Facial Recognition Technology & Palestinian Digital Rights

Position Paper Prepared by 7amleh - The Arab Center for the Advancement of Social Media

Threat of Mass Surveillance Technology to Digital Human Rights

Mass surveillance is the practice of spying on an entire, or significant part of a population. It can involve anything from CCTV monitoring and email interceptions, to wiretapping and computer hacking.[1] Often, mass surveillance is carried out by the state but it can also be carried out by companies, either on behalf of the government or on their own initiative. Any information a person does not want to reveal or does not want anyone to know about is considered private and is protected. For instance, if a person does not want to reveal his whereabouts, location or any other information related to his face, he's entitled to do so under Article 17 of the ICCPR.[2] Any interference with this right to privacy should be legal, necessary, proportionate and judicially authorized.[3]

Unfortunately, the legal framework authorizing and regulating the use of facial recognition technology is insufficient, and there are questions about whether the surveillance technologies are inherently disproportionate and inaccurate. Facial recognition technology can expose people to potential discrimination not only due to the potential misuse by state agencies in relation to certain demographic groups, whether intentionally or otherwise, but also research indicates that ethnic minorities, people of color and women are misidentified at higher rates than the rest of the population.[4] This inaccuracy may lead to members of certain groups being subjected to heavy-handed policing or security measures and their data being retained inappropriately. As a result, civil liberties experts warn that the technology — which can be used to track people at a distance without their knowledge — has the potential to lead to ubiquitous surveillance, threatening freedom of movement and speech.[5]

An individual's face has a particular sensitivity in the context of mass surveillance, and as a very personal form of personal data, agreements like the General Data Protection Regulation (GDPR) have protected live and non-live images of people's faces from unlawful processing.[6] Unlike a password, each person's face is unique. Therefore while passwords can be kept out of sight and reset if needed, a face cannot.[7] If your eye is hacked,[8] there is no way to wipe the slate clean. Furthermore, an individual's face is also distinct from other forms of biometric data such as fingerprints because it is almost impossible to avoid

[1] Egwuonwu, B. (2016, April 11). What Is Mass Surveillance And What Does It Have To Do With Human Rights? Retrieved from https://eachother.org.uk/explainer-mass-surveillance-human-rights/

[2] OHCHR. (n.d.). International Covenant on Civil and Political Rights Article 17. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[3] OHCHR. (2014, May). Article (19), "*NECESSARY & PROPORTIONATE International (Principles on the Application of Human Rights Law to Communications Surveillance).*" Retrieved from: https://www.ohchr.org/Documents/Issues/RuleOfLaw/PCVE/Article_19.pdf

[4] The Conversation. (2018, November 26). Why regulating facial recognition technology is so problematic - and necessary. Retrieved from https://theconversation.com/why-regulating-facial-recognition-technology-is-so-problematic-and-necessary-107284

[5] Singer, N., & C., Metz. (2019, March 19). Many Facial-Recognition Systems Are Biased, Says U.S. Study. Retrieved from https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

[6] Jakubowska, E. (2019, December 4). European Digital Rights. Facial recognition and fundamental rights 101. Retrieved from: https://edri.org/facial-recognition-and-fundamental-rights-101/

[7] Ibid

[8] Chaos Computer Clubs breaks the iris recognition system of the Samsung Galaxy S8. (2017, May 22). Retrieved from https://www.ccc.de/en/updates/2017/iriden

being subject to facial surveillance when such technology is used in public places.[9] Unlike having fingerprints taken, a face can be surveilled and analyzed without prior knowledge. This absence of consent combined with the fact that a face can also be a marker of protected characteristics under international law, such as the right to freely practice your religion, makes facial recognition highly intrusive and able to easily infringe on rights to privacy and personal data protection, among many other rights.

Researchers have highlighted the frightening assumptions underpinning much of the current hype about facial recognition, especially when used to categorize emotions or qualities based on individuals' facial movements or dimensions. This harks back to the discredited pseudoscience of physiognomy[10] – a favorite of Nazi eugenicists – and can have massive implications on individuals' safety and dignity when used to make a judgment about things like their sexuality or whether they are telling the truth[11] about their immigration status.[12] Its use in recruitment also been shown to increase discrimination against people with disabilities.[13] Experts warn that there is no scientific basis for these assertions – but that has not stopped tech companies from producing facial recognition systems.[14] When used in authoritarian societies, this sort of mass surveillance threatens the lives of journalists, human rights defenders, and anyone that does not conform – which in turn threatens everyone's freedom.[15]

Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use. In fact, facial recognition technology has received significant attention as it has the potential for a wide range of applications related to law enforcement as well as other enterprises. Facial recognition is often used as a mass surveillance[16] technique by governments. To that end it violates the *right to privacy* as it is a clear

[9] Jakubowska, E. (2019, December 4). Facial recognition and fundamental rights 101. Retrieved from https://edri.org/facial-recognition-and-fundamental-rights-101/

[10] Chinoy, S. (2019, July 10). The Racist History Behind Facial Recognition When will we finally learn we cannot predict people's character from their appearance? NYTimes. Retrieved from: https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html

[11] European Union Agency for Fundamental Human Rights. (2019, January) Facial recognition technology: fundamental rights considerations in the context of law enforcement. Retrieved from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

[12] Digitalis, H. (2018, November 21). Greece: Clarifications sought on human rights impacts of iBorderCtrl. European Digital Rights. European Digital Rights. Retrieved from: https://edri.org/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/

[13] Lee, A. (2019, November 26). An AI to stop hiring bias could be bad news for disabled people The technology that helps recruiters cut through the CV pile might be pushing disabled candidates out of the running. Wired. Retrieved from https://www.wired.co.uk/article/ai-hiring-bias-disabled-people

[14] Toh, A. (2019, November 18). Rules for a New Surveillance Reality. Human Rights Watch.Retrieved from https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality

[15] Kaye, D. (2019, November 26). The surveillance industry is assisting state suppression. It must be stopped. The guardian. Retrieved from https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware

[16] Egwuonwu, B. (2016, April 11). What Is Mass Surveillance And What Does It Have To Do With Human Rights? Retrieved from https://eachother.org.uk/explainer-mass-surveillance-human-rights/

interference in people's private lives.[17] It is also abusive in the sense that it might include shifting the ideal from "presumed innocent" to "people who have not been found guilty of a crime, yet."[18]

Facial recognition technology also enables a host of other abuses and corrosive activities. This is not limited to but includes:

- Due process harms, which might include shifting the ideal[19] from "presumed innocent" to "people who have not been found guilty of a crime, yet."
- Facilitation of harassment[20] and violence.
- Denial of fundamental rights and opportunities, such as protection against[21] "arbitrary government tracking of one's movements, habits, relationships, interests, and thoughts."
- The suffocating restraint[22] of the relentless, perfect enforcement of law.
- The normalized elimination of anonymity and the right to disapppear.[23]
- The amplification of surveillance capitalism.[24]

One of the main problems in terms of regulating facial recognition technology is that there exists a growing gap between public awareness and the rapid development and adoption of AI applications, which is made more significant as a result of increasing prioritization on security within the political sphere and a decline in human rights worldwide.[25] Additionally there is pressure from the private sector to protect industrial secrecy, which they see as essential to innovation and remaining competitive within the marketplace. In particular in application cases where the public sector employs AI for facial recognition, agencies find themselves in a conflict of interest between their organizational goals and the public interest

[17] OHCHR. (n.d.) International Covenant on Civil and Political Rights Article 17. . Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[18] Hartzog, W. (2018, August 2). Facial Recognition Is the Perfect Tool for Oppression. Medium. Retrieved from https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

[19] Slaughter, A.-M., & Hare, S. (2018, July 23). Our Bodies or Ourselves. Project Syndicate. Retrieved from https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-slaughter-and-stephanie-hare-2018-07?barrier=accesspaylog

[20] Facial recognition service becomes a weapon against Russian porn actresses. (2016, April 26). Retrieved from https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/

[21] Wehle, K. L. (2014, November 3). Anonymity, Faceprints, and the Constitution. George Mason Law Review, Vol. 21, No. 2, Winter 2014, pp. 409-466. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394838

[22] Chen, T. F. (2018, February 18). 22 eerie photos show how China uses facial recognition to track its citizens as they travel, shop — and even use toilet paper. Retrieved from: https://www.businessinsider.com/how-china-uses-facial-recognition-technology-surveillance-2018-2

[23] Selinger, E., & Hartzog, W. (2014, May 14). Obscurity and Privacy. Routledge Companion to Philosophy of Technology (Joseph Pitt & Ashley Shew, eds., 2014 Forthcoming). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866

[24] Zuboff, S. (2019). The Age of Surveillance Capitalism. Retrieved from https://shoshanazuboff.com/book/about/

[25] Comiter, M. (2019, August). Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Retrieved from https://www.belfercenter.org/publication/AttackingAI

in transparency and accountability.[26] Moreover, AI development and employment occur in a context of rapid innovation in an arms race with domestic and foreign competitors. Lastly, regulating innovation in the area of AI is often opposed based on the argument that public consultation processes slow down the innovation process, which may lead to competitive disadvantages or, in the case of applications relevant to national security, geopolitical vulnerability.[27]

Palestinian context

For years, Israel has been expanding its occupation of the Palestinian territories and annexation of East Jerusalem using mass surveillance technologies. Such policies and practices are enabled by a violently repressive security apparatus, designed to suppress any form of resistance to Israel's occupation and annexation,[28] while engineering a "façade of normalcy."[29] At the same time, Israel has become a world leader in cybersecurity technologies and home to the highest number per capita of surveillance companies in the world.[30] The state hosts a wide array of tech companies and in particular social media giants, whom the Israeli government and business sector have built strong political relationships with, producing practices and policies that impact Palestinian digital rights and human rights globally. It is well documented that Israel's prominence in the surveillance industry stems from the close links between the Israeli military and the private sector, as well as investment from international companies, and governments.[31]

In 2004, the International Court of Justice held that international law places certain obligations not only on Israel but also on third parties. These obligations include not rendering aid or assistance in maintaining the situation created by an unlawful act in occupied Palestinian territory and seeing to it that any impediment to the exercise by the Palestinian people of its right to self-determination is brought to an end. [32] Funding like Horizon 2020,[33] which supports research projects in the IT and surveillance sector[34]

[26] Whittaker, M. et al. AI Now Report 2018. (2018). AI Now Institute. Retrieved from: https://ainowinstitute.org/AI_Now_2018_Report.pdf

[27] Comiter, M. (2019, August). Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Belfer Center. Retrieved from https://www.belfercenter.org/publication/AttackingAI

[28] Who Profits. (2018, November). "Big Brother in Jerusalem's Old City: Israel's Militarized Surveillance System in Occupied East Jerusalem." Retrieved from: https://www.whoprofits.org/wp-content/uploads/2018/11/surveil-final.pdf

[29] Volinz, L. (2017, Feb). "Comparative Military Urbanism: Topographies of Citizenship and Security Threats in Brussels and Jerusalem", International Journal of Urban and Regional Research, ijurr.org.

[30] Privacy International. "The Global Surveillance Industry." (2016, July). Retrieved from https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

[31] Shezaf, H. and Jacobson, J. "Israeli Cyber Industry". (2018, October) Accessed at: https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

[32] International court of Justice. (2004, July). Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, AdvisoryOpinion, para. 159 .

[33] Israel and Europe Research Innovation Directive. (2019). Retrieved from: https://www.innovationisrael.org.il/ISERD/contentpage/israel-participation-horizon-2020

[34] Stop the Wall (2011). "European funding for Israeli actors that are complicit with violations of international law must not be allowed to continue" Retrieved from: https://ec.europa.eu/research/horizon2020/pdf/contributions/post/palestinian_territory/stop_the_wall_campaign.pdf

between the EU and Israel, and US foreign aid defense funding to Israel, has had a large impact on the development of surveillance technologies in Israel and in many cases have been developed and tested at the expense of Palestinian human rights. Although this is no by means an exhaustive case, some examples include:

- Open Architecture for UAV-based Surveillance Systems (OPARUS) that received an EU subsidy of €11.88m for the development of Unmanned Ariel Vehicles, despite the fact that their use is illegal above Europe. Israeli Aerospace Industries (IAI) participated in the project. According to Human Rights Watch, armed Heron drones manufactured by IAI were involved in at least some of the deadly drone attacks on Palestinian civilians during Operation Cast Lead, which in total killed 29 civilians, eight of them children.[35]
- IDETECT4ALL, receiving an EU subsidy of €2.29m for the development of intruder detection and authentication optical sensing technology. According to the project website, the project is developing technology "to detect the presence of objects inside or in the surrounding area of restricted critical infrastructures".[36] One of the four Israeli companies in the consortium, Motorola Israel, provides very similar surveillance systems for at least twenty illegal Israeli settlements and the illegal apartheid wall.

The impact of Israeli surveillance technology on human rights is undeniable. Surveillance of individuals - often journalists, activists, opposition figures and critics - has been shown to lead to arbitrary detention, torture, and extrajudicial killings. The Israeli government is poorly managing the export of weapons-grade surveillance technologies by Israeli companies to countries violating human rights around the world.[37]

For years Israeli military has overtly and covertly collected photographs of Palestinians, creating fear amongst Palestinians and limiting their ability to participate in peaceful assemblies and to document human rights violations. Today, facial recognition technology enables expansive monitoring, infringing on Palestinians' right to privacy, and further limiting their right to freedom of expression and their ability to demand for their human rights to be respected. Mass surveillance technologies, including facial recognition, adopted by Israel are in violation of freedom of expression and the right to privacy. Additionally, mass surveillance technologies are also in violation of the ideal principle of "presumption of innocence."

Mabat 2000': Surveilling the Old City

As part of its unlawful annexation efforts, Israel has implemented various policies in order to achieve its stated demographic objective of 70:30 Israeli Jews to Palestinians in the city of Jerusalem.[38] The Old City of Jerusalem represents a microcosm of these policies, where Israel seeks to create a coercive

[35] Precisely Wrong. (2009). Human Rights Watch. Retrieved from: http://www.hrw.org/en/reports/2009/06/30/precisely-wrong-0

[36] iDetecT4ALL (2010) Product descriptionhttp://www.idetect4all.com/category/produc

[37] Defense News (2013). "Israel defense industry exports under scrutiny". UPI. Retrieved from: https://www.upi.com/Defense-News/2013/07/19/Israeli-defense-industry-exports-under-scrutiny/11581374259134/

[38] Al-Haq, Law in the Service of Man. (2019, February 13). The Surveillance Industry and Human Rights: Israel's Marketing of the Occupation of Palestine Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Retrieved from http://www.alhaq.org/cached_uploads/download/alhaq_files/images/stories/PDF/Submission_to_the_UN_Special_Rapporteur_on_the_Promotion_and_Protection_of_the_Right_to_Freedom_of_Opinion_and_Expression.pdf

environment aimed at driving Palestinians out of the city.[39] To this end, Israel launched the 'Mabat 2000' project in the Old City, which is a system of 320-400,[40] closed-circuit television (CCTV) cameras capable of maneuvering 360 degrees to follow and track movements."[41] Since the launch of this project in 2000, the Israeli police have increasingly integrated pan-optic visual surveillance as part of its strategy in Jerusalem, relying on the software used to allegedly predict behavior based on algorithms.[42] The use of algorithms as part of "predictive policing" methods have been subjected to critique by scholars who have highlighted the biased and discriminatory nature of its application. These policing methods support subordination, targeting and discrimination against specific groups. In the words of Israel's former Public Security Minister, Gilad Erdan (most recently appointed the Regional Cooperation Minister of Israel), "The algorithm leads you to suspect someone."[43]

In 2014, Resolution 1775 was approved by the Israeli government and puts forward a strategy for increasing security in East Jerusalem and in Palestinian communities within the Green Line.[44] Since then, the plan has been reinforced and expanded.[45] In 2015, the Jerusalem Police district plan included the investment of 48.9 million NIS in the strengthening, purchase and installation of CCTV cameras and surveillance technology in East Jerusalem.[46] Since that time, over 200 Palestinians on both sides of the Green Line have been preemptively arrested using data analysis technology.[47] This was followed in 2017, by the Israeli government pledge to upgrade the system Mabat system to include enhanced facial recognition abilities, in order to detect if an individual is carrying a weapon, including concealed weapons, and providing full profiles of individuals who walk through the streets of the Old City.[48] In that same

[39] Al-Haq, Law in the Service of Man. (2019, February 13). The Surveillance Industry and Human Rights: Israel's Marketing of the Occupation of Palestine Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Retrieved from http://www.alhaq.org/cached_uploads/download/alhaq_files/images/stories/PDF/Submission_to_the_UN_Special_Rapporteur_on_the_Promotion_and_Protection_of_the_Right_to_Freedom_of_Opinion_and_Expression.pdf

[40] Jerusalem's Mabat 2000: Catching terrorists in the act, Ynetnews, 18 November 2015, https://www.ynetnews.com/articles/0,7340,L-4727621,00.html

[41] The Eyes of the Old City: 'Mabat 2000' Captures All, The Jerusalem Post, 18 June 2013, https://www.jpost.com/National-News/The-eyes-of-the-Old-City-Mabat-2000-captures-all-316885

[42] "Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem, Who Profits, November 2018, Retrieved from https://whoprofits.org/wp-content/uploads/2018/11/surveil-final.pdf

[43] Agencies, "Police Minister: Social Media Monitoring has foiled 200 terror attacks", The Times of Israel, 12 June 2018. Retrieved from: https://www.timesofisrael.com/police-minister-social-media-monitoring-has-foiled-200-terror-attacks/

[44] Prime Minister's Office. (2014, June). "Resolution 1775: The Plan to Increase Personal Security and Socio-Economic Development in Jerusalem for the Benefit of All its Residents" Retrieved in (Hebrew) from: https://www.gov.il/he/departments/prime_ministers_office

[45] Ministry of Public Security, "Budget Propos-al for the Year 2019." Retrieved in (Hebrew) from: mof.gov.il.

[46] Hasson, Yaniv Jovovich and Harel, A. (2015, Jan). "The Police Plan for Jerusalem: Placing Another 1,000 Policemen and Setting Up Stations in Arab Neighbor-hoods" Retrieved in (Hebrew) from Haaretz News.

[47] Associated Press. (2018, June). "Israel claims 200 attacks predicted, prevented with data tech", CBS News, Retrieved from: https://www.cbsnews.com/news/israel-data-algorithms-predict-terrorism-palestinians-privacy-civil-liberties/

[48] "Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem, Who Profits, November 2018, Retrieved from https://whoprofits.org/wp-content/uploads/2018/11/surveil-final.pdf

summer, Palestinians in East Jerusalem protested the installation of metal detectors and CCTVs at the Al Aqsa mosque, forcing the Israeli government to remove them.[49] In response, the Israeli government announced the investment of 100 million NIS in enhancing and upgrading its already invasive visual surveillance system in the Old City.[50] The upgrade includes the installation of advanced software which can provide the po-lice with facial recognition abilities, the ability to detect if an individual is carrying a weapon, including concealed weapons, and providing full profiles of individuals who walk through the streets of the Old City, including "suspects from the West Bank"[51]

As disturbing as the actions of the Israeli state are, perhaps the more significant element contributing to their ability to continue their oppressive policies can be understood through an examination of the depth and scale of the public-private partnership between the Israeli state and for-profit corporations in implementing these visual surveillance systems in East Jerusalem. A prime example can be seen in an examination of Athena, a fully owned subsidiary of C. Mer Group, and the main company providing soft-ware for 'Mabat 2000.' Established by Shabtai Shavita[52], former head for the Israeli National Intelligence Agency (Mossad), in 2003, Athena sells advanced espionage solutions for cameras and cyber surveillance, boasting software that can "predict to prevent" and the ability to detect the "wolf in sheep's clothing."[53] To do this, the company offers customers three products: OSCAR, OS-CAR + and SAIP. This software engages in constant collection of data and analytical cross-matching of information and metadata from – multilingual texts, images and videos, websites, social media, dark-net, and more – creating profiles of individuals and "identifying persons of interest."[54] An additional example can be found in Everon Systems CCTV camera which includes facial recognition technology in the Old City and whose headquarters is located in the Hebrew University, in which part of it is located in occupied East Jerusalem.[55] Through the use of Evron's Aureus 3D-AI facial recognition technology, Israel can analyze still and video footage, as well as harness this technology's ability to use 3D technology, sophisticated algorithms and computer intelligence.[56]

Microsoft and AnyVision

In July of 2018, Brad Smith, the president of Microsoft shared the corporation's views about the need for government regulations and responsible industry measures to address advancing facial recognition technology. Smith noted that facial recognition technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression and that these issues

[49] Al Jazeera. (2017, July). "Israel removes metal detectors from al-Aqsa compound", Al-Jazeera. Retrieved from: https://www.aljazeera.com/news/2017/07/israel-removing-metal-detectors-al-aqsa-compound-170724214814179.html

[50] Itamar Ekhner and Hassan Shalan, "The Cabinet decided to remove the magnetometers, praying: "We will not enter the Temple Mount" (He-brew), Yediot Ahronot, 25 July 2017

[51] Tal Shelo, "The Cabinet Decided to Remove Metal Detectors and Cameras from the Entrance to Temple Mount" (Hebrew), Walla News, 25 July 2017.

[52] Weizmann Institute of Science. (n.d.). Shabtai Shavit. Retrieved May 19, 2020, from http://www.weizmann.ac.il/conferences/InternationalBoard2016/shabtai-shavit

[53] Athena, "Oscar – Open Source Collection and Analysis Solution" Retrieved from: https://Athenaiss.com .

[54] Ibid

[55] Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem, Who Profits, November 2018, Retrieved from https://whoprofits.org/wp-content/uploads/2018/11/surveil-final.pdf

[56] Evron Systems Ltd., "Facial Recognition Software." Retrieved from: www.evronsystems.co.il

heighten responsibility for tech companies that create these products.[57] Then in December 2018, Smith laid out Microsoft's 'Facial recognition Principles', which encompass: Fairness, transparency, Accountability, Non-discrimination, Notice and Consent and Lawful Surveillance.[58] Then in 2019, several technology giants including Microsoft developed public relations campaigns that stress the ethical superiority of their facial recognition technology in response to public pressure to ensure that facial recognition technology is not being developed and used in ways that violate human rights. In contradiction with their own guiding principles on facial recognition technology, in June of 2019, Microsoft's M12 venture capital arm announced it was joining American and European companies, including LightSpeed Venture Partners, Robert Bosch and Qualcomm Ventures in a $78 million Series A funding round for AnyVision.[59] Considering that Microsoft published their six ethical principles to govern its use of facial recognition technology prior to its decision to fund AnyVision, it is particularly in violation of their sixth principle which states, "We (Microsoft) will advocate for safeguards for people's democratic freedoms in law enforcement surveillance scenarios and will not deploy facial recognition technology in scenarios that we believe will put these freedoms at risk."[60]

AnyVision is an Israeli company, which is headquartered in Israel but has offices in the United States, the United Kingdom and Singapore. It sells an "advanced tactical surveillance" software system, Better Tomorrow, which lets customers identify individuals and objects in any live camera feed, such as a security camera or a smartphone, and then track targets as they move between different feeds.[61] It is undeniable that there is a strong connection that can be drawn between AnyVision and the Israeli government, including the fact that the former Mossad chief Tamir Pardo heads the AnyVision advisory board, whilst the president is Amir Kain, former head of the defense ministry's security department.[62] In addition to being led by former Israeli military and intelligence personnel, AnyVision was also the recipient

[57] Smith, B. (2018, July 13). Facial recognition technology: The need for public regulation and corporate responsibility. Retrieved from: https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

[58] Sauer, R. (2018, December 17). Six principles to guide Microsoft's facial recognition work. Microsoft. Retrieved from: https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/

[59] Brewster, T. (2019, August 1). Microsoft Slammed For Investment In Israeli Facial Recognition 'Spying On Palestinians.' Forbes. Retrieved from: https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/#33e978e46cec

[60] Microsoft set to divest from Israeli facial recognition firm tracking Palestinians (2020, March 28). Middle East Eye. Retrieved from: https://www.middleeasteye.net/news/microsoft-set-divest-israeli-facial-recognition-firm-tracking-palestinians

[61] Salon, O. (2019, October 28). Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians? NBC News. Retrieved from: https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

[62] Brewster, T. (2019, August 1). Microsoft Slammed For Investment In Israeli Facial Recognition 'Spying On Palestinians.' Retrieved from: https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/#33e978e46cec

of Israel's top defense prize in 2018.[63] While not publicly named as the winner due to the classified nature of the surveillance project, five sources familiar with the matter confirmed to NBC News in October of 2019, that AnyVision's technology powers a secret military surveillance project throughout the West Bank.[64] One source said the project is nicknamed "Google Ayosh," where "Ayosh" refers to the occupied Palestinian territories and "Google"[65] denotes the technology's ability to search for people.[66] Furthermore, despite the company's claim of the benign use of their software, one of the company's technology demonstrations shows that the facial recognition system has been used to track suspects through occupied East Jerusalem and activists have spotted dozens of cameras 'deep inside the West Bank.'[67] This clear promotion of the idea that governments should have the ability to track individuals without consent is a flagrant disregard for their human rights. It is important to note however that despite criticism and mounting evidence, AnyVision continues to deny that its facial recognition technology has been developed with Israel and used to surveil Palestinians in the West Bank, claiming that it is only used on Israeli border crossings and at checkpoints.[68]

Considering AnyVision's track record many found it disappointing that Microsoft would invest in such an organization. In response to this investment, Shankar Narayan, the Director of Technology and Liberty Project at the American Civil Liberties Union (ACLU) claimed that "This particular investment should not be seen as a big surprise---there's a demonstrable gap between action and rhetoric in the case of most big tech companies and Microsoft in particular" he said.[69] Unsurprisingly, this investment led to public

---

[63] Kim, G. (2019, December 12). Microsoft funds facial recognition technology secretly tested on Palestinians throughout the Occupied Territories. Retrieved from https://www.alaraby.co.uk/english/Comment/2019/12/19/Microsoft-funds-facial-recognition-technology-secretly-tested-on-Palestinians

[64] Salon, O. (2019, October 28). Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?. NBC News. Retrieved from: https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116
secretly watched West Bank Palestinians. Retrieved from https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

[65] Google has publicly stated that they have no connection to this project or to AnyVision.

[66] Salon, O. (2019, October 28). Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians? NBC News. Retrieved from: https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

[67] Ziv, A. Haaretz. This Facial Recognition Startup is Secretly Tracking Palestinians. (2019, July 15). Retrieved from https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359

[68] Al-Arabiya. (2019, November 16). Microsoft to probe Israeli facial recognition company accused of 'unethically' tracking Palestinians. Retrieved from: https://www.alaraby.co.uk/english/news/2019/11/16/microsoft-probes-israeli-facial-recognition-accused-of-tracking-palestinians

[69] Brewster, T. (2019, August 1). Microsoft Slammed For Investment In Israeli Facial Recognition 'Spying On Palestinians.' Forbes. Retrieved from: https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/#33e978e46cec

outcry by activists and civil society actors, who pointed to evidence that AnyVision has been identified as wielding its software to help enforce Israel's military occupation.[70] Even with global coordinated efforts from a number of civil society organizations[71] including public petitions, it was only in October 2019, after an investigative report into the deal broke in NBC News[72] that Microsoft responded and decided to investigate whether the use of facial recognition technology developed by AnyVision complied with its ethics and principles.[73]

In late 2019, taking the allegations seriously, Microsoft hired Eric Holder and his team at the law firm of Covington & Burling to conduct an audit of facial recognition company AnyVision to determine whether it complies with Microsoft's ethical principles on how the biometric surveillance technology should be used. [74] At that time Microsoft spokesman said, "If we discover any violation of our principles, we will end our relationship."[75] In response to the audit, AnyVision said at the same time, "All of our installations have been examined and confirmed against not only Microsoft's ethical principles, but also our own internal rigorous approval process."[76]

In March 2020, Microsoft and AnyVision published a joint statement: "After careful consideration, Microsoft and AnyVision have agreed that it is in the best interest of both enterprises for Microsoft to divest its shareholding in AnyVision."[77] It is important to note that the findings of the audit did not find evidence to support the allegations about a mass surveillance program in the West Bank, and concluded that AnyVision had not violated its facial recognition pledge. Despite the positive outcome from the audit, there are many who point to the fact that much of the project information related to AnyVision's work was deemed as related to Israeli national security and therefore was not accessible by Holder and his team.

---

[70] Jewish Voice for Peace. (2019). Retrieved from: https://dropanyvision.org

[71] Kim, G. (2019, December 12). Microsoft funds facial recognition technology secretly tested on Palestinians throughout the Occupied Territories. Al Arabiya. Retrieved from https://www.alaraby.co.uk/english/Comment/2019/12/19/Microsoft-funds-facial-recognition-technology-secretly-tested-on-Palestinians

[72] Solon, O. (2019, October 26). Why did Microsoft fund an Israeli firm that surveils West Bank citizens? NBC News. Retrieved from: https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

[73] Dastin, J. (2019, November 16). Microsoft to probe work of Israeli facial recognition startup it funded. Reuters. Retrieved from: https://www.reuters.com/article/us-microsoft-AnyVision/microsoft-to-probe-work-of-israeli-facial-recognition-startup-it-funded-idUSKBN1XQ03M

[74] Solon, O. (2019, November 16). Microsoft hires Eric Holder to audit AnyVision overuse of facial recognition on Palestinians According to five sources, AnyVision's technology has powered a secret military surveillance project that has monitored Palestinians in the West Bank. Retrieved from https://www.nbcnews.com/tech/security/microsoft-hires-eric-holder-audit-AnyVision-over-use-facial-recognition-n1083911

[75] Solon, O. NBC News. Why did Microsoft fund an Israeli firm that surveils West Bank citizens? (2019, October 26). Retrieved from https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

[76] Ibid

[77] Joint Statement by Microsoft & AnyVision – AnyVision Audit. (2020, March 27). Retrieved from https://m12.vc/news/joint-statement-by-microsoft-AnyVision-AnyVision-audit/

However, AnyVision did acknowledge that its technology has been deployed at border checkpoints between the West Bank and Israel.[78] Even so, Microsoft said that as a result of the probe it decided to exit the business of investing in facial recognition startups altogether. "For Microsoft, the audit process reinforced the challenges of being a minority investor in a company that sells sensitive technology, since such investments do not generally allow for the level of oversight or control that Microsoft exercises over the use of its own technology," Microsoft and AnyVision said in a joint statement posted on M12's website.[79] This does not however speak to the internal development of facial recognition software within Microsoft.

Recommendations

Israel

1. Israel must uphold its obligations under International Humanitarian Law and its obligation to protect human rights as outlined in the Universal Declaration of Human rights. Israel must remove all cameras from East Jerusalem, the West Bank and Gaza.
2. Israel must cease to collect, store or transfer any data of Palestinians and respect the right to privacy as defined in Article 17 of the ICCPR
   > *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
   > *2. Everyone has the right to the protection of the law against such interference or attacks*
3. Israel shall follow the recommendations of the United Nations Special Rapporteur on Freedom of Expression and Opinion and immediately halt the export of all surveillance technologies until international safeguards and regulations are in place.
4. Israel shall conduct human rights audits of surveillance technology companies and ensure that their technology does not violate human rights.
5. Israel shall revoke the export licenses of any companies that have been known to violate human rights.
6. Israel shall increase the transparency of the relationships between the military and technology companies, in particular in terms of how the technology is being used unlawfully in the occupied territories or in the targeting of Palestinians.
7. Israel shall develop laws that protect privacy and human rights against the misuse of this surveillance technology, this also needs to be supported by the courts and the emphasis on security can not be used to excuse such gross human rights violations.

[78] Microsoft Divests from AnyVision After Audit into Alleged Mass Surveillance Program. (2020, March 31). Retrieved from https://findbiometrics.com/microsoft-divests-AnyVision-following-audit-into-alleged-mass-surveillance-program-033104/

[79] Microsoft to divest AnyVision stake, end face recognition investing. (2020, March 30). IT News. Retrieved from: https://www.itnews.com.au/news/microsoft-to-divest-AnyVision-stake-end-face-recognition-investing-540033

Third-Party States

States must not be complicit with violations of international law and Palestinian Rights and must take specific measures to ensure the protection of the law against such interference.

1. ***States** purchasing surveillance* technologies should take measures to ensure that their use is in compliance with international human rights law. This includes reinforcing national laws limiting surveillance, creating public mechanisms for approval and oversight of surveillance technologies, and ensuring that victims of abuse have domestic legal tools of redress.
2. ***States** licensing the export* of surveillance technologies should request public input and conduct consultations and should ensure transparency in licensing. States that have not yet done so should join the existing Wassenaar Arrangement, which in turn should develop a framework for the human rights review of companies to ensure their compliance with the UN Guiding Principles.
3. **States** must demand that when a company provides mass surveillance technology or equipment without adequate safeguards in place, or where information is used in violation of human rights, that companies risk being complicit in or otherwise involved with human rights abuse.
4. **States** must not use surveillance measures that *arbitrarily or unlawfully interfere* with an individual's privacy, family, home or correspondence as this is a violation of Article 17 (Right to Privacy) of the ICCPR.[80]
    1. Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed.[81]
    2. Mass or "bulk" surveillance programs may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.[82]

Technology Company principles must be applied to the use/support of the development of mass surveillance technology. It is therefore recommended that the case of Microsoft be taken as a good example of establishing standards and holding partners accountable to these principles. However it is important to recognize that this result in the case of AnyVision was directly connected to the work of digital rights activists, human rights defenders and journalists applying pressure.

1. Technology companies need to support the development of co-regulatory initiatives that develop rights-based standards for surveillance technologies and implement these standards through independent audits, and learning and policy initiatives.

---

[80] General comment No.16 on Article 17 of the ICCPR. Retrieved from: https://www.refworld.org/docid/453883f922.html

[81] Article (19), "*NECESSARY & PROPORTIONATE International (Principles on the Application of Human Rights Law to Communications Surveillance).*" OHCHR, May 2014 Retrieved from: https://www.ohchr.org/Documents/Issues/RuleOfLaw/PCVE/Article_19.pdf

[82] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2014, March). Retrieved from https://www.ohchr.org/en/issues/freedomopinion/pages/opinionindex.aspx

2. Measure of monitoring and oversight needs to ensure human rights due diligence. Potential rights harming outcomes should be identified and effective action take to prevent and manage harms as well as track responses.
3. Technology must include transparency and explainability and explain to voluntary users how the technology will be used in a clear way that provides meaningful information about how the AI works and how their data is being collected, stored and protected
4. Internal accountability mechanisms are needed and companies should ensure individuals have access to meaningful remedy and redress.

Digital Rights Activists, Human Rights Defenders and Journalists need to continue to coordinate and share their information in order to not only identify violations of human digital rights, but also in order to raise awareness of the public.

1. Support legal action and apply pressure on corporations and governments in order to ensure the protection of human rights within the development of facial recognition technology
2. Engage with International (UN bodies) and Regional organizations (EU, NATO, African League, etc.) in order to bring about consensus around the legal framework to protect human rights threatened by mass surveillance technologies and innovations in facial recognition technology
3. Call for collective action to reject unlawful mass surveillance.
4. Inform the public of their rights and empower them with tools to protect themselves.