers Gaza solidarity speech during graduation ceremony* [Video]. YouTube. <https://www.youtube.com/watch?v=y2-K1wLg-CU>
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- Offenhardt, J. (2025, March 10). ICE arrests Palestinian activist Mahmoud Khalil. *AP News*. <https://apnews.com/article/columbia-university-mahmoud-khalil-ice-15014bcbb921f21a9f704d5acdcae7a8>
- Parenti, C. (2003). *The soft cage: Surveillance in America from slavery to the war on terror*. Basic Books.
- Pickerrill, J. (2003). *Cyberprotest: Environmental activism online* (1st ed.). Manchester University Press.
- Puig de la Bellacasa, M. (2017). *Matters of care: Speculative ethics in more than human worlds*. University of Minnesota Press.
- Rieder, B., Matamoros-Fernández, A., & Coromina, Ò. (2018). From ranking algorithms to “ranking cultures”: Investigating the modulation of visibility in YouTube search results. *Convergence*, 24(1), 50–68.
- Roberts, S. T. (2019). *Behind the screen: Content moderation in the shadows of social media*. Yale University Press.
- Robinson, C. J. (2000). *Black Marxism: The making of the Black radical tradition*. University of North Carolina Press.
- Schrecker, E. (1986). *No ivory tower: McCarthyism and the universities*. Oxford University Press.
- Scott, J. C. (1990). *Domination and the arts of resistance: Hidden transcripts*. Yale University Press.
- Simpson, A. (2014). *Mohawk interruptus: Political life across the borders of settler states*. Duke University Press.
- Spivak, G. C. (1988). Can the subaltern speak? In C. Nelson & L. Grossberg (Eds.), *Marxism and the interpretation of culture* (pp. 271–313). University of Illinois Press.

- Stoler, A. L. (2008). *Along the archival grain: Epistemic anxieties and colonial common sense*. Princeton University Press.
- TikTok. (2025, August 1). *Community guidelines report, second quarter 2025*. <https://www.tiktok.com/transparency>
- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- Wohlert, I. K., Vega, D., Magnani, M., & Segerberg, A. (2025). Detecting coordination on short-video platforms: The challenge of multimodality and complex similarity on TikTok. *arXiv*. <https://doi.org/10.48550/arXiv.2506.05868>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

SCRR