PODCAST

Palestine Under Surveillance with Mona Shtaya

By: Al-Shabaka: The Palestinian Policy Network · November, 2021

The transcript below has been lightly edited for brevity and clarity.

Mona Shtaya 0:00

Unfortunately, today we are talking about mass surveillance of Palestinians in the digital spaces and on the ground. And it is clear that we are sinking in a pool of surveillance. And I'm not sure if we can get out of it.

Yara Hawari 0:20

This is Rethinking Palestine, a podcast from Al-Shabaka, the Palestinian Policy Network. We are a virtual think tank that aims to foster public debate on Palestinian human rights and self-determination. We draw upon the vast knowledge and experience of the Palestinian people, whether in Palestine or in exile, to put forward strong and diverse Palestinian policy voices. In this podcast, we will be bringing these voices to you so that you can listen to Palestinians sharing their analysis wherever you are in the world.

Over the last few weeks, we've seen some major news stories break about Israeli cyber surveillance of Palestinians — from the hacking of Palestinian NGO staff phones to the mass deployment of facial recognition software to be used against Palestinians across the West Bank.

Now, mass surveillance of Palestinians by the Israeli regime is nothing new. And

whilst this level of technological sophistication is novel, it's important to contextualize it within the panoptic reality that Palestinians have always experienced since the establishment of the Zionist settler colonial project in historic Palestine.

Joining me to discuss this topic is Mona Shtaya, a digital communication and advocacy strategist and the advocacy advisor for 7amleh, the Arab Center for Social Media Advancement. Mona, thank you for joining me on Rethinking Palestine.

Mona Shtaya 1:46

Thanks, Yara, for having me here. I really love the podcast.

Yara Hawari 1:51

Mona, Palestinians have long argued that they are essentially a laboratory or testing ground for weapons and surveillance technologies. Before we delve into what has been happening over the last few weeks, could you summarize what surveillance looks like for Palestinians on a daily basis, particularly in the West Bank and Gaza?

Mona Shtaya 2:12

Definitely, Yara. So nowadays, with the spread of surveillance technologies and with technologies generally, I can say the Israeli colonization was also developed to include using people's data and privacy.

And for the past decade, the Israeli regime has been producing and testing surveillance technologies on Palestinians as a part of their military industry. And then it's produced them massively and sold them to other governments and regimes around the world to be used to control their people.

Facial recognition techniques, spyware on mobile phones, spreading cameras to

control the population, monitoring every telephone call in the West Bank and Gaza Strip, and monitoring social media platforms and either arresting people based on what they published on social media or pushing the social media companies to take down specific content — are all forms of the shrunk spaces that Palestinians are facing because of these systematic efforts to surveil them.

Over the past couple of weeks, we saw many reports on the surveillance tools that are used to monitor Palestinians. Some may be surprised by them, but as digital rights defenders, we were expecting something like this — especially when the Israeli regime worked systematically during the pandemic to normalize surveillance culture in order to expand its profit from this occupation.

Yara Hawari 3:41

Mona, you mentioned that Palestinians were not particularly surprised by the recent events and the recent news of this mass surveillance. And that's because surveillance of Palestinians, even prior to these relatively new and novel technologies, has a historic track record. The Israeli regime has often used human personnel, spies, various different mechanisms to surveil Palestinians. What does this mean for the daily life of Palestinians in the West Bank and Gaza? How does that surveillance affect their lived reality?

Mona Shtaya 4:13

Well, let's talk about people's feelings towards these surveillance technologies. Last week, we at 7amleh produced and published a new report on the facial recognition cameras that were in East Jerusalem. But also, the same report came out of *The Guardian*, which mentioned the Blue Wolf and the White Wolf. It also mentioned surveillance cameras and facial recognition in Hebron and many other places around the West Bank.

This kind of surveillance usually creates higher self-censorship among Palestinians,

and it creates a feeling of living in an unsafe place. While we are living under this kind of occupation — or settler colonialism regime that we are living under, for the past decades — now we recognize that this kind of occupation is not only on the ground. It's also applicable to the digital spaces, the online spaces. So this kind of militarization and securitization affects people's behavior, affects people's feelings towards the society that they are living in.

And to be honest with you, in our report, we heard people's experiences with these cameras. One of them is a woman who's living in East Jerusalem. And she mentioned that she cannot take off her hijab even inside her home, because she feels that she is surveilled all the time. Even inside her home, she swears that she's sleeping with her hijab. And this kind of politics of fear are intended to spread and to normalize amongst Palestinians. But people are much more aware.

We've seen also other kinds of surveillance that they also utilize and use with Palestinians. For example, during the May escalations, we saw how they sent SMS messages to people, to worshippers who were in Al-Aqsa Mosque. They told them that "you have participated in violent" — quote-unquote — "violent work in the Al-Aqsa Mosque. And because of that, we will hold you accountable."

And by doing so, we recognize that they also are using GPS to monitor Palestinians and to surveil Palestinians. And this is also a violation of their right to privacy. When we are violating people's right to privacy, people start fearing, start feeling afraid for their life. And sometimes, with self-censorship, they stop talking, stop criticizing, and even stop expressing themselves. And that's scary. That's disastrous in terms of the context that we are living in, in Palestine.

Yara Hawari 6:51

Mona, that's incredibly important to note — that this kind of surveillance is not only about gathering information, but it's also part of scaremongering tactics and attempts to make Palestinians constantly uncomfortable so that they can't do

anything else, and that they have to self-censor. So it's also part of this attempt to depoliticize Palestinian society.

Now, some weeks ago, the Israeli Ministry of Defense criminalized six Palestinian human rights NGOs. And it's not particularly surprising, but questions were asked: why now? And what purpose does it serve? Particularly as the Israeli regime doesn't need any excuse to arrest Palestinians, to raid offices, to confiscate files.

But what's becoming clear is that the Israeli regime likely rushed this criminalization because both Citizen Lab and Amnesty International found Israeli spyware — in particular Pegasus — on the devices of staff members. And in other words, one of the reasons for this criminalization was an attempt to whitewash or to excuse this hacking. And indeed, it's a lot easier to justify this level of surveillance on organizations that you've claimed are terrorist rather than human rights organizations. So could you perhaps tell us a bit more about this?

Mona Shtaya 8:11

Well, the six Palestinians were surveilled by Pegasus, which is malicious spyware developed by the Israeli company NSO, which was recently listed on the US blacklist for manufacturing and supplying foreign authorities with the spyware.

And as I mentioned previously, oppressive regimes such as the Israeli regime usually use surveillance techniques to restrict human rights work, silencing human rights activists, and preventing them from documenting human rights violations against the Occupied Palestinian Territories in a systematic manner.

And for years, Palestinian civil society organizations — including the six mentioned organizations — have faced restrictions on civic workspace, some of which had previously faced systematic smear campaigns with the aim of defaming them and restricting their work.

Al-Haq was one of the organizations that were accused by the Israeli regime of

being a "terrorist organization," which had previously witnessed a smear campaign with the aim of restricting its work and preventing it from practicing human rights work and documenting human rights violations that we as Palestinians are exposed to on the ground.

It is clear that these campaigns were not fruitful as the Israeli authorities desired, and accordingly, the authorities began monitoring a group of workers in these organizations. And as we can see from the Front Line Defenders report, they had started surveilling two of these six human rights defenders since 2020.

And earlier this year, Amnesty International had published a detailed report about NSO, which historically used to be a suspicious link that should be clicked to hack your device. But in the last couple of years, the company developed its technology to create this zero-click spyware, where they can hack your device whenever they want. And this dangerous spyware could have access to all your data, messages, photos, and calls.

And this is not the first time that the Israeli regime uses the logic of whitewashing the crimes and the human rights violations. This is their method of work. For example, at the beginning of the pandemic, the authorities started using mobile applications under the pretext of protecting public health. And we knew that this reason was a justification for legislating the use of surveillance technologies and normalizing people's acceptance of them. Unfortunately, many governments succeeded in this.

The Israeli authorities also asked Palestinian citizens to download the Coordinator — al-Munasiq — application on their phones to obtain permits to go to work.

And unfortunately, today we are talking about mass surveillance of Palestinians in the digital spaces and on the ground. And it is clear that we are sinking in a pool of surveillance. And I'm not sure if we can get out of it.

Yara Hawari 11:18

If you're enjoying this podcast, please visit our website, al-shabaka.org, where you'll find more Palestinian policy analysis, and where you can join our mailing list and donate to support our work.

And Mona, as if this spyware wasn't scary enough, around the same time as the news broke about Pegasus, the *Washington Post* published an exposé on how the Israeli regime is incorporating facial recognition software known as Blue Wolf into its mass surveillance of Palestinians across the West Bank. What will this look like? And what will it mean for Palestinians?

Mona Shtaya 12:00

The *Washington Post* report pointed to another type of surveillance that you've mentioned, Yara, where Israeli authorities are monitoring Palestinians by integrating facial recognition with a growing network of cameras and smartphones.

As the report mentioned, over the past two years, when the world was struggling with a pandemic, the Israelis were developing a new surveillance initiative called Blue Wolf that captures photos of Palestinians' faces and matches them to a database of images. Later on, the phone app flashes in different colors to alert soldiers if a person is to be detained, arrested, or left alone.

The report also mentioned another smartphone application called White Wolf that has been developed for use by settlers in the West Bank. So they can use the White Wolf app to scan Palestinians' identification cards before the person enters the settlement. The military in 2019 acknowledged the existence of White Wolf in right-wing Israeli publications.

Adding to that, the report was also talking about surveillance cameras that the Israeli authorities are using in Hebron — as I mentioned before — and, as 7amleh's

report mentioned, Jerusalem.

All of these are systematic efforts to surveil Palestinians, to prevent them from living their normal life and also from practicing their normal life — especially people who are working in human rights documentation.

But to be honest with you, if you are a Palestinian, you could be surveilled not only because you are working in the human rights sector. As we have seen over the past couple of weeks, we saw systematic efforts to surveil Palestinians — the normal people in the streets — with cameras, with these mobile applications. If you are going to work in the settlements, you are surveilled.

Yesterday, we saw also another new report on *Middle East Eye*, where they were telling us that the Israeli authorities, the Israeli regime, is also monitoring all the phone calls in the West Bank and Gaza Strip. And that is disastrous, because people cannot call their loved ones or talk to their loved ones as they want.

And as a human rights defender, but also as a normal person who's living in Palestine, I feel that this could restrict not only the freedom of expression and violate my privacy, but it's also affecting my behavior. It's also affecting how I communicate with my close family, with my first-circle people.

So that also could, in the long term, change people's behavior, could also change people's mindset on how they use these technologies and on how they also receive this kind of surveillance and deal with it in their daily life. And also, it could affect people's trust of each other and also of their societies. And that's disastrous.

Yara Hawari 15:08

Yeah, Mona. And I think it's really important to highlight how the Israeli regime manages to infiltrate even the most intimate areas of life — even the communication with your closest family members and friends.

If we go back for a moment to the notion that Palestine is this laboratory or testing ground for these kinds of surveillance technologies, what implications does this have for the rest of the world?

Mona Shtaya 15:37

Let's have a starting point. Colonial and oppressive regimes usually agree on one point, which is the oppression of people. For this, the Israeli regime usually sells these technologies to other repressive regimes in general, and to regimes in the Global South in particular. And this has an impact on the safety of people first.

And contrary to the image that security companies and governments usually export — that these technologies are important to maintain the safety of people — I see that in the first place, it violates people's safety, people's privacy, and it works to normalize militarization and securitization in people's subconscious, thus violating their right to privacy.

And because oppressive regimes and colonial regimes usually do not allow anyone to criticize them, they use these techniques to prevent people from expressing their right to freedom of opinion and expression, and thus preventing them from their right to self-determination.

So we feel with all oppressed people who usually suffer with their governments, with the regime, because of the use of surveillance technologies — especially those imported from the Israeli regime.

If we have a look back into other regimes' histories, like the UAE regime for example, we can see how they also use the same technology — which is NSO, or Pegasus — against their political opponents. For example, there is a human rights defender who passed away a couple of months ago called Alaa al-Siddiq, and she was living in the United Kingdom because she couldn't go back to the UAE. After her death, they discovered that there was NSO spyware on her mobile phone.

Also, Jamal Khashoggi had such spyware on his mobile phone. In Morocco, the government was using surveillance technologies, specifically NSO, against their political opponents and against human rights defenders and lawyers in previous years. They have a long history of how they are using that.

In a systematic manner, these regimes are using these against journalists who could criticize them, against political opponents, activists, and human rights defenders. And it's clear that these colonial and oppressive regimes have one mission, which is to surveil people and prevent people from living in a safe world without having this kind of feeling of being surveilled and monitored all the time.

Yara Hawari 18:14

So Mona, with all of that in mind and considering everything we've discussed, how can Palestinians protect themselves from this kind of pervasive surveillance? And what about non-Palestinians? What can they do to disrupt Israeli surveillance in Palestine, but also Israeli surveillance exports?

Mona Shtaya 18:34

So for Palestinians, I have this kind of fear that we can't trust our devices. We can't trust technology. That technology usually is being utilized by oppressive regimes and also by colonial regimes to suppress people.

And because of that, Palestinians should be aware that we can't trust technology and we can't trust anything that is being shared online. Communicating with our people is very important, and using technology, utilizing technology to spread our narrative to the world is also important. But we should keep in mind that someone is watching us all the time while we are chatting with even our closest family members or beloved ones.

And because of that, people should be aware and should educate themselves more and more about digital safety and digital security tactics, where they can

protect themselves and protect their family members and their colleagues and friends.

So the first thing is raising awareness about digital security practices — that is really needed for young people, for everyone in our society. And we should keep in mind that the Israelis, as *The Guardian* mentioned, use specific information about people who they surveil — like with the LGBT community, with females, and so on — to intimidate them and to prevent them from practicing or living their normal life. And sometimes, to get more information from them about their society.

Being aware of what could happen is very important. Change your settings — your mobile settings should be the safest. We know, even if we change that, even if we prevented the location and so on, some applications could access your location. But we should make our maximum effort to prevent any kind of surveillance.

We should not click on any suspicious link. And I'm afraid of mentioning that, because now NSO has developed to be zero-click malicious spyware. But for others, they can support Palestinians and support themselves. They can escalate the pressure on their governments, on their MPs, on their congressional representatives to prevent buying these technologies from the Israeli regime.

And to have better legislation that prevents their security forces, their governments, from using such surveillance, spyware, and surveillance technologies. They can also, through their government, through their representatives, escalate the pressure to prevent Israelis from using these technologies against Palestinians, because we believe that international pressure could do something for Palestinians.

We've seen in May how the international pressure, how amplifying Palestinian voices, how the international pressure was really recentering the Palestinian cause. And by doing that, it was, let's say, fruitful to some extent. And because of that, we

should escalate the pressure more and more and prevent their governments from buying such surveillance technologies.

Yara Hawari 21:58

Mona, thank you for ending on those really important points about international pressure and for the more practical security tips. This is such an important topic, and it is incredibly worrying. And I think that's why it's so important that we highlight it. So really, thank you so much for joining me on this episode of Rethinking Palestine.

Mona Shtaya 22:21

Thank you, Yara. Thanks for having me.

Yara Hawari 22:26

Thank you for listening to Rethinking Palestine. Don't forget to subscribe and leave us a review. For more policy analysis and to donate to support our work, please visit our website, al-shabaka.org. You can also follow us on Facebook and Twitter.

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.