POLICY BRIEF | CIVIL SOCIETY

Surveillance of Palestinians and the Fight for Digital Rights

By: Marwa Fatafta, Nadim Nashif · October, 2017

Overview

Surveillance of Palestinians has always been an integral part of Israel's colonial project. Before the creation of the state of Israel, squads from the Zionist paramilitary group the Haganah roamed Palestinian villages and cities, gathering information on Palestinian residents. Such surveillance over Palestinian lives continued after Israel's 1967 occupation of the Golan Heights, the Gaza Strip, and the West Bank, including East Jerusalem. Tools deployed included population registries, identification cards, land surveys, watchtowers, imprisonment, and torture.[1]

While these low-tech surveillance techniques are still in use today, a plethora of new technologies, such as phone and internet monitoring and interception, CCTV, and biometric data collection, have enabled Israel to surveil the population it occupies on a massive, intrusive scale. Israel particularly uses social media to monitor what individual Palestinians say and do, as well as to gather and analyze information on attitudes among the Palestinian public more broadly.

In this policy brief, 24474 and Nadim Nashif discuss this Israeli use of social media as a tool of Palestinian surveillance.[2] They examine Israeli tactics, as well as other digital obstacles to Palestinian rights, including Facebook's pro-Israel bias through censorship and lack of transparency, as well as the Palestinian Authority's (PA)

new cybercrime law. Fatafta and Nashif conclude with recommendations for how Palestinians can counter the use of social media for surveillance and protect their rights online.

Social media as a space of surveillance

The wave of Palestinian anger that began in October 2015 in response to Israeli incursions at the Al-Aqsa Mosque presented a new challenge for Israel's security apparatus. Historically, individuals affiliated with the military wings of Palestinian factions such as Fatah, Hamas, and the Popular Front for the Liberation of Palestine have carried out attacks, to which Israel has responded with violence, destruction, and collective punishment. For example, Israel launched its last three wars on the Gaza Strip, in 2009, 2012, and 2014, under the pretext of halting Hamas rocket attacks.

This time, however, Palestinian teenagers, most of whom do not belong to a Palestinian political faction or military wing, carried out the attacks. The Israeli government blamed social media for this new trend, and Israel's military intelligence increased its monitoring of Palestinian social media accounts. As a result, Israel has arrested around 800 Palestinians because of their posts on social media, particularly on Facebook, Palestinians' preferred platform.

Haaretz revealed earlier this year that these arrests are the result of a policing system that uses algorithms to build profiles of what Israel views as likely Palestinian attackers. The program monitors tens of thousands of young Palestinians' Facebook accounts, looking for words such as *shaheed* (martyr), Zionist state, Al Quds (Jerusalem), or Al Aqsa. It also searches for accounts that post photos of Palestinians recently killed or jailed by Israel. The system thus identifies "suspects" based on a prediction of violence, rather than any actual attack – or even a plan to commit an attack.

Any Facebook profile marked suspicious by the system is a potential target for arrest, and Israel's main accusation of those detained is "incitement to violence." As incitement is vaguely defined, the term includes all kinds of resistance to Israeli policies and practices. "Popularity," or how much influence a person has on social media, is a factor in whether Israel presses charges against Palestinians accused of incitement. The higher the number of likes, comments, and shares a user's content has, for example, the higher the chance they will be charged – and the longer and harsher their sentence will be.

Israeli intelligence also sets up fake Facebook accounts to track and gain access to Facebook profiles in order to talk with Palestinians and extract private information that they would not otherwise share. In October 2015, for instance, a number of Palestinian activists reported that they received messages from Facebook accounts with Arabic names and cover photos of Palestinian flags inquiring about the names of Palestinians joining protests.

Further, Israel hacks Facebook accounts to gain access to such private information as sexual orientation, medical and mental conditions, and marital and financial status. A veteran of Unit 8200, an elite Israeli army intelligence agency often compared to the US National Security Agency, testified that such material is collected as leverage. "Any information that might enable extortion of an individual is considered relevant information," he said. "Whether said individual is of a certain sexual orientation, cheating on his wife, or in need of treatment in Israel or the West Bank – he is a target for blackmail." Israeli intelligence has particularly targeted gay Palestinians, threatening to expose their intimate photos in order to persuade them to collaborate with Israel.

Such intrusion into Palestinian private life is enabled by the fact that Israel occupies and controls the entire telecommunications infrastructure used by Palestinian companies and internet service providers. The lack of any legal or ethical limitations on how far Israel can go in its surveillance of Palestinians even

led 43 veterans of Unit 8200 to send a letter to Israeli Prime Minister Benjamin Netanyahu in 2014 to protest "the continued control of millions of people and in-depth inspection that's invasive to most areas of life."

The country's military industrial complex is an even more profound enabler of the digital surveillance of Palestinians. Israel manufactures and exports a massive amount of military and cyber security technologies. According to a 2016 report by Privacy International, an NGO that investigates government surveillance and the companies that enable it, Israel is home to 27 surveillance companies – the highest number per capita of any country in the world. In 2014, Israel's world exports of cyber security and surveillance technologies, such as phone and internet monitoring, exceeded its military equipment exports. Such technologies were sold to authoritarian and repressive regimes in Colombia, Kazakhstan, Mexico, South Sudan, the UAE, and Uzbekistan, among others.

Dubious ties between Israel's army and technology sector bolster the country's prominence in the surveillance industry. Veterans of Unit 8200 have founded some of Israel's leading cyber security companies, such as the Mer Group and the NSO Group. The veterans take their military and intelligence expertise developed in the elite unit to the private sector, where there are no legal barriers regarding the overlap between the military and the surveillance industry.

Facebook: neutral or biased?

Facebook touts itself as an open platform in the service of all. Facebook founder and CEO Mark Zuckerberg recently said, "Every day I work to bring people together and build a community for everyone. We hope to give all people a voice and create a platform for all ideas."

The social media giant's dealings with Israel call such a statement into question. While Facebook has clear protocols and mechanisms for government requests to

remove content, and even publishes a biannual Government Requests Report, the company is often criticized for its lack of transparency and arbitrary decisions. A *Guardian* investigation revealed Facebook's confidential rules for moderating content related to violence, hate speech, terrorism, and racism – rules that expose its pro-Israel bias.

For instance, Facebook lists Zionists as a "globally protected group," meaning that content attacking them is to be removed. Another rule explains that "people must not praise, support, or represent a member…of a terrorist organization, or any organization that is primarily dedicated to intimidate a population, government, or use violence to resist occupation of an internationally recognized state." As a result, Facebook has censored activists and journalists in disputed territories such as Palestine, Kashmir, Crimea, and Western Sahara. According to media reports, Facebook revised the definition of terrorism to include the use of premeditated violence by non-governmental organizations "to achieve a political, religious or ideological aim." Regardless, the definition still allows the punishment of those resisting occupation and oppression, and does not include the state terror and violence inflicted on Palestinians by Israel.

Moreover, in 2016, the Israeli Justice Minister Ayelet Shaked and Public Security Minister Gilad Erdan announced an agreement between Israel and Facebook to set up teams to monitor and remove "inciteful" content.

Facebook's policy director, Simon Milner, denies that any special agreement exists between his employer and Israel. He also reiterated that all Facebook users are subject to the same community policies. However, a recent report by Adalah reveals that the Israeli Attorney General's office has been running a cyber unit since the second half of 2015 in collaboration with Facebook and Twitter to remove online content. The unit's 2016 end-of-year report boasts that it handled 2,241 cases and removed content in 1,554 of them.

The collaboration between Israel and Facebook is likely due to a number of reasons. First, Israel has a booming high tech industry and provides a profitable market for Facebook. Second, Facebook's office in Tel Aviv brings the company closer to the influence of Israeli decision makers. The appointment of Netanyahu's longtime senior adviser, Jordana Cutler, as Facebook's head of policy and communications in the Israel office is a case in point.

Third, Facebook may fear being sued. In 2015, a pro-Israeli organization, Shurat HaDin-Israel Law Center, filed a suit against Facebook in the US on behalf of 20,000 Israeli plaintiffs, who charged the company with "incitement and encouragement of violence against Israelis." Facebook's fear of legal action is expressed in a leaked internal document regarding content that denies the Holocaust. The document explains that Facebook will only hide or remove such content in four countries – Austria, France, Germany, and Israel – to avoid lawsuits.

Finally, although Facebook denies discrimination between Palestinians and Israelis, Palestinian Facebook users tell a different story. For example, shortly after a Facebook delegation met with representatives from the Israeli government in September 2016, Palestinian activists documented suspensions of personal Facebook accounts of Palestinian journalists and media organizations. The accounts of four editors at the Palestinian Shehab News Agency and three journalists from Al Quds News Network were closed. After online protests and campaigning under the hashtags #FBCensorsPalestine and #FacebookCensorsPalestine, Facebook apologized for the suspension, explaining that it was mistake.

The Palestinian Authority's new cybercrime law

It is not only Israel that suppresses Palestinian social media users: The Palestinian Authority does this as well, to quash unfavorable political views or criticisms of

Palestinian leadership. However, there is a fundamental difference between the scale of Israel's digital surveillance and the PA's violations of freedom of expression online. Whereas Israel's world-class digital surveillance makes every Palestinian a suspect and a target, the PA uses publicly shared information to target political dissent.

The PA recently passed a law that further curbs Palestinians' freedom to express themselves online. The controversial Electronic Crimes Law was signed by Palestinian President Mahmoud Abbas on June 24, 2017, without any public consultations with Palestinian civil society organizations or internet service providers. It was published by a presidential decree two weeks after it was signed and was enacted immediately.

The pretext of the new law is to fight online crimes such as sextortion, fiscal fraud, and identity theft. However, its use of vague terms such as "social harmony," "public manners," "state security," and "public order" indicates that the law has a different purpose, namely to suppress online freedom of expression and to crack down on any political criticism. It makes Palestinian internet users, especially activists and journalists, vulnerable to prosecution by the PA, who can interpret the terms as they wish.

The first two cases charged under the law demonstrate its purpose. Both employed Article 20, which stipulates that any internet user who owns or manages a website that publishes "news that endangers state safety, its public order, or internal or external security" can be imprisoned for a year or fined up to approximately $1,400. In the first case, six Palestinian journalists who work for Hamas-affiliated media outlets in the West Bank were arrested. In the second, the PA's Preventive Security Services detained Issa Amro, a prominent Palestinian human rights defender and nonviolent political activists from Hebron, who had protested the PA's arrest of a journalist in a Facebook post.

The law is in stark contravention of basic privacy protection laws and freedom of speech. It confers extensive power to state institutions to monitor, collect, and store data pertaining to online activities of Palestinians in the Occupied Palestinian Territory (OPT), and to provide this information to law enforcement entities at their request. Private internet service providers are also obliged to cooperate with security agencies by collecting, storing, and sharing users' information data for at least three years, in addition to blocking any website on orders of the judiciary.

The law's enforcement extends outside the judicial borders of the PA-controlled territories and allows for the prosecution of Palestinians living abroad. This poses a real threat to Palestinian political activists based abroad but who have a wide social media influence at home. However, the law does not specify whether the authorities would seek to extradite Palestinians based abroad for committing a cybercrime.

Countering digital surveillance

While the violation of Palestinians' digital rights presents a unique case given the Israeli military occupation, the fight for these rights is a global battle. Governments, civil society organizations, social media companies, and internet users all have an important role to play in protecting freedom of online expression and privacy from state surveillance and censorship.

In Palestine, the PA must immediately revoke its Electronic Crimes Law. To better fit its explicitly intended purpose – fighting cybercrime – the PA should consult with Palestinian civil society organizations and other relevant stakeholders to ensure that any cyber-related laws can effectively reduce cybercrime without infringing on Palestinians' political rights and public freedoms. Instead of cracking down on Palestinians for expressing their political views, the PA must seek to protect its people from being arrested and prosecuted by Israel under baseless

charges of incitement and terrorism.

Digital rights, which is part of the human rights matrix, is a relatively new concept in the OPT. Palestinian civil society organizations have a responsibility to raise awareness about these rights, most importantly regarding digital security. Keeping one's accounts protected and private information private should be a priority, especially for journalists and activists. This is especially true in the context of an occupation in which the occupier has powerful surveillance capacities and controls all telecommunications infrastructure.

Palestinian civil society and media must also expose and mobilize against Israel's unethical surveillance practices, censorship, and persecution of Palestinians' freedom of expression. Grassroots online campaigning, such as #FBCensorsPalestine and #FacebookCensorsPalestine, has proven effective in addressing social media companies' digital rights violations due to biased positions, despite claims of neutrality. Palestinians also need to build coalitions with international digital rights organizations that can help exert pressure on social media companies and the Israeli government to discontinue their violations.

1. *Al-Shabaka publishes all its content in both English and Arabic (see Arabic text here). To read this piece in French, please click here. Al-Shabaka is grateful for the efforts by human rights advocates to translate its pieces, but is not responsible for any change in meaning.*
2. *This policy brief draws on a May 2017 roundtable organized by Al-Shabaka and the Heinrich Boell Stiftung in Ramallah, in partnership with 7amleh: The Arab Center for the Advancement of Social Media. The views expressed in this policy brief are those of the author and therefore do not necessarily reflect the opinion of the Heinrich Boell Stiftung.*

Al-Shabaka: The Palestinian Policy Network, is an independent, non-profit organization. Al-Shabaka convenes a multidisciplinary, global network of Palestinian analysts to produce critical policy analysis and collectively imagine a new policymaking paradigm for Palestine and Palestinians worldwide.

Al-Shabaka materials may be circulated with due attribution to Al-Shabaka: The Palestinian Policy Network. The opinion of individual members of Al-Shabaka's policy network do not necessarily reflect the views of the organization as a whole.