

How Israel uses facial-recognition systems in Gaza and beyond

Publication Date: 2024-04-19

Author: Nick Robins-Early

Section: Technology

Tags: Facial recognition, Israel, Gaza, Palestinian territories, explainers

Article URL: <https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians>



Governments around the world have increasingly turned to facial-recognition systems in recent years to target suspected criminals and crack down on dissent. The recent boom in artificial intelligence has accelerated the technology's capabilities and proliferation, much to the concern of human rights groups and privacy advocates who see it as a tool with immense potential for harm. Few countries have experimented with the technology as extensively as Israel, which the New York Times recently reported has developed new facial-recognition systems and expanded its surveillance of Palestinians since the start of the Gaza war. Israeli authorities deploy the system at checkpoints in Gaza, scanning the faces of Palestinians passing through and detaining anyone with suspected ties to Hamas. The technology has also falsely tagged civilians as militants, one Israeli officer told the Times. The country's use of facial recognition is one of the new ways that artificial intelligence is being deployed in conflict, with rights groups warning this marks an escalation in Israel's already pervasive targeting of Palestinians via technology. In an Amnesty International report on Israel's use of facial recognition last year, the rights group documented security forces' extensive gathering of Palestinian biometric data without their consent. Israeli authorities have used facial recognition to build a huge database of Palestinians that is then used to restrict freedom of movement and carry out mass surveillance, according to the report. The Israeli ministry of defense did not return a request for comment on the findings of Amnesty's report or the New York Times article on its facial-recognition programs. The Guardian spoke with Matt Mahmoudi, an adviser on AI and human rights at Amnesty and lead researcher on the report, about how Israel deploys facial-recognition systems and how their use has expanded during the war in Gaza. One thing that stands out from your report is that there's not just one system of facial recognition but several different apps and tools. What are the ways that Israeli authorities collect facial data? There's a slew of facial-recognition tools that the state of Israel has experimented with in the occupied Palestinian territories for the better part of the last decade. We're looking at tools by the names of Red Wolf, Blue Wolf and Wolf Pack. These are systems that have been tested in the West Bank, and in particular in Hebron. All of these systems are effectively facial-recognition tools. In Hebron, for a long time, there was a reliance on something known as the Wolf Pack system – a database of information pertaining to just Palestinians. They would effectively hold a detained person in front of the CCTV camera, and then the operations room would pull information from the Wolf Pack system. That's an old system that requires this link-up between the operations room and the soldier on the ground, and it's since been upgraded. One of the first upgrades that we saw was the Blue Wolf system, which was first reported on by Elizabeth Dvoskin in the Washington Post back in 2021. That system is effectively an attempt at collecting as many faces of Palestinians as possible, in a way that's akin to a game. The idea is that the system would eventually learn the faces of Palestinians, and

soldiers would only have to whip out the Blue Wolf app, hold it in front of someone's face, and it would pull all the information that existed on them. You mentioned that there's a gamification of that system. How do incentives work for soldiers to collect as much biometric data as possible? There's a leaderboard on the Blue Wolf app, which effectively tracks the military units that are using the tool and capturing the faces of Palestinians. It gives you a weekly score based on the most amount of pictures taken. Military units that captured the most faces of Palestinians on a weekly basis would be provided rewards such as paid time away. So you're constantly put into the terrain of no longer treating Palestinians as individual human beings with human dignity. You're operating by a gamified logic, in which you will do everything in your power to map as many Palestinian faces as possible. And you said there are other systems as well? The latest we've seen happen in Hebron has been the additional introduction of the Red Wolf system, which is deployed at checkpoints and interfaces with the other systems. The way that it works is that individuals passing through checkpoints are held within the turnstile, cameras scan their faces and a picture is put up on the screen. The soldier operating it will be given a light indicator – green, yellow, red. If it's red, the Palestinian individual is not able to cross. The system is based only on images of Palestinians, and I can't stress enough that these checkpoints are intended for Palestinian residents only. That they have to use these checkpoints in the first place in order to be able to access very basic rights, and are now subject to these arbitrary restrictions by way of an algorithm, is deeply problematic. What's been particularly chilling about the system has been hearing the stories about individuals who haven't been able to even come back into their own communities as a result of not being recognized by the algorithm. Also hearing soldiers speaking about the fact that now they were doubting whether they should let a person that they know very well pass through a checkpoint, because the computer was telling them not to. They were finding that increasingly they had a tendency of thinking of Palestinians as numbers that had either green, yellow or red lights associated with them on a computer screen. These facial-recognition systems operate in a very opaque way and it's often hard to know why they are making certain judgments. I was wondering how that affects the way Israeli authorities who are using them make decisions. All the research that we have on human-computer interaction to date suggests that people are more likely to defer agency to an algorithmic indicator in especially pressing circumstances. What we've seen in testimonies that we reviewed has been that soldiers time and time again defer to the system rather than to their own judgment. That simply comes down to a fear of being wrong about particular individuals. What if their judgment is not correct, irrespective of the fact that they might know the person in front of them? What if the computer knows more than they do? Even if you know that these systems are incredibly inaccurate, the fact that your livelihood might depend on following a strict algorithmic prescription means that you're more likely to follow it. It has tremendously problematic outcomes and means that there is a void in terms of accountability. What has the Israeli government or military said publicly about the use of these technologies? The only public acknowledgment that the Israeli ministry of defense has made – as far as the Red Wolf, Blue Wolf and Wolf Pack systems – is simply saying that they of course have to take measures to guarantee security. They say some of these measures include innovative tech solutions, but they're not at liberty to discuss the particularities. That's kind of the messaging that comes again and again whenever they're hit with a report that specifically takes to task their systems for human rights violations. What's also interesting is the way in which tech companies, together with various parts of the ministry of defense, have boasted about their technological prowess when it comes to AI systems. I don't think it's a secret that Israeli authorities rely on a heavy dose of PR that touts their military capabilities in AI as being quite sophisticated, while also not being super detailed about exactly how these systems function. There's been past statements from the Israeli government, I'm thinking specifically of a statement on the use of autonomous weapons, that argue these are sophisticated tools that could actually be good for human rights. That they could remove the potential for harm or accidents. What is your take on that argument? If anything, we have seen time and time again how semi-autonomous weapons systems end up dehumanizing people and leading to deaths that are later on described as "regrettable". They don't have meaningful control and they effectively turn people into numbers crunched by an algorithm, as opposed to a moral, ethical and legal judgment that has been made by an individual. It has this sort of consequence of saying: "Well, look, identifying what counts as a military target is not up to us. It's up to the algorithm." Since your report came out, the New York Times reported that similar facial-recognition tech has been developed and deployed to surveil Palestinians in Gaza. What have you been seeing in terms of the expansion of this technology? We know that facial-recognition systems were being used for visitors coming in and out of Gaza, but following the New York Times reporting it's the first time that we've heard it being used in the way that it has been – particularly against Palestinians in Gaza who are fleeing from the north to the south. What I've been able to observe is largely based on open-source intelligence, but what we see is footage that shows what look like cameras mounted on tripods that are situated outside of makeshift checkpoints. People move slowly from north to south through these checkpoints, and then people are pulled out of the crowd and detained on the basis of what we suspect is a facial-recognition tool. The issue there is that people are already being moved around chaotically from A to B under the auspices of being brought to further safety, only to be slowed down and asked to effectively be biometrically checked before they're allowed to do so. We also hear about individuals that have been detained and beaten and questioned after having been biometrically identified, but later have it been established that was a mistake. The Israeli government's justifications for its use of checkpoints and detentions is that it's based on national security fears. When it comes to facial recognition, how does that argument hold up from a human rights perspective? Your rights aren't less viable or active just because there's a national security threat. There is, however, a three-part test that you deploy when it comes to figuring out in what particularly unique kinds of circumstances

a state would violate certain rights in order to uphold others. That three-part test tries to assess the necessity, proportionality and legitimacy of a particular intervention. At Amnesty, under international human rights law, we don't believe that there is necessity, proportionality or legitimacy. This facial-recognition technology isn't compatible with the right to privacy, the right to non-discrimination, the right to peaceful assembly or freedom of movement. All these rights are severely compromised under a system that is, by design, effectively a system of mass surveillance and therefore unlawful. You've talked about the lack of accountability and accuracy with these tools. If the Israeli government knows these are not accurate, then why continue to use them? I think AI-washing is a significant part of how governments posture that they're doing something about a problem that they want to seem like they're being proactive on. It's been clear since the 2010s that governments around the globe have relied on tech solutions. Now, since the explosion of generative AI in particular, there's this idea that AI is going to solve some of the most complex social, economic and political issues. I think all it does is absolve states of the responsibilities that they have to their citizens – the obligations that they have under international law to uphold the rights of those whom they subject to their power by basically saying "the system will take care of it" or "the system was at fault". It creates these neat grounds for states to be able to seem like they're doing something, without being held to account on whatever they're actually doing. There's a technical system that is mediating both accountability and responsibility. This interview has been edited and condensed for clarity