Digital Diplomacy, Surveillance Technology: Implications on Palestinian Rights to Digital Expression and Privacy

Madeleine Walker
Laidlaw Scholars Programme
2022

Faculty Mentor: Professor Ori Soltes
Georgetown University

Dear Reader,

Due to time constraints, this deliverable only contains a small percentage of my research observations and analyses. I have conducted research on all of the following sections, but was only able to include several in this document. The final draft, to be completed in the coming months, will include the following sections:

General: Digital Diplomacy and Surveillance

- The Rise of Digital Surveillance, Its Usage and Dangers
- The International Community's Opinions on Surveillance
- Traditional and Digital Diplomacy, Differences and Challenges

An Introduction to the General Trend of Unfair Treatment of Palestinians by the Israeli Government and Israeli Defense Forces

The Case of Israel-Palestine: Surveillance

- Israel's Expansive Surveillance, Consequential Rights Abuses
    - Pegasus, the NGO Group
    - Blue Wolf
    - AnyVision

The Case of Israel-Palestine: Facebook and Instagram Content Removal, Arrests

The Case of Israel-Palestine:

- The Significance of Social Media for Palestinians Located in the Territories and the State of Israel
    - Proof of Repression, International Audience
    - The Organization of Protests and Other Political Movements
    - Engagement with Palestinian Culture, History
    - Communication with Family and Friends

Legal Obstacles

- Analyses and Criticisms of:
    - Corporate Obligations to Protect Human Rights
    - Facebook's Corporate Human Rights Policy
    - UN Guiding Principles on Business and Human Rights
    - The Corporate Responsibility to Respect Human Rights
    - Global Principles on Freedom of Expression and Privacy ("the Principles")
- International Human Rights Law as Performative, Unenforceable

Suggestions to Reduce Abuses of Palestinians' Rights, directed at:

- The NSO Group
- The Israeli Government and Israeli Defense Forces
- The International Community
- The US Government
- Meta

Sections in this Deliverable:

- The Rise of Digital Surveillance, Usage and Dangers
    - Past Governmental Overstepping in Digital Surveillance, with Market Assistance
    - Potential Measures to Protect Privacy
- Traditional and Digital Diplomacy, Differences and Challenges
    - How Change is Made
    - Digital Diplomacy - Trends and Utility
    - Balancing Traditional Diplomacy with Digital Diplomacy
    - Prevalence of Social Media Usage in Diplomacy
    - Key Problem #1: Too Much Data
    - Key Problem #2: Is Digital Diplomacy a Tool for Imperialism, Cultural Erasure?
    - Key Problem #3: Gap Between Speeds of Technology and Bureaucratic Processes
    - Social Media: a tool to elevate silenced voices, reach farther audiences
- Pegasus Software and the NSO Group
    - Introduction to Pegasus and The NSO Group
    - Rights Abuses Committed With Pegasus
    - NSO Response to the hacking
    - Prohibiting Pegasus Usage
- The Relationship between Judaism and Israel as Defined by The Jerusalem Declaration on Anti-Semitism
    - The Relevance of the JDA to this Research Project
    - Introduction to the JDA
    - Limitations on the Use of the JDA
    - Permitting Human Rights Abuses
    - Perpetuating Anti-Semitism
    - Examples of Anti-Semitism
    - Reasonable and Unreasonable Speech
    - Additional Notes on the JDA
- Discriminatory Social Media Content Removal, Arbitrary Arrests
    - An important Note
- Palestinian Freedom Online: Significance and Immediate Threats
    - The Significance of Digital Sovereignty

The Rise of Digital Surveillance, Usage and Dangers

The concept of privacy as one's control of their own data against unwarranted surveillance is considered by some scholars to be "a critical dimension of civic power."[1] However, with the rise of the digital age, smartphones, computers, and other personal, digital interactions and data exchanges have become a constant occurrence. What used to be a safe haven from one's neighbors, friends, and general public life - the home - has become increasingly infiltrated by those very elements. This overlap has led to the blurring of private-public boundaries."[2] The home in the digital age is, therefore, no longer congruent with Nissenbaum's idea of privacy as a matter of seclusion in a space away from the unwanted gaze of others."[3]

Pinch and Goffman combined their ideas of public self-presentation into a fascinating analogy:

> **"...** on a merry-go-round in a theme park, a fun, mundane, staged setting where the person becomes part of everyone's spec- tacle. We can understand how a person manages, in a moment of fleeting joy, to perform the delicate task of handling selves. She may be staging her face and expression while maneuvering around the carousel's horse. And yet she is still consciously aware of surroundings, other people, and most important, a self. Here the overarching point is clear: human agency remains, and it is how individual interactions with technology are shaped by institutions that will push the surveillance properties of technology in a positive or a pessimistic direction."[4]

Unfortunately, while it is indeed true that "a person's decision to be private or public depends on deliberate consideration of the context,"[5] it is becoming more and more common for online users of various platforms to be misled, their information used in ways that they did not anticipate and would not knowingly condone. For instance, "A person who divulges health-related personal data to an electronic medical service may be unaware of potential exploitation by insurance companies, and thus has not considered the context."[6] A similar issue could emerge if governments claim that expansive surveillance is used for one purpose, but do not provide transparency of such usage and ultimately proof of information abuse arises.

Many of my peers say "Eat the rich" or "Boycott Amazon" - some because they oppose America's capitalistic structure, and some because they consider Bezos and others like him to be villains "whose microtargeting innovations encouraged economic discrimination based on profiling."[7] This profiling is inherently flawed because it relies on monism, or a "methodological singularity confined to a single unit of analysis."[8] There is no room for nuance as would be present in human-to-human interaction and multi-faceted research methods. "Monistic" and

---

[1] Park, Yong Jin. (2021). "The Future of Digital Surveillance: Why Digital Monitoring Will Never Lose Its Appeal in a World of Algorithm-Driven AI," pg. 7. 10.3998/mpub.10211441.
[2] Ibid, 10.
[3] Ibid, 11.
[4] Ibid, 11.
[5] Ibid, 12.
[6] Ibid, 12.
[7] Ibid, 6.
[8] Ibid, 7.

"holistic" are, in this case, complete opposites. And, because a holistic picture is necessary in order to obtain most accurate results in one's research, one must wonder if such could ever be accomplished on a solely digital level. Are human interactions necessary for ethical and accurate research analyses to be made?

The complexity of human beings combined with the generalized profiling of surveillance algorithms inevitably results in "... societal disadvantages and discriminatory practices."[9]

The key point made in the report "The Future of Digital Surveillance" is the following: "... privacy does not exist in a societal vacuum, since institutional conditions and individual agency interact to shape the direction of digital surveillance technologies."[10] This is to say that, while a user may post on a private Instagram account with no followers, leave a comment in drafts, or make a Google search in "incognito mode," all data content is immediately distributed to digital institutions and uploaded into algorithms.

The exchange of the innovations of technology and one's privacy is, at this time, non-negotiable. Meta platforms such as Instagram and Facebook, search engines such as Google and Yahoo, and online shopping sites such as Amazon have centralized and made cheaper and simpler our communications, purchases, and information attainment. They are able to do so by "... curating an endless barrage of news and information tailored to our personal interests. But there are personal data that we do not want to reveal and that if revealed may have unintended consequences. Some data are just meant to be private."[11]

On this topic, a sociologist named Gary Marx is known for presenting behavioral strategies to counter digital surveillance, "among them avoidance, masking, and refusal to allow the release of data." However, his work was conducted largely in the late 1990s, and the leaps of technological and surveillance innovations since have outdated and overpowered much of his proposed solutions. Consider the Terms and Conditions documents that people must sign, digitally and in pen, before enrolling in a school, downloading a free smartphone application, or buying a car. Consider the "Accept all cookies" notifications that pop up on most websites when they are first opened. To get to our destination faster, we rarely read such conditions or look into the content or purpose of these cookies. We sign, we click "accept," and we move on, without thinking for a second about what data is going where, to whom. When terms and cookies can be found, and are often prevalent, in almost every aspect of daily life, it becomes less and less possible to avoid providing data, or refusing its release. These are just two examples in a world run on digital services that, if rejected, would impair one's participation in cultural, political, or economic activities.[12]

Past Governmental Overstepping in Digital Surveillance, with Market Assistance

While this research paper will largely address the Israeli government's violations of privacy made on digital platforms, it is not the only country to have engaged in such abuses. For example, in 2013, Edward Snowden became famous for blowing the whistle on the PRISM surveillance program in which "companies have been charged with lying to the public about their

[9] Ibid, 12.
[10] Ibid, 15.
[11] Ibid, 16.
[12] Ibid, 80-81.

relationship with the spy agency, gathering domestic intelligence for the NSA and violating the Fourth Amendment, which prohibits any search without warrant."[13]

Some believe that unwarranted surveillance is not the issue itself, but rather the symptom of larger, an institutional obsession with data collection, and corruption. However, what seems to be a massive governmental overstep into civilian privacy may become normalized with time. The US census, first collected in 1790, was debated by citizens who felt uncomfortable sharing personal details required for taxation purposes. To this day, some scholars even "question[ed] whether such a massive mechanism of collecting, processing, and retaining information regarding individual citizens exists for the sake of efficiency (Beniger 2009) or for the sake of bureaucratic social control."[14]

Currently, a prominent form of digital data collection is conducted by markets. Retail stores, credit card companies, and even baby food factories purchase data from websites that people use, and then publish personalized advertisements on users' pages and frequented sites. However, the benefit of increased surveillance comes at a cost to consumers: their privacy: "... data surveillance is justified on the basis of tangible benefits, media services in commercial platforms or improved public safety produced by governmental surveillance."[15]

Economics, as opposed to political gains or other motives, are the root cause of modern day surveillance.[16] However, there is notable overlap between market corporations and governmental institutions. For instance, "private companies, like Amazon, provide contractual data services for local and national governments, blurring private and public sectors where citizens resist the power of institutions."[17] This overlap of powers, civil and governmental, makes citizens' resistance or refusal to provide data, as encouraged by Gary Marx, nearly impossible.

Potential Measures to Protect Privacy

The inevitability of data distribution and collection via everyday, modern technologies has led to "the end of privacy as we have known it in the past."[18] There is no undoing this change. Those who have played on an iPad, FaceTimed a friend, ordered an Uber, participated in a TeleHealth conference, or attended a virtual Zoom class in recent years have become desensitized to their gradually decreasing data privacy. These forms of constant digital engagement, among countless others, have led us "to lose a sense of privacy, data control, and, more fundamentally, the ability to determine how our identities are defined by algorithmic codes."[19]

However, there are several steps that citizens and institutions alike can make to reduce algorithm-based discrimination and privacy violations caused by surveillance technology.
To start, Furthermore, states' governmental policies can and should be adjusted. One critical realm of policy adjustment is that which would limit the harm inflicted by private institutions' data collection. Law should evolve to accommodate the increasing rates of data collection and the specifics of its usage. Some legal scholars have already started analyzing legal precedents, "for

[13] Ibid, 21-22.
[14] Ibid, 26.
[15] Ibid, 30-31.
[16] Ibid, 40.
[17] Ibid, 41.
[18] Ibid, 18.
[19] Ibid, 81.

example in tort disputes in which a person files suit against a digital platform for breach of service terms and related violations."[20]

Stricter data regulations would also serve the economy and America's ideal "free markets." Although more difficult to assess than tangible corporations, Meta's Instagram and Facebook are nearing monopoly-esque domination in the world of digital platform market shares. There also exists an oligopoly of manufacturers for Internet products and related services, such as Apple and Samsung smartphones, and Google Home and Alexa. Even the Internet itself is controlled by monopolies in different regions, namely Verizon and Comcast.[21] Additionally, governments' surveillance usage goals and the execution of said goals should be provided to their citizens and residents on a regular basis. An audit is necessary to ensure that the surveillance is being used as advertised so that personal data is not unknowingly given away.

Unfortunately, "even after a certain level of transparency is achieved, these emergent systems can use people's data in ways that are disguised as consumer benefits or rewards. In this way, AI will function as a de facto gatekeeper that decides who participates in particular digital systems. And this is the fundamental cause for alarm."[22] Therefore, policies should also be devised and enforced with marginalized peoples in mind. Differing social demographic backgrounds create disparities among digital users in their capacity to respond effectively to digital surveillance.[23] The Palestinian peoples, for instance, come from a demographic background of poverty and oppression, deemed "stateless" and treated as terrorists when the majority are not. Therefore, those who are most likely to be exploited by digital surveillance should be pinpointed and aided in preventionary measures.

The most evident way to prevent further marginalization based on privacy awareness and caution is free, related educational workshops. One's knowledge and access to knowledge affects how they retrieve and internalize information, and informs their awareness of personal privacy risks. The cognitive principle entailed by such workshops would also empower people "... to take informed control of their digital identities."[24] As relates to this paper, the Palestinian people receive inferior educational resources to their Israeli counterparts, even though they may live in the same neighborhood. These Palestinians are therefore likely to attain less knowledge on digital privacy and protections than their non-Palestinian neighbors, exacerbating their already high vulnerability to digital exploitation and attacks. Even with education on privacy rights and common phishing scams, among other abuses of data collection capabilities, Palestinian peoples' "... ability to cooperate, negotiate, or defect is hindered by the fact that the other actor (the institution) not only controls, but also monopolizes, the digital environment and its institution) not only controls, but also monopolizes, the digital environment and its rules."[25]

Traditional and Digital Diplomacy, Differences and Challenges

[20] Ibid, 62.
[21] Ibid, 78.
[22] Ibid, 86.
[23] Ibid, 49.
[24] Ibid, 49.
[25] Ibid, 62.

The prevailing theme of a source that I consulted frequently throughout my research, *Digital Diplomacy, Theory and Practice,* is "diplomacy as change management."[26] As is evident by the name, the book's contents focus on the utility of technological and digital innovations in said change management.

The term "digital diplomacy" stands for the amalgamation of public diplomacy, soft power, smart power, and digital innovations, although it has many nicknames: e-diplomacy, cyber diplomacy, twiplomacy, etc..[27]

Digital Diplomacy, Theory and Practice treats the concept of public diplomacy as synonymous with soft power - a persuasive approach to engaging in international relations, often with the use of economic or cultural influence.[28] The "soft" modifier here refers to the lack of military or economic hostility. Instead, as explained by Joseph Nye in 1990, post-Cold-War, soft power is "the ability to set the agenda in world politics through persuasion, enticing and attracting others through the force of one's beliefs, values and ideas."[29]

As a governmental strategy, digital diplomacy is considered by some to be the "novel and practical extension of soft power," in reference to the "novel," or *modern*, digital and technological innovations that alter former methods of soft power. However, digital diplomacy is considered by others to be a form of "smart power," which is ultimately a combination of soft and hard powers[30] - a lack of military or economic hostility and added, innovative digital tools - that work together to "protect US interests and leverage influence abroad to forge alliances and bolster relations."[31]

In any case, digital diplomacy is unique in that it is a combination of intelligence collection and diplomatic use of said intelligence, all made possible through digital technologies and platforms.

How Change is Made

Before diving into the effectiveness or ethics of digital tools in diplomacy, as a student or a digital diplomat, one must first understand the trends by which societal change is made.

The first way to make change is incrementally, "through alterations in daily practices over time."[32] These changes are provoked by internal factors. One may picture a frog in a pot of water that slowly begins to boil. It is often difficult, if not impossible, to detect any changes being made since they are so gradual and minute. A real-life example of this incremental change is American society's gradual attempts to slow climate change via education, increased recycling and composting, and natural energy extraction, among other efforts.

The second method of making change is through abrupt, significant alterations within the bodies that allow change to occur.[33] These are institutional changes often provoked by, and always provocative of, societal and/or cultural shifts. Exogenous shock changes, which occur quickly, are included in this method. They have been described as "top-down structural-level

---

[26] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy,* pg. 33. Taylor & Francis.
[27] Ibid, pg. 35.
[28] https://languages.oup.com/google-dictionary-en/
[29] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy,* pg. 35. Taylor & Francis.
[30] Ibid.
[31] Ibid, pg. 35.
[32] Ibid, pg. 21.
[33] Ibid, pg. 22.

shifts" due to modifications in how change processes are conducted.[34] An example of an exogenous shock was the Taliban's quick takeover of Kabul following the removal of US troops in the country. The country was forced to shift "from one set of collective understandings or 'paradigms' to another" in less than a week.[35]

These ways in which change is made are crucial for states deciding when to pursue which form of diplomacy: traditional or digital.

Digital Diplomacy - Trends and Utility

Digital diplomacy is best utilized when attempting to make incremental shifts. This specialization is due to the main capability of digital tools to gather data, construct visual analyses, and theorize correlations.[36]

Internet communication technologies (ICTs), a key element of digital diplomacy, are a popular vehicle for surveillance and consequenting data collection. ICTs allow for the production, dissemination, and maintenance of knowledge by numerous witnesses to help further state interests.[37] Via ICT content production and, more importantly, consumption, diplomats no longer interact with only certain echelons of society; the general public is now an actor.[38] Notably, during the Boston marathon bombing in 2013, citizens' social media posts reported the situation before news organizations did.[39] ICTs (especially on social media) have become strong and reliable informants of data for states, efficiently handling vast amounts of information and subsequently, knowledge.[40] Their usage should not be overlooked.[41]

Perhaps the most unique aspect of ICTs is its efficiency. Before the age of smartphones and Google, diplomats reached wide audiences via newspaper articles, radio interviews, and television features. However, obstacles such as time and institutionally mandated censorship slowed and altered the information presented. Social media posts, among other ICT communications, allow for information to be transmitted to more people, faster, in its original form.

ICT platforms also act as a digital medium for public diplomacy initiatives. For instance, critical activity within the Foreign Commonwealth Office of the United Kingdom is listening to angles and tones of discussions taking place and posting content to encourage debate and foster partnerships.[42]

As relates most pertinently to this research topic, digital diplomacy functions such as advocacy have also served to elevate the voices of the oppressed. For instance, "during attempted democratic transitions, such as those during the Arab Spring," digital diplomacy manifested in raising awareness of what was happening in the countries, beyond the countries' borders.[43] Given that government officials were denying most claims of rights abuses, it was

[34] Ibid, pg. 22.
[35] Ibid, pg. 22.
[36] Ibid, pg. 24.
[37] Ibid, pg. 18.
[38] Ibid, pg. 36.
[39] Ibid, pg. 14.
[40] Ibid, pg. 18.
[41] Ibid, pg. 15.
[42] Ibid, pg. 37.
[43] Ibid, pg. 41.

crucial that American diplomats use their credibility and audience to bypass “governments and state-controlled media that may distort the initial communications.”[44]

Balancing Traditional Diplomacy with Digital Diplomacy

Face-to-face diplomacy is best for crisis diplomacy and conflict resolution - both of which are inevitable needs following a national exogenous shock. Face-to-face (or traditional) diplomacy is best utilized in this instances because personal interactions allow for easier relationship management, improved understanding of another’s intentions and/or their sincerity, and “identity construction,”[45] or more human, empathetic engagement than the often detached, cold realities of digital engagement.

In digital interactions, it is difficult if not impossible to gather information through not only what is said, but what is not said.[46] Such unspoken details are unique to in-person interactions, and often cannot even be grasped on video calls where one is technically “facing” another. Several studies show that meetings on video calls tend to be more task-oriented and less social.[47]

Furthermore, the human element of having a conversation with someone else in person is more likely to have positive psychological effects such as the increased likelihood of mutual empathy and trust.[48] One historical example of successful traditional diplomacy following an exogenous shock was the deescalation and trust-building that occurred following the Ukrainian crisis in 2014.[49]

Both biological elements and human sentiment affect the outcome of digital versus traditional, face-to-face interactions, as well as “... specific effects of the environment on the individual psychology at the body level.”[50] However, it is most efficient to gather and share statistical-based data, reach far audiences in little time, and observe others’ opinions and posts, via digital communications. Governments should keep these factors in mind when choosing which form of diplomacy to partake in.

Prevalence of Social Media Usage in Diplomacy

Statistically, it’s evident how deeply intertwined governments and social media are when it comes to diplomacy. As early as 2012, the US government employed over 150 staff in twenty five different ediplomacy agencies. By 2015, US missions abroad included at least 900 individual employees engaged in e-diplomatic work. The vast majority of all 193 UN member states have Twitter accounts.[51]

In recent decades, nations’ digital diplomacy strategies have centered on the usage of two major social media platforms: Facebook and Twitter. US State Government officials Alex Ross and Jared Cohen even visited Twitter, Facebook, and Google to discuss their potential for

[44] Ibid, pg. 41.
[45] Ibid, pg. 24.
[46] Ibid, pg. 28.
[47] Ibid, pg. 29.
[48] Ibid, pg. 17.
[49] Ibid, pg. 29.
[50] Ibid, pg. 17.
[51] Ibid, pg. 14.

the government. State government officials often attend similar training programs in Silicon Valley.[52]

However, as is true for most digital diplomacy operations, “the use of Twitter for diplomats and foreign actors is more about listening than talking.”[53] The main benefit is data collection.

Key Problem #1: Too Much Data

When it comes to digital diplomacy, “the problem is not too little data, but too much.”[54] Where there is significant data, as exists on the internet, about people and their behaviors, there is neither enough time nor manpower to accurately and thoughtfully parse through information. And, when numbers, GPS points, hashtags, and comments are weighted as heavily, if not heavier than, individuals’ nuanced intentions, perspectives, and identities, the result is a generalization. In some cases, such as the Open Source Indicators program at the CIA’s Intelligence Advanced Research Projects Activity, data is collected to detect significant population-level change.[55] Because the goal of this data collection is to make a general observation, the potential for harm is reduced. However, when digital programs sort through selective data to determine a person’s potential behavior or motives - for instance, data on race, age, several political opinions, offensive jokes posted years ago, etc. - danger arises.

Furthermore, given border, spending, and other limitations on surveillance and data collection that vary from country to country, it is important for nations’ intelligence units and diplomats to pool their data.[56] However, the United States State Department alone has over 70 communities/agencies that share this information.[57] This vast amount of data, combined with the data shared by other countries, makes it impossible to assess every piece of information. As an added challenge, according to an argument made by Jovan Kurbalija, “diplomatic practice is in some sense *about* knowledge construction” and “... about controlling strategically what information is shared to the public, creating an important link between knowledge management and public diplomacy.”[58] Because deemed “knowledge” about data collection is constructed by humans, it is inevitable that individual intelligence officers’s analyses will be tainted by internal biases, and a possibility that data analyses sent from one country to another have been deliberately sabotaged.

Key Problem #2: Is Digital Diplomacy a Tool for Imperialism, Cultural Erasure?

Nine of the top ten most popular social media platforms in the world are based in the United States. Only a few international cities outside the United States have enough digital capital to be considered tech hubs (think London, Beijing, Tel Aviv). It is perhaps this trend of wealth and digital power, plus a history of colonization and colonialism that are causing concern

[52] Ibid, pg. 42.
[53] Ibid, pg. 27.
[54] Ibid, pg. 25.
[55] Ibid, pg. 26.
[56] Ibid, pg. 14.
[57] Ibid, pg. 14.
[58] Ibid, pg. 18.

among the international community: “Some believe that American digital diplomacy is another Trojan horse for American imperialism.”[59]

Indeed, the Web 2.0 Revolution is founded on American interests and Western values. “Web 2.0” refers to Facebook, Twitter, and other popular digital platforms that feature “user generated content and the growth of social media.”[60] The clear domination of control over such media companies and content has raised the question of whether states are disseminating information to groups abroad selectively, likely only with each other, to perpetuate their own global power and weaken that of other countries.[61]

Key Problem #3: Gap Between Speeds of Technology and Bureaucratic Processes

There is a significant speed gap between that of technological processes and that of bureaucratic, or restricted human, processes. This discrepancy requires that calculated, but not wholly informed, decisions be made.[62]

According to Doug Frantz, it is indeed inevitable that mistakes will occur, but that latitude must be given so that people can take “responsible risks.” As put rhetorically by Tom Fletcher, “Would we have been better prepared for the Arab spring if we had discovered the hashtag #tahrir earlier?”[63]

Social Media: a tool to elevate silenced voices, reach farther audiences

Social media has been used as a tool to elevate silenced voices and reach far audiences since its creation. This has been true on both the governmental (diplomatic) and individual level.

Regarding such advocacy and awareness in digital diplomacy, online tools are often used to promote democratic parties and alert other countries of human rights abuses. Some historical instances of these alerts include the Green Revolution in Iran, the Arab Spring, and shared video footage of Neda Agha-Soltan in 2009.[64]

The ability to post and view internet content freely was one of Hillary Clinton’s priorities as former secretary of state. Her initiative involved American diplomats promoting Internet freedom in authoritarian countries, and “multimillion dollar initiatives to support digital activists” by training them to use online tools strategically to express universal rights. Clinton also pushed for the funding of panic-button programs for activists spying on corrupt governments so they can erase any incriminating information.[65]

Large-scale protests against oppression have also been organized through Facebook and Skype, and focus groups aimed at bringing peace to the Middle East have formed.[66]

Politicians and other community leaders are also able to connect with everyday citizens from around the world, on personal and group levels. For example, Farah Pandith, a US special representative to Muslim communities at the State Department, spoke on behalf of the United

---

[59] Ibid, pg. 40.
[60] https://languages.oup.com/google-dictionary-en/
[61] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy,* pg. 18. Taylor & Francis.
[62] Ibid, pg. 27.
[63] Ibid, pg. 27.
[64] Ibid, pg. 44.
[65] Ibid, pg. 46.
[66] Ibid, pg. 44.

States. Via digital tools, her talking points and Q&As were then translated into numerous languages and disseminated by influencer Muslims on social media platforms."[67]

International conflicts have caused countries to prohibit certain embassies. This physical exclusion has prevented critical information and meetings from taking place. However, virtual embassies have been a digital (at least partial) solution. Israel, for one, opened a virtual embassy to the Persian Gulf countries (GCC) in 2013. This allowed for Israel to direct its voice at a target audience despite no formal diplomatic ties in the region at the time.

The US also opened a virtual embassy in Iran in 2011 to "enhance dialogue opportunities with Iranian citizens," share American culture and policies, and challenge the regime's "efforts to place an electronic curtain of surveillance, satellite jamming and online filtering around its people."[68]

The US virtual embassy also listed opportunities for Iranians in the US, consular information for American citizens, links to other official social media accounts in Farsi, and the prohibited, so-called "Western propaganda."[69] Unfortunately, this win was short-lived. The virtual embassy in Iran was shut down by the Tehran government less than 12 hours later.[70]

Pegasus Software and the NSO Group

Introduction to Pegasus and The NSO Group

Pegasus is a spy software developed by the NSO Group, based in Israel. When downloaded on a device, those with access to the software pathway can access the camera, microphone, and text messages on the host device.

The NSO Group notably markets its technology as critical for international law enforcement and intelligence agencies "to defend the public from serious crime and terror."

Rights Abuses Committed With Pegasus

The NSO Group is a prominent name on the Human Rights Watch website due to recent findings of Pegasus software in the phones of journalists, dissidents, and human rights activists from 45 different countries. They were not aware of the software on their phone prior to the research, and therefore did not consent to its download or usage.

The first case in which Pegasus was discriminately used against an individual was in 2016, when Ahmed Mansoor, an Emirati father, poet, engineer, and human rights activist, "received a text containing a link that the sender promised would divulge information on detainee torture in UAE prisons." Fortunately, "instead of clicking on the link, Mansoor forwarded the message to Citizen Lab researchers who determined that this was a sophisticated phishing attempt using technology from… the NSO Group."[71] This scam was orchestrated by the UAE government who was attempting to hack the activist's cell phone and virtual accounts.

More recently, in 2021, the software was found on the devices of six different Palestinian human rights activists, "three of whom worked for civil society groups that Israel wrongfully

---

[67] Ibid, pg. 44.
[68] Ibid, pg. 45.
[69] Ibid, pg. 45.
[70] Ibid, pg. 46.
[71] https://www.hrw.org/report/2021/01/27/persecution-ahmed-mansoor/how-united-arab-emirates-silenced-its-most-famous-human

designated as ‘terrorist organizations’ in October.”[72] The discovery of the software was uncovered by the Front Line Defenders (FLD) and confirmed by the Citizen Lab and Amnesty International.

The word “wrongfully,” as used above in the Human Rights Watch article, refers to the organization’s disapproval of Israel’s blanket term “terrorist,” often used to describe Palestinian peoples or those who advocate for Palestinian rights. The organizations represented by the people whose devices were hacked have been fiercely defended by key leaders and committees in the international community. Some of the bodies condemning such hacking are:

- Sweden’s Minister of International Development Cooperation and Humanitarian Affairs
- The High Representative of the EU for Foreign Affairs and Security Policy
- Ireland’s Minister of Foreign Affairs and Minister of Defense
- The French Ministry of Foreign Affairs
- The EU Special Representative for Human Rights
- US Congressional representatives
- United Nations experts such as the UN High Commissioner for Human Rights
- The UN Special Rapporteur for Freedom of Association
- International groups including Amnesty International and Human Rights Watch

The quote below includes details on those Palestinians whose devices were hacked, as well as the organizations with which they associate.

> “The people hacked include Ghassan Halaika, a field researcher and human rights defender working for Al-Haq; Ubai Al-Aboudi, the executive director of Bisan Center for Research and Development; Salah Hammouri, a lawyer and field researcher at Addameer Prisoner Support and Human Rights Association, based in Jerusalem, in addition to three other human rights defenders who wish to remain anonymous. Two of the people targeted are dual nationals – one French, the other American.”[73]

NSO Response to the hacking

In response to these findings, the NSO Group announced that they would neither confirm nor deny who uses the Pegasus software. They then diverted blame by explaining that the company only produces the software and approves governments to use it - they do not know how it is used once in government hands.

Surveillance such as Pegasus has been perceived by many human rights organizations, as well as the often already-marginalized peoples whom it affects, as a violation of their privacy, an intimidation tactic, and discriminatory in its usage.

Prohibiting Pegasus Usage

A Human Rights Watch article endorses an “immediate moratorium on the sale, transfer, and use of surveillance technology until adequate human rights safeguards are in place.”[74]

---

[72] https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders
[73] https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders
[74] https://www.amnesty.org/en/documents/doc10/4516/2021/en/

However, it is unlikely that international safeguards will be effective. The organization is also pressing UN experts on human rights to publicize the abuse of Pegasus software and conduct independent research and continued oversight.

Remarkably, on November 3, 2022, the US Department of Commerce added the NSO Group to its Entity List, which aims to "aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad."[75]

The signatory organizations encouraging states to prohibit Pegasus usage are the following[76]:

Organization	**Biography**
Access Now	Access Now "defends and extends the digital rights of users at risk around the world" via a Digital Security Helpline, policy, advocacy, grants, annual RightsCon events, and legal assistance.[77]
Article 19	"ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms: the Freedom to Speak, and the Freedom to Know. When either of these freedoms come under threat, ARTICLE 19 speaks with one voice."[78]
CyberPeace Institute	The Cyber Peace Institute is a "non governmental organization (NGO) which assists humanitarian NGOs to manage their cybersecurity so they can maintain their operations."[79]
Democracy for the Arab World – DAWN	"Democracy for the Arab World Now (DAWN) is a nonprofit organization that promotes democracy, the rule of law, and human rights for all of the peoples of the Middle East and North Africa (MENA)."[80]

[75]https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
[76] https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders
[77] https://www.accessnow.org/about-us/
[78] https://www.article19.org/what-we-do/
[79] https://cyberpeaceinstitute.org/who-we-are/
[80] https://dawnmena.org/about/our-mission/

Heartland Initiative	The Heartland Initiative is a "nonprofit practice-based research organization that promotes the fundamental rights and freedoms of people impacted by armed conflict."[81]
Human Rights Watch	"Human Rights Watch investigates and reports on abuses happening in all corners of the world."[82]
Masaar - Technology and Law Community	Masaar is "a group of lawyers and technologists interested in enhancing and promoting digital rights and related freedoms in Egypt." The group focuses on "merging law and technology and deepening our understanding of their impact on human rights and fundamental freedoms."[83]
Red Line for Gulf	Red Line is an "independent, non-profit group concerned with issues of freedom of opinion and expression, press freedoms and electronic security in the countries of the Cooperation Council for the Arab States of the Gulf (Kingdom of Bahrain, State of Kuwait, Kingdom of Saudi Arabia, United Arab Emirates, State of Qatar and the Sultanate of Oman."[84]
7amleh - The Arab Center for the Advancement of Social Media	"The Arab Center for the Advancement of Social Media is a non-profit organization that advocates for Palestinian digital rights. 7amleh's mission is to create a safe, fair and free digital space for Palestinians. 7amleh studies and researches issues related to Palestinian digital rights, provides digital rights, digital activism and digital security capacity building opportunities to Palestinian activists and civil society, and manages local and international advocacy campaigns."[85]
SMEX	"SMEX is a registered Lebanese NGO that works to advance self-regulating information societies in the Arab-Speaking region."[86]

[81] https://fmep.org/grant-program/heartland-initiative/
[82] https://www.hrw.org/about/about-us
[83] https://masaar.net/en/about-us/
[84] https://rl4g.org/ (Translated into English by Google Translate)
[85] https://7amleh.org/about
[86] https://smex.org/who-we-are/

INSM Network for Digital Rights - Iraq	"INSM network, Iraqi Network for Social Media, is a network of bloggers and social media trackers on a number of various issues that concern Iraq."[87]

The Relationship between Judaism and Israel as Defined by The Jerusalem Declaration on Anti-Semitism

The Relevance of the JDA to this Research Project

The reason that I found the Jerusalem Declaration significant to my research is that it attempts to revise and reduce the unequal attention placed on the relationship between the State of Israel and Judaism. Notably, "The IHRA Definition includes 11 "examples" of anti-Semitism, 7 of which focus on the State of Israel… this puts undue emphasis on one arena."[88]

Indeed, one roadblock in my discussions about the Israel-Palestine relationship is the assumption that all statements in favor of Palestinian rights are anti-Semitic. The State of Israel, and especially its human rights violations against Palestinians, should not be conflated with Judaism and all Jewish peoples.

Religion is undeniably a strong motivational and now enthic-political factor in the creation and governance of the State of Israel. However, painting non-violent pro-Palestinian digital content and social media criticisms of the Israeli government with a broad brush, defining all such behavior and beliefs as anti-Semitic, will 1) allow human rights abuses against Palestinian peoples to be brushed under the rug, and 2) further the contagion of anti-Semitism that persists worldwide, although at varying levels geographically and socially.

Introduction to the JDA

The Jerusalem Declaration on Anti-Semitism (JDA) seeks to provide "a usable, concise, and historically-informed core definition of anti-Semitism with a set of guidelines."[89] The definition and its corresponding guidelines are meant to be seen as an alternative to the definition provided by the International Holocaust Remembrance Alliance (IHRA). Some arguments with the IHRA's definition are that it is unclear and ambiguous in meaning in some sections, and therefore is actively weakening the fight against anti-Semitism. And yet, the Declaration is proposed as a non-legally binding alternative.

The Declaration was initially signed by 210 scholars and now has approximately 350 signatories. Notably, the co-writers and signatories do not all share the same ethnic or religious identity by any means: "The signatories have diverse views about Zionism and about the Israeli-Palestinian conflict, including political solutions, such as one-state versus two-states. What

[87]https://cnxus.org/members/insmnetwork/#:~:text=INSMnetwork%2C%20Iraqi%20Network%20for%20Social,updates%20of%20the%20Digital%20Rights.
[88] https://jerusalemdeclaration.org
[89] https://jerusalemdeclaration.org

they share is a twofold commitment: fighting anti-Semitism and protecting freedom of expression on the basis of universal principles."[90]

The preamble features a self-introduction by its various signatories who are "... international scholars working in Anti-Semitism Studies and related fields, including Jewish, Holocaust, Israel, Palestine, and Middle East Studies."[91] Further, the text of the Declaration "has benefited from consultation with legal scholars and members of civil society."[92]

The document was largely inspired and informed by several significant human rights and Holocaust-related documents: the 1948 Universal Declaration on Human Rights; the 1969 Convention on the Elimination of all Forms of Racial Discrimination; the 2000 Declaration of the Stockholm International Forum on the Holocaust; the 2005 United Nations Resolution on Holocaust Remembrance. [93]

The new definition of anti-Semitism as provided in the JDA is the following: "Discrimination, prejudice, hostility or violence against Jews as Jews (or Jewish institutions as Jewish)."

Limitations on the Use of the JDA

The JDA lists several restrictions on its usage. For instance, it states that "[The JDA] can be used to support implementation of anti-discrimination legislation within parameters set by laws and norms protecting free expression." However, the declaration draws the line at its usage in hate speech codes, explaining that it is not designed to be a legal or quasi-legal instrument of any kind… codified into law… used to restrict the legitimate exercise of academic freedom, whether in teaching or research… to suppress free and open public debate that is within the limits laid down by laws governing hate crime."

Permitting Human Rights Abuses

The modifiers "as Jews" and "as Jewish" included in the JDA's definition of anti-Semitism are new and remarkable. Not every act of discrimination, prejudice, hostility or violence or against a Jewish person or institution can be deemed anti-Semitic if the activity is unrelated to their being Jewish. However, these specifications should not be seen as a justification for the general mistreatment of any person. Indeed, the aforementioned four forms of acts are largely inherently bad without rational cause [this "rational cause" and the term "bad" are both opinions or normative forms of thought which will be addressed in another section]. Instead, one should take away from this wording that not all behavior by individuals and institutions can be justified or protected simply due to their Jewish identity or majority. After all, in the words of the declaration, "The two concepts are categorically different. Nationalism, Jewish or otherwise, can take many forms, but it is always open to debate. Bigotry and discrimination, whether against Jews or anyone else, is never acceptable."[94]

In fact, violations of Palestinians' rights to privacy, digital and traditional expression, and association are often permitted because any international disagreement with the Israeli

[90] https://jerusalemdeclaration.org
[91] https://jerusalemdeclaration.org
[92] https://jerusalemdeclaration.org
[93] https://jerusalemdeclaration.org
[94] https://jerusalemdeclaration.org

government or military could be labeled as anti-Semitic. Given the horrors and subsequent international condemnation of the Holocaust, “anti-Semitism” is not a reputation that any government is eager to have. Thus, as stated by the Jerusalem Declaration, “... there is a widely-felt need for clarity on the limits of legitimate political speech and action concerning Zionism, Israel, and Palestine.”[95] The JDA attempts to provide this.

The JDA mentions multiple forms of acceptable international intervention that should not be seen, on their face, as anti-Semitism. Indeed, many of which are common acts meant to weaken or pressure countries whose governments commit human rights violations. For instance, the Declaration unambiguously includes boycott, divestment and sanctions as acceptable because they are commonplace, non-violent forms of political protest against states: “In the Israeli case they are not, in and of themselves, anti-Semitism.”[96]

The JDA also places unprecedented emphasis on context, unbiased judgment, and sensitivity in regards to hostility to Israel. After all, such hostility could be an expression of an antisemitic animus, or it could be a reaction to a human rights violation, or it could be the emotion that a Palestinian person feels on account of their experience at the hands of the State.”[97]

Unambiguously again, the JDA lists several examples of behaviors that could be seen as anti-Semitic but are not if their intentions are unrelated to the Jewish religion, ethnicity, culture, or biology. For instance, pushback against rights violations as defined under international law cannot be deemed anti-Semitism, even those that involve “supporting the Palestinian demand for justice and the full grant of their political, national, civil and human rights.” Similarly, any political opposition to Zionism - in this case, as a form of nationalism - and advocacy for the full equality to all inhabitants “‘between the river and the sea,’ whether in two states, a binational state, unitary democratic state, federal state, or in whatever form,” is also acceptable.

Lastly - and this idea will re-emerge later in my research - “Even if contentious, it is not anti-Semitic, in and of itself, to compare Israel with other historical cases, including settler-colonialism or apartheid.”[98]

Perpetuating Anti-Semitism

The JDA acts to explicitly disconnect Judaism and Jewish peoples as responsible for abuses committed by the current Israeli State. It rightfully deems “Holding Jews collectively responsible for Israel’s conduct or treating Jews, simply because they are Jewish, as agents of Israel” as anti-Semitic. To continue to associate all Jewish peoples as being pro-Israel, anti-Palestinian, or as simply an agent of the State of Israel is a blatant generalization of the Jewish peoples.

As put by the JDA itself, it is racist to essentialize (treat a character trait as inherent) or to make sweeping negative generalizations about a given population.”[99] For this reason, among others, the JDA is self-defined as “a resource for strengthening the fight against

[95] https://jerusalemdeclaration.org
[96] https://jerusalemdeclaration.org
[97] https://jerusalemdeclaration.org
[98] https://jerusalemdeclaration.org
[99] https://jerusalemdeclaration.org

antisemitism."[100] Such essentializations are what allow hatred of and physical violence against the Jewish peoples to exist.

Examples of Anti-Semitism

The JDA not only provides revised and less generalized definitions of anti-Semitism, but also vivid examples of prevalent anti-Semitic content for the curious and unclear. Such examples include: "utterances that all Jews are wealthy, inherently stingy, or unpatriotic," caricatures in which Jews are depicted as "grotesque, with big noses and associated with wealth." Some examples of anti-Semitic deeds are: "assaulting someone because she or he is Jewish, attacking a synagogue, daubing swastikas on Jewish graves, or refusing to hire or promote people because they are Jewish."[101]

Furthermore, Holocaust denialism - "Denying or minimizing the Holocaust by claiming that the deliberate Nazi genocide of the Jews did not take place, or that there were no extermination camps or gas chambers, or that the number of victims was a fraction of the actual total" - is anti-Semitic."[102]

Lastly, and related to the previous section "Perpetuating Antisemitism," the JDA declares it anti-Semitic to require people, "... because they are Jewish, [to] publicly to condemn Israel or Zionism (for example, at a political meeting)."[103]

Reasonable and Unreasonable Speech

One key point made in the JDA that has been a recurring struggle throughout this research project, especially as I dive deeper into human rights protections, is that "Political speech does not have to be measured, proportional, tempered, or reasonable to be protected under Article 19 of the Universal Declaration of Human Rights or Article 10 of the European Convention on Human Rights and other human rights instruments."

However, and this is a big "however" - this sentence is followed by the idea that "... the line between anti-Semitic and non-anti-Semitic speech is different from the line between unreasonable and reasonable speech." I had to consult multiple people in order to wrap my mind around this idea.

The general idea in this section is that unreasonable criticism of the State of Israel - while it may be unfounded, uninformed, or lacking in nuance - is not inherently anti-Semitic. That said, those who make grand statements without adequate information may not just be ignorant or lacking in nuanced perspective. Often, internalized anti-Semitism can manifest in double standards when calling out nation's rights' violations or the implementation BDS.

This section of the JDA also explains that,"Criticism that some may see as excessive or contentious, or as reflecting a "double standard," is not, in and of itself, anti-Semitic. In general, the line between anti-Semitic and non-anti-Semitic speech is different from the line between unreasonable and reasonable speech."[104]

---

[100] https://jerusalemdeclaration.org
[101] https://jerusalemdeclaration.org
[102] https://jerusalemdeclaration.org
[103] https://jerusalemdeclaration.org
[104] https://jerusalemdeclaration.org

So, while it's not inherently anti-Semitic to call out one nation's human rights violations, it is of utmost important for the safety of all people, but especially those historically marginalized such as Jewish people, that one constantly re-analyze their sources of information and maintain a skeptical mindset when engaging ideas related to Israel. Otherwise, one may, even inadvertently, perpetuate anti-Semitic thought. This is a task that I personally need to undertake often to keep myself accountable.

Additional Notes on the JDA

The use of the word "Jerusalem" in the "Jerusalem Declaration on Anti-Semitism" is not a political statement. Instead, "The JDA was convened in Jerusalem by the Van Leer Jerusalem Institute."[105]

Jewish people as described in the JDA are those understood to be ethnically, biologically, religiously, culturally, or otherwise Jewish.[106]

Discriminatory Social Media Content Removal, Arbitrary Arrests

According to Aaron Sagui of the Israeli Embassy in Washington, "Incitement and the encouragement of terror and murder on social media might end in actual violence." This idea is reasonable, but what is deemed "incitement" by the Israeli Government should not simply be the truth, such as the reality of Palestinian suffering, or opinions, like comments criticising the Israeli government. The publication of non-violent political opinions and personal experiences do not "... drive[s] young Palestinians to go out and kill Israelis."[107] And yet, everyday Palestinians see their social media content removed and often even face arrest and fines for what they post.

For instance, accused of inciting violence in their Facebook posts, at least dozens of Palestinians were arrested by Israeli authorities between October of 2015 and June of 2016. The Israeli military claims that the number of arrests rounds to 60, although the Haifa-based rights group Adallah Legal Center claims that the real number is about 400, "including 150 Palestinians in the West Bank and 250 Arab citizens of Israel."[108] Given the lack of transparency and the clear biases of both sources, it is difficult to say which number is more accurate. In any case, the reasoning for such arrests was loosely supported by a statement made by Lt. Col. Peter Lerner, spokesman of the Israel Defense Forces: "Following attacks, many assailants have stated that they were directly inspired by incitement on social media, which led them to carry out the attacks."[109]

Many similar statements are made by the IDF in which they claim that Palestinian speech on Facebook and Instagram is "inciting violence," although they have little to no data to support such claims in most arrest cases.

Undoubtedly, plenty of incitements to violence against Israelis and Jewish people are posted by Palestinians and have been rightfully removed. For instance, a Palestinian beautician

---

[105] https://jerusalemdeclaration.org
[106] https://jerusalemdeclaration.org
[107]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/
[108]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/
[109]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/

named Majd Atwan was arrested and fined “for praising a recent bus bombing in Jerusalem.”[110] Praise for violence of any kind, but especially violence against civilians based on their religion or nationality, should never be condoned, nevermind praised. It is obvious how a comment such as this would incite further violence.

However, it is the everyday, arbitrary application of the label “incitement to violence” that is harming the Palestinian peoples’ right to digital expression and in turn, the only voice they have. Furthermore, it is a common occurrence for the IDF and Israeli government to embellish stories in a way that advocates for extreme censorship of Palestinian speech online.

For instance, in Lerner’s above statement, he mentions “assailants,” plural. However, the only explicit account that he named was “the teenager accused of stabbing to death Israeli Dafna Meir in front of her young children in the West Bank settlement of Otniel. This boy allegedly said that “he watched incitement on social media “and then set out to murder Jews,’”[111] as stated by Lerner. However, in reality, the murderer was inspired by “… a Palestinian television show in which a Palestinian girl is seen arrested for refusing to comply with an order by Israeli soldiers to strip.”[112] While it was certainly media that inspired the murder of the innocent Jewish-Israeli mother, the show was not a social media post, and most importantly, did not directly incite violence. Instead, the show featured an accurate scene in which Israeli forces violate Palestinian women’s rights to privacy. The truth, in and of itself, is not an incitement to violence.

Another example of non-violent content taken down was an Instagram post made during the resurgence of fighting in May of 2021. A Palestinian posted a photo of damage caused by Israeli bombs dropped in residential neighborhoods in Gaza. The corresponding caption was descriptive of the scene - “this is a photo of my family’s building before it was struck by Israeli missiles … We have three apartments in this building.”[113] The post was removed by Meta.

Not dissimilarly, Anas Khateeb, a Palestinian youth activist, not only had his content removed, but was arrested in November of 2015 and imprisoned for over a month. His crime was a Facebook post in which he commented “I’m next in line” about attacks made by Israel on Palestinians, ”Jerusalem is Arab,” and “Long live the Intifada.”[114] The comment “I’m next in line” references the physical and legal dangers faced by all Palestinian Arabs’ in the region due to Israeli oppression. While Anas was only a teenager at the time, and a activist for peaceful Palestinian resistance to Israeli oppression, he considered himself to be a target of the Israeli Defense Forces, whether by airstrikes or arrests based on arbitrary claims of incitement to violence. The comment “Jerusalem is Arab” was likely taken down because the idea opposes that of Israel’s Zionist government. Lastly, the term “intifada” means “uprising” in Arabic. The word “intifada” in the Israel-Palestine context refers to the resistance of the Palestinian peoples against oppression. It does not have inherently violent connotations.

---

[110]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/

[111]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/

[112] https://www.timesofisrael.com/dafna-meir-fought-back-fiercely-her-teen-killer-says/amp/

[113]https://foreignpolicy.com/2021/12/03/palestinian-israeli-occupation-social-media-censorship-facebook-silicon-valley/

[114]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/

Such support of Palestinian resistance, without praise or encouragement of violence, was also censored in 2021 when a Palestinian's reposts of *The New York Times* headlines and the corresponding phrase "never concede," in regards to one's rights under international law and the Palestinian resistance, were removed.[115]

Beyond content removal, approximately 2000 Palestinians in the territories like Anas Khateeb have been arrested by the Israeli Defense Forces due to social media posts since 2017 - around 400 annually. According to Israeli governmental authorities themselves, such arrests were made based on information collected through Artificial Intelligence algorithms. This AI technology is also referred to as "predictive policing," and said predictions are based on "demographic and psychological profiling"[116] which is compiled and analyzed in order to determine who may commit violent acts. Again, this technology has been declared successful in preventing terrorist attacks. However, a lack of transparency regarding the validity of such algorithms and their consequential analyses, combined with the power disparity between Israelis and Palestinians in Palestinian territories and Israel, make such claims questionable in validity.

Furthermore, the period of fighting between the IDF and Palestinians beginning in May of 2021 also brought to light a clear double standard: Instagram or Facebook posts featuring any words in the Arabic language, even unrelated to the fighting, would likely be taken down. However, explicitly and often violent anti-Palestinian hate speech, written in the Hebrew language, remained untouched across the same platforms: Facebook and Instagram.[117]

An important note:

The Palestinian Authority and Hamas have also made arrests or targeted those who have "only criticized the authority and didn't threaten or praise violence."[118] This behavior is not unique to the Israeli government. However, for the purposes of this research paper, such censorship of Palestinians by Palestinian authorities will not be addressed thoroughly.

Palestinian Freedom Online: Significance and Immediate Threats

The Significance of Digital Sovereignty

In her article entitled "How to End Israel's Digital Occupation," Eliza Campbell at the Middle East Institute shares with the reader the idea of a Digital Palestine: while Palestinians lack political sovereignty - a problem that has only grown more complex since the creation of the State of Israel - the Palestinian peoples should at least be allowed digital sovereignty. Campbell's definition of such digital sovereignty seems to be the Palestinians' ability to post as they wish without discriminatory and arbitrarily applied punishment.[119]

---

[115]https://foreignpolicy.com/2021/12/03/palestinian-israeli-occupation-social-media-censorship-facebook-silicon-valley/

[116] https://7amleh.org/2022/07/07/april-june-2022-quarterly-report

[117]https://foreignpolicy.com/2021/12/03/palestinian-israeli-occupation-social-media-censorship-facebook-silicon-valley/

[118]https://www.usatoday.com/story/news/world/2016/05/24/facebook-incitement-posts-lead-arrests-israel/84603130/

[119]https://foreignpolicy.com/2021/12/03/palestinian-israeli-occupation-social-media-censorship-facebook-silicon-valley/

Campbell suggests that this sovereignty can only be established and protected if its three key threats are eliminated, or at least sufficiently reduced.

The first threat is that of the “network of formal and informal institutions used by the Israeli government to target pro-Palestinian expression across the globe.” She then lists two more key threats, which are the focus of this research project: the surveillance apparatus of the State of Israel, “which is used to track, intimidate, and imprison Palestinians in the occupied territories for their online speech,” and that of American social media companies “which have shown a willingness to silence Palestinian voices if it means avoiding potential political controversy and pressure from the Israeli government.”[120]

[120]https://foreignpolicy.com/2021/12/03/palestinian-israeli-occupation-social-media-censorship-facebook-silicon-valley/