International Review of the Red Cross (2020), **102** (914), 823–849.
Emerging Voices
doi:10.1017/S1816383121000746

IRRC

EMERGING VOICES

Automating occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory

Rohan Talbot
Rohan Talbot is Advocacy and Campaigns Manager at Medical Aid for Palestinians (MAP). Email: rohan.talbot@gmail.com.

Abstract

In 2019, media investigations revealed that Israel had added facial recognition technologies (FRTs) to the panoply of security and surveillance technologies deployed in its administration and control of the occupied Palestinian territory (oPt). Despite growing academic and judicial scrutiny of the legal implications of these technologies for privacy and freedom of assembly in domestic contexts, scant attention has been paid to their uses by militaries in contexts where international humanitarian law (IHL) applies. This article seeks to establish the international legal framework governing an Occupying Power's deployment of FRTs, particularly in surveillance, and apply it to Israel's uses in the oPt. It is demonstrated that IHL provides flexible, but incomplete, provisions for balancing an Occupying Power's

right to employ surveillance technologies within its measures of control and security against the imprecisely defined humanitarian interests of the population under occupation. The relevant legal framework is completed through the concurrent application of an Occupying Power's international human rights law (IHRL) obligations. What is known of Israel's use of FRTs in surveillance appears prima facie *not to satisfy the cumulative IHRL criteria for limitations on the right to privacy – legality, legitimate aims, necessity and proportionality – even where these are broadened by reference to IHL. Consideration is also paid to corollary human rights impacts of these technologies, and the potential that they may entrench an Occupying Power's control while simultaneously rendering this control more invisible, remote and less reliant on the physical presence of troops.*

Keywords: international humanitarian law, surveillance technologies, facial recognition technologies, law of occupation, international human rights law, right to privacy.

Introduction

Recent advancements in artificial intelligence (AI) have given rise to security and surveillance technologies of hitherto unthinkable scope, speed and intrusiveness. At least seventy-five governments are known to use AI-powered surveillance technologies,[1] including "predictive policing" systems that aggregate and analyse data to predict potential crime, "smart city" platforms that monitor crowd behaviour, and facial recognition technologies (FRTs) which permit rapid, covert and automated identification of individuals from distance.

To policing and intelligence agencies, FRTs promise increased reach and efficiency in the surveillance of perceived security threats and criminals. The mass processing of biometric data and identification of individuals in public spaces means that FRTs may, however, interfere with privacy on a massive scale. Ethical and legal debates have inevitably arisen, particularly concerning compliance of States' domestic uses of FRTs with their human rights obligations. These technologies are also increasingly deployed by militaries in the conduct of hostilities and the control of populations and territories held under occupation. Nevertheless, the international legal framework governing such uses remains largely unexplored.

This article will first describe the contemporary domestic uses of FRTs and concerns that have arisen regarding civil liberties and freedoms. Application of FRTs by militaries will then be briefly examined, focusing on recent media revelations regarding Israel's reported deployment of FRTs at checkpoints and in automated surveillance inside the occupied Palestinian territory (oPt).

1 Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace Working Paper, September 2019, available at: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf (all internet references were accessed in November 2021).

International humanitarian law (IHL) will then be applied to Israel's use of FRTs within its security measures in the oPt. It will be demonstrated that the law of occupation provides a flexible framework applicable to contemporary occupations and technologies, but grants only general guidance for balancing the humanitarian interests threatened by FRTs with the military exigencies of the Occupying Power, creating a *lacuna* that may be filled by international human rights law (IHRL).

Israel's obligations toward Palestinians' right to privacy under IHRL, and the permissible limitations on this right, will then be analysed. It will be concluded that Israel's reported use of FRTs in surveillance appear *prima facie* to fail to satisfy the cumulative requirements of lawfulness, legitimate aims, necessity and proportionality, even where these are interpreted by reference to the more permissive framework of IHL as the body of law which specifically applies to contexts of belligerent occupation. Finally, the broader human rights implications of FRTs will be briefly considered, including the potential that such technologies may entrench and further prolong occupations, while simultaneously rendering an Occupying Power's control more invisible, remote and less reliant on the physical presence of troops.

Facial recognition technologies – a new challenge to human rights

Facial recognition technologies

FRTs are computer systems that identify individual humans from digital photographs or video according to their unique facial feature characteristics. Modern AI-powered systems use algorithmic techniques to isolate and detect patterns from faces, convert these into mathematical representations ("templates"), and statistically compare these to other facial data stored in a database.[2] These algorithms are trained on large datasets of faces, often taken from public sources.[3]

There are two primary applications for FRTs. Verification systems involve one-to-one matching of a face against a single reference template, and are used to confirm a person's official identity.[4] Identification, or one-to-many, FRTs compare captured templates against a database to establish whether the identity of the person is known.[5] Such algorithms can "be deployed in anything from cell

2 Benda Leong, "Facial Recognition and the Future of Privacy: I Always Feel Like … Somebody's Watching Me", *Bulletin of the Atomic Scientists*, Vol. 75, No. 3, 2019, p. 110.
3 Madhumita Murgia, "Who's Using Your Face? The Ugly Truth About Facial Recognition", *Financial Times*, 19 April 2019, available at: https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e.
4 Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York University Press, New York, 2011, p. 18.
5 B. Leong, above note 2, p. 109.

phones to large multi-server search engines" and are claimed to be "capable of searching over 100,000,000 faces in just a few seconds".[6]

These technologies have valuable applications for a variety of actors. Companies deploy facial verification to prevent banking fraud and offer security protection for mobile phones. Social media corporations use facial identification to help users "tag" others in photographs. The International Committee of the Red Cross (ICRC) has tested FRTs to aid family tracing for those affected by conflict.[7]

FRTs also form part of the post-millennium boom in new security technologies. Alongside predictive policing and digital surveillance technologies, their development has been fuelled in part by the perceived exigencies of national security and counterterrorism since 2001, and advancements in AI, camera technology and computer processing power.[8] FRTs are deployed to control movement, verifying identities of those crossing borders or accessing secure buildings, and enabling investigation or exclusion of those deemed a security threat.[9] Police and intelligence agencies use FRTs to compare faces from crime-scene photographs and video against mugshot databases to provide investigatory leads.[10] The U.S. Federal Bureau of Investigations' Next Generation Identification System permits law enforcement agencies to search a database of thirty million criminal photographs and has access to wider state and federal databases of non-criminal facial images, such as visa applications and driver licences.[11]

Live facial recognition (LFR) systems integrate automated facial recognition into live video feeds, allowing operators to scan public spaces to identify people in real time, matching against "watch lists" of wanted individuals such as criminals or suspected terrorists.[12] Police forces in the United Kingdom, for example, have deployed LFR at sports events, shopping centres and protests.[13]

LFR systems are promoted as "a potential solution to … problems of surveillance labor and video overload".[14] Though facial recognition functions can be done by humans, automation makes verification and identification more efficient, reducing human resource costs and issues of distraction or fatigue, and vastly expanding the number of possible comparisons in a given time.[15] By

6 Brian Martin, *Statement before U.S. Senate Judiciary Committee Subcommitee on Privacy, Technology, and the Law: "What Facial Recognition Technology Means for Privacy and Civil Liberties"*, 18 July 2012, p. 4, available at: https://www.judiciary.senate.gov/imo/media/doc/12-7-18MartinTestimony.pdf.

7 ICRC, "Rewards and Risks in Humanitarian AI: An Example", *Inspired Blog*, 6 September 2019, available at: https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence.

8 Kelly A. Gates, "Identifying the 9/11 'Faces of Terror'", *Cultural Studies*, Vol. 20, No. 4–5, 2006, p. 417.

9 *Ibid.*

10 B. Leong, above note 2, p. 112.

11 Gretta L. Goodwin, "Testimony Before the Committee on Oversight and Reform, House of Representatives", *United States Government Accountability Office*, 2019, p. 12, available at: https://www.gao.gov/assets/gao-19-579t.pdf.

12 Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing*, London, May 2018, p. 5, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

13 *Ibid.*, p. 1.

14 K. A. Gates, above note 4, p. 64.

15 *Ibid.*

identifying individuals at distance, without physical contact, and using a feature usually visible in public, FRTs are less physically obtrusive, or more covert, than other biometric technologies, such as fingerprint scanners.[16]

Ethical and legal issues

The ability to discover people's identities, without their knowledge, on a mass scale, opens a new frontier of concern regarding privacy and freedoms. This is made more acute given the exponential growth of personal data held by governments and corporations – including social media profiles, social connections and interactions, location history, and financial information – to which identification through FRTs may facilitate access.[17] U.S. Senator Al Franken aptly described these concerns:

> Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores that you visit, the Government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you.[18]

FRTs are also situated within wider national projects of bureaucratization and mass individuation. Establishing and verifying the identity of individuals has become central to the interaction between State and citizen, regulating participation in public life, such as accessing services or crossing borders. The "securitization" of these identities, Gates argues, has increasingly become:

> a means of tying individuals into circuits of inclusion and exclusion, determining their status as legitimate self-governing citizens or more problematic identities deemed to fall outside the realm of legal rights who can therefore be subjected to a range of repressive strategies.[19]

New digital surveillance technologies including FRTs have been deployed by States in ways that "produce racially discriminatory structures that holistically or systematically undermine enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics".[20]

The use of FRTs to intentionally restrict the rights or freedoms of individuals or populations with specific racial, ethnic or national identities is inherently discriminatory. FRTs may also have indirect discriminatory effects. As

16 *Ibid*., p. 46.
17 Alessandro Acquisti, Ralph Gross and Frederic Stutzman, "Face Recognition and Privacy in the Age of Augmented Reality", *Journal of Privacy and Confidentiality*, Vol. 6, No. 2, 2014, p. 1.
18 Al Franken, *Opening Statement before U.S. Senate Judiciary Committee Subcommitee on Privacy, Technology, and the Law: "What Facial Recognition Technology Means for Privacy and Civil Liberties"*, 18 July 2012, available at: https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/html/CHRG-112shrg86599.htm
19 K. A. Gates, above note 4, p. 34.
20 Tendayi Achiume, Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc. A/HRC/44/57, 18 June 2020, paras. 38–43.

Leong highlights, "[b]y using machine learning programs as the underlying foundation, these systems are built on existing data that reflect human biases, and automate them".[21] Inherent algorithmic biases which cause higher rates of "false-positives" when identifying certain groups such as women and people of colour imbue these technologies with "a striking capacity to reproduce, reinforce and even to exacerbate racial inequality within and across societies".[22]

The use of FRTs during the policing of public demonstrations may also have a "chilling effect" on freedoms of assembly and expression.[23] During 2019 protests in Hong Kong, demonstrators expressed fears that FRTs were being used to identify and target them for arrest, leading many to don face masks.[24] Police in Russia have reportedly used Moscow's comprehensive LFR-enabled surveillance system to identify and detain journalists and activists taking part in peaceful demonstrations.[25]

At least sixty-four countries are known to use FRTs, including LFR surveillance systems.[26] The implications for privacy and other freedoms have prompted scrutiny of the compatibility of these uses with States' human rights obligations.[27] As with other modern surveillance technologies, they are often deployed with limited transparency, public oversight, or adequate domestic legal frameworks,[28] engendering calls for a moratorium on their use, sale and transfer.[29]

Military uses of face recognition technologies

Militaries have been at the vanguard of the development and deployment of FRTs since the 1960s.[30] As Gates explains: "The war-fighting promise of automated facial recognition … lay precisely in their potential to identify objects automatically and "at a distance", whether the final aim was to control, capture, or destroy these targets."[31] These functions are of increasing interest to militaries involved in counterterrorism and asymmetric warfare. The U.S. Military maintains a database of 7.4 million identities, including face scans, many

21 B. Leong, above note 2, p. 113.
22 T. Achiume, above note 20, para. 12.
23 Laura Mills and Maya Wang, "Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights", *Human Rights Watch*, 15 November 2019, available at: https://www.hrw.org/news/2019/11/15/facial-recognition-deal-kyrgyzstan-poses-risks-rights.
24 Rosalind Adams, "Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched", *BuzzFeed News*, 17 August 2019, available at: https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers.
25 Umberto Bacchi, "Fears Raised Over Facial Recognition Use at Moscow Protests", *Reuters*, 4 February 2021, available at: https://www.reuters.com/article/russia-protests-tech-idUSL8N2KA54T.
26 S. Feldstein, above note 1, p. 7.
27 See, for example, Pete Fussey and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Project Report, Universty of Essex Human Rights Centre, 2019.
28 David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35, 28 May 2019, para. 46; Amos Toh, "Rules for a New Surveillance Reality", *Human Rights Watch*, 18 November 2019, available at: https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality.
29 D. Kaye, above note 28, para. 66.
30 K. A. Gates, above note 8, p. 432.
31 K. A. Gates, above note 4, p. 104.

obtained during operations in Afghanistan and Iraq.[32] Its Automated Biometric Information System enables individuals placed on a watchlist to be "identified through surveillance systems on battlefields, near borders around the world, and on military bases".[33] Between 2008 and 2017, the U.S. military "used biometric and forensic capabilities to capture or kill 1,700 individuals [and] deny 92,000 individuals access to military bases".[34] The Turkish military has reportedly integrated FRTs into lethal unmanned aerial vehicles to aid targeting.[35]

Militaries may therefore use FRTs to control physical access to secured areas and to identify "wanted" individuals for detention, questioning, or even lethal targeting in contexts where IHL applies – namely armed conflicts and belligerent occupations. Nevertheless, the implications of IHL for military use of the technologies remain under-explored.

Israel's use of face recognition technologies in the occupied Palestinian territory

In 2019, investigations by *Haaretz*,[36] *NBC*[37] and *NPR*[38] reported that the Israeli army had deployed two FRT systems supplied by Israeli company AnyVision, in the oPt. The first, a verification system, was installed at twenty-seven checkpoints controlling access for Palestinians from the West Bank to East Jerusalem and Israel:

> Palestinians who request permits to enter Israel must first get photographed and fingerprinted at an Israeli military office. Their photos are stored in a biometric database and are connected to electronic ID cards they scan at the checkpoint. Facial recognition software at the checkpoint matches their face to their photos in Israel's biometric database.[39]

Around 450,000 Palestinians have electronic ID cards and are therefore known to have their facial data stored in databases by Israel.[40]

32 Dave Gershgorn, "This Is How the U.S. Military's Massive Facial Recognition System Works", *OneZero*, 6 November 2019, available at: https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.
33 *Ibid*.
34 United States Government Accountability Office, *DOD Biometrics and Forensics*, Report to Congressional Committees, August 2017, available at: https://www.gao.gov/assets/gao-17-580.pdf.
35 Daily Sabah, "Domestically-Developed Kamikaze Drones to Join Turkish Army's Inventory as of 2020", 12 September 2019, available at: https://www.dailysabah.com/defense/2019/09/12/domestically-developed-kamikaze-drones-to-join-turkish-armys-inventory-as-of-2020.
36 Amitai Ziv, "This Israeli Face-Recognition Startup is Secretly Tracking Palestinians", *Haaretz*, 15 July 2019, available at: https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359.
37 Olivia Solon, "Why Did Microsoft Fund an Israeli Firm that Surveils West Bank Palestinians?", *NBC News*, 28 October 2019, available at: https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116.
38 Daniel Estrin, "Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns", *NPR*, 22 August 2019, available at: https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc.
39 *Ibid*.
40 *Ibid*.

Israel has also deployed FRT verification to facilitate control over the movement of Palestinians in and out of neighbourhoods in Hebron, in the southern West Bank.[41] Here, again, FRTs are deployed to verify Palestinians' identity against a database of individuals permitted certain freedom of movement.

AnyVision also reportedly provided an LFR surveillance system, deployed "deep inside the West Bank [to] spot and monitor potential Palestinian assailants".[42] The Israeli military has installed more than 1700 surveillance cameras at "roads, intersections and in settlements" in the West Bank,[43] and AnyVision's software purportedly "lets customers identify individuals and objects in any live camera feed … and then track targets as they move between different feeds".[44] A significant visual surveillance infrastructure has been documented in the Old City in occupied East Jerusalem, including closed-circuit television (CCTV) cameras with visibility covering 95% of public areas, reportedly upgraded to include LFR capabilities.[45]

As is typical of States' surveillance practices, many details of the Israeli military's use of FRTs in the oPt are secret, though these reports are consistent with the known "plethora of new technologies, such as phone and internet monitoring and interception, CCTV, and biometric data collection [which] have enabled Israel to surveil the population it occupies on a massive, intrusive scale".[46] Israel is also known to monitor Palestinians' social media activity, and uses predictive policing algorithms to arrest those it considers guilty of "incitement" and that it deems a future security threat.[47]

The deployment of FRTs in the oPt raises similar ethical and legal issues to uses in domestic contexts, relating to the direct effects on privacy, and wider impacts on movement and other freedoms to which privacy is a gateway. Human rights organizations have accordingly expressed concerns about the lack of transparency around the use of these technologies, and their impact on Palestinians.[48] The specific legal framework governing FRT uses in occupied territory, however, currently remains under-explored.

41 Six checkpoints in the city were installed with FRTs in 2015, "allowing for total separation between the soldiers or Border Police officers staffing them and the Palestinians passing through them": see B'Tselem, *Playing the Security Card: Israeli Policy in Hebron as a Means to Effect Forcible Transfer of Local Palestinians*, Jerusalem, September 2019, p. 16.

42 A. Ziv, above note 36.

43 Amos Harel, "Israel Speeds Up Camera Placements in West Bank in Effort to Deter Terrorism", *Haaretz*, 22 June 2017, available at: https://www.haaretz.com/israel-news/.premium-idf-speeds-up-camera-placements-in-w-bank-in-effort-to-deter-terrorism-1.5485764.

44 O. Solon, above note 37.

45 Who Profits, *"Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem*, Tel Aviv, November 2018, pp. 4–11.

46 Nadim Nashif and Marwa Fatafta, *Surveillance of Palestinians and the Fight for Digital Rights*, Policy Brief, Al Shabaka, 23 October 2017, available at: https://al-shabaka.org/briefs/surveillance-palestinians-fight-digital-rights.

47 Human Rights Watch (HRW), *Born Without Rights: Israel's Use of Draconian Military Orders to Repress Palestinians in the West Bank*, New York, November 2019, pp. 48–9.

48 Shoshanna Solomon, "As AnyVision Probed, Israeli Watchdog Urges Curbs on Sales of Surveillance Tech", *Times of Israel*, 18 November 2019, available at: https://www.timesofisrael.com/as-anyvision-probed-israeli-watchdog-urges-curbs-on-sales-of-surveillance-tech.

Facial recognition technologies under the law of occupation

The applicability of international humanitarian law

During the 1967 war, Israel took military control over the West Bank, including East Jerusalem, from Jordan, and Gaza from Egypt.[49] As these Palestinian territories were "actually placed under the authority of a hostile army", and Israel established and exercised its authority, the criteria for determining the existence of a belligerent occupation under Article 42 of the Regulations annexed to the 1907 Hague Convention ("Hague Regulations") were met.[50]

The Government of Israel does not recognize the *de jure* applicability of the law of occupation to its actions in the oPt,[51] including the Fourth Geneva Convention (GC IV) to which it is a party. It asserts, however, that it applies the Convention's "humanitarian provisions" *de facto* without specifying which provisions those are.[52] The Israeli Supreme Court, nevertheless, accepts that Israel holds the West Bank at least under belligerent occupation, and has subjected Israel's conduct to judicial review on the basis of the Hague Regulations[53] and those provisions of GC IV that it considers to reflect customary IHL.[54]

The applicability of the law of occupation is affirmed by almost total unanimity among the international community,[55] demonstrated by successive United Nations (UN) Security Council (UNSC)[56] and General Assembly resolutions.[57] In its Advisory Opinion considering the legal consequences of Israel's building of the separation wall in the oPt ("Wall Opinion"), the International Court of Justice (ICJ) found that developments since 1967 "have done nothing to alter this situation", and that Israel remains an Occupying Power.[58]

Modern AI-powered security technologies, such as FRTs, were not envisioned by the drafters of the core IHL treaties, and are therefore not addressed directly by their provisions. Nevertheless, the law of occupation is imbued with inherent flexibility, enabling its application to the varied scenarios arising in contemporary occupations.[59] This includes two key treaty provisions

49 Eyal Benvenisti, *The International Law of Occupation*, 2nd ed., Oxford University Press, Oxford, 2012, p. 203.
50 Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land (entered into force 26 January 1910) (Hague Regulations), Art. 42.
51 E. Benvenisti, above note 49, p. 208.
52 *Ibid*., p. 206.
53 Supreme Court of Israel, *Beit Sourik Village Council v. Israel and IDF Commander in the West Bank*, HCJ 2056/04, 2004, para. 23.
54 Yoram Dinstein, *The International Law of Belligerent Occupation*, 2nd ed., Cambridge University Press, Cambridge, 2019, pp. 31–3.
55 Adam Roberts, "Prolonged Military Occupation: The Israeli-Occupied Territories Since 1967", *American Journal of International Law*, Vol. 84, No. 1, p. 69.
56 See, for example, UNSC Res. 2334, 23 December 2016.
57 See, for example, UNSC Res. 73/97, 18 December 2018.
58 International Court of Justice (ICJ), *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, *ICJ Reports 2004*, para. 78.
59 A. Roberts, above note 55, p. 51.

explored below, which provide an IHL framework governing the deployment of these new technologies.

The law of occupation: Balancing humanitarian imperatives and military exigencies

1907 Hague Regulations

The balancing of military exigencies and humanitarian imperatives is a core function of IHL. Article 43 of the Hague Regulations stipulates two duties of the Occupying Power: to "take all the measures in his power to restore, and ensure, as far as possible, public order and civil life",[60] and to do so "while respecting, unless absolutely prevented, the laws in force in the country".[61] Benvenisti characterizes this as "a sort of mini-constitution for the occupation administration; its general guidelines permeate any prescriptive measure or other acts taken by the occupant".[62]

The first duty requires the Occupying Power to protect the local population from a breakdown in both "security or general safety" and ensure continuance of "social functions [and] ordinary transactions which constitute daily life".[63] The caveats to this duty indicate that an Occupying Power is neither required to act beyond its means or the level of control it can exert, nor guarantee public order and civil life as an outcome.[64] These exceptions provide leeway to the Occupying Power to balance this duty against its own interests – including its security – as does the caveat in the second duty that it respects existing laws "unless absolutely prevented".

1949 Fourth Geneva Convention

GC IV further clarified an Occupying Power's humanitarian obligations toward the occupied population. Article 27 outlines the Convention's core humanitarian principle, asserting that protected persons, including civilians in occupied territory, "are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs" and that "[t]hey shall at all times be humanely treated, and … protected especially against all acts of violence or threats thereof".[65] These

60 While the ICRC's English translation references "public order and safety", a more authoritative translation of the original French ("l'ordre et le vie publics") is "public order and civil life". See Y. Dinstein, above note 54, p. 99.

61 Hague Regulations, above note 50, Art. 43.

62 E. Benvenisti, above note 49, p. 69.

63 Edmund Schwenk, "Legislative Power of the Military Occupant Under Article 43, Hague Regulations", *Yale Law Journal*, Vol. 54, No. 2, 1945, p. 398.

64 Marco Sassòli, "Legislation and Maintenance of Public Order and Civil Life by Occupying Powers", *European Journal of International Law*, Vol. 16, No. 4, 2005, p. 664.

65 Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) (GC IV), Art. 27(1).

duties are to be applied "without adverse distinction based, in particular, on race, religion or political opinion".[66]

Balancing these humanitarian duties, Article 27 also authorizes Occupying Powers to "take such measures of control and security in regard to protected persons as may be necessary as a result of the war".[67] This general provision permits the Occupying Power to take action necessary to address security threats arising from the occupied territory, and is flexible to a broad array of factual scenarios and measures. Pictet's *Commentary* to the Convention underlines that "[a] great deal is … left to the discretion of the Parties to the conflict as regards the choice of means". It also provides a non-exhaustive list of examples of permissible measures, including less intrusive restrictions such as requiring the carrying of identity cards or prohibiting the carrying of weapons, to harsher measures, such as assigned residence or internment.[68]

Facial recognition technologies under the law of occupation

Consistent with Hague Regulations Article 43's duty to "restore, and ensure … public order and civil life", an Occupying Power may seek to deploy FRTs to protect the security of the local population, much as they are used by police in a domestic context. FRTs may also be deployed within the "measures of control and security" permitted under GC IV, Article 27(4). Deployed at checkpoints within occupied territory, or crossings into the Occupying Power's sovereign territory, they may be intended to identify those permitted access and restrict those considered a security risk. In surveillance, FRTs may be deployed to help identify and capture individuals considered a threat, such as civilians taking direct part in hostilities.

FRTs deployed like this can, however, have adverse humanitarian effects on protected persons. Examining the role of digital technology in contexts where IHL applies, the ICRC has identified "potential humanitarian consequences – digital risks – for civilian populations from misuse of AI-enabled digital surveillance, monitoring and intrusion technologies", including FRTs, such as "being targeted, arrested, facing ill-treatment … or suffering from psychological effects from the fear of being under surveillance".[69] The ICRC further reports that "[u]nprecedented levels of surveillance of the civilian population" from such technologies "can exacerbate … existing vulnerabilities of persons affected by armed conflicts".[70]

66 *Ibid.*, Art. 27(3).
67 *Ibid.*, Art. 27(4).
68 Jean Pictet (ed.), *Commentary on the Geneva Conventions of 12 August 1949*, Vol. 4: *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, ICRC, Geneva, 1958, p. 207.
69 ICRC, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach", *International Review of the Red Cross*, Vol. 102, No. 913, 2020, p. 469.
70 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Report to 33rd International Conference of the ICRC, Geneva, 12 December 2019, p. 21.

In the oPt, LFR surveillance could further facilitate detention of Palestinian children, journalists and human rights defenders by Israel's security forces,[71] with clear impacts on the wellbeing of those affected. They are likely to exacerbate the "generalized feeling of being watched and surveilled" experienced by Palestinians under Israel's broader surveillance and control practices.[72]

Similarly, physical and bureaucratic restrictions on freedom of movement within the oPt, of which FRTs are now a key component at checkpoints, cause well-documented disruptions to family life, access to healthcare and livelihoods.[73] This is particularly true of Israel's isolation of East Jerusalem from the rest of the West Bank which, as the city is "an important centre for Palestinian economic, cultural and social activity, has a serious impact on surrounding communities".[74] FRTs are now an integral part of Israel's separation wall's "associated regime" of administrative measures, including permits and ID cards, that the ICJ considered "gravely infringe a number of rights of Palestinians".[75]

FRTs sit at the fulcrum of interests balanced by IHL. On the one hand, they may facilitate an Occupying Power's attempts to "ensure public order and civil life" and constitute "measures of control and security" enacted to ensure its own security. On the other, obtrusive surveillance and movement restrictions facilitated by these technologies may diminish "civil life" and undermine the local population's humanitarian interests.

Though an Occupying Power is granted significant discretion as to measures of control and security permissible under GC IV Article 27(4), this choice is not unlimited. Such measures deemed "necessary as a result of the war", including the deployment of FRTs, must be balanced against the duty to treat protected persons humanely "at all times", and that they be entitled "in all circumstances, to respect for their persons".[76]

Thus, an Occupying Power's control and security measures must be proportionate: the harm caused to protected persons must not be excessive in relation to the security interest being advanced. Indeed, in its judicial review of security measures imposed by Israel's security forces in the West Bank, the Israeli Supreme Court has recognized that proportionality, as a "general principle of international law", applies as the "standard for balancing the authority of the military commander in the area with the needs of the local population".[77]

Delineating the proportionality of such measures under IHL, however, is challenged by the lack of precision regarding the humanitarian interests to be balanced against the Occupying Power's security interests. Privacy and freedom of movement – threatened by FRTs – are not explicitly guaranteed to protected persons under GC IV Article 27(1) or other IHL treaty provisions.

71 Report of the High Commissioner for Human Rights, UN Doc. A/HRC/37/42, 21 February 2018.
72 Elia Zureik, "Strategies of Surveillance: The Israeli Gaze", *Jerusalem Quarterly*, No. 66, 2016, p. 14.
73 Report of the UN Secretary-General, UN Doc. A/HRC/31/44, 20 January 2016.
74 *Ibid*., para. 30.
75 ICJ, above note 58, paras. 133–7.
76 GC IV, above note 65, Art. 27(1).
77 Supreme Court of Israel, *Beit Sourik* case, above note 53, para. 39.

Pictet's *Commentary* provides some guidance in this regard, explaining that "respect for the person" in Article 27(1) "must be understood in the widest sense: it covers all the rights of the individual which are inseparable from the human being by very fact of his existence".[78] He identifies among those rights "in particular, the right to physical, moral and intellectual integrity – an essential attribute of the human person".[79]

Pictet identifies "[t]he right to personal liberty, and in particular, the right to move about freely" among individual rights covered implicitly by Article 27(1), providing some guidance on the balancing of interests: while this right "may certainly be restricted, or even temporarily suppressed, if circumstances so require" it is not to be "suspended in a general manner".[80] Rather, Pictet argues, "the regulations concerning occupation … are based on the idea of the personal freedom of civilians remaining in general unimpaired".[81]

Regarding "respect for intellectual integrity", Pictet makes limited reference to the privacy of protected persons by asserting that: "[i]ndividual persons' names or photographs, or aspects of their private lives must not be given publicity".[82] Relatedly, Article 27(2) requires that protected persons be afforded protection against "public curiosity". However, the prohibition on the "publicity" of private information and protection from "public curiosity" do not encapsulate a full protection of an individual's privacy. In particular, it does not regulate the non-public capture, storage and processing of personal information – including biometric data – by the Occupying Power, in ways that may have profound effects on the wellbeing of the protected person, as outlined above.

Determining whether an Occupying Power's use of FRTs within its measures of control and security is proportionate and consequently permissible therefore requires an assessment of their impact on rights – in particular the right to privacy – not expressly protected under IHL. If the duty of "respect for the person" under Article 27(1) is understood to cover "all rights of the individual" as Pictet asserts, it may be possible to interpret the content of this duty by reference to the body of law which does expressly protect these rights, IHRL. As Dinstein asserts: "Human rights law may … fill a gap in an occupied territory, when the norms governing belligerent occupation are silent or incomplete."[83] Van der Heijden similarly states:

> Considering that Article 27 is seen as reflecting the intrinsic rights and freedoms of the human being, international human rights law (IHRL) can and should be used to a certain extent as a means to interpret the provisions contained in this Article.[84]

78 J. Pictet, above note 68, p. 201.
79 *Ibid.*
80 *Ibid.*, p. 202.
81 *Ibid.*
82 *Ibid.*
83 Y. Dinstein, above note 54, p. 94.
84 Iris van der Heijden, "Other Issues Relating to the Treatment of Civilians in Enemy Hands", in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary*, Oxford University Press, Oxford, 2015, p. 1243.

The ICRC, examining the military uses of digital surveillance technologies, has too concluded that "[o]ther bodies of law, including international human rights law, might also be relevant when assessing surveillance".[85]

IHL therefore provides flexible, but incomplete, instructions regarding the permissibility of a given deployment of FRTs by an Occupying Power, either in its measures to ensure its own security, or in the maintenance of public order and civil life. The proportionality of such deployments may therefore be assessed by reference to IHRL, which can fill the *lacuna* in IHL as pertains to the content of humanitarian interests threatened by FRTs, in particular the right to privacy. Below, the applicability of IHRL to the context of the oPt will be assessed, as will the scope of Israel's obligations regarding the right to privacy of protected persons in light of the concurrent applicability of IHL.

Facial recognition technologies under international human rights law in the context of occupation

Human rights obligations of an Occupying Power

Israel ratified the International Covenant on Civil and Political Rights (ICCPR) in 1991 but contends that its treaty obligations do not extend to the oPt, arguing instead that IHL and IHRL "are codified in separate instruments, remain distinct and apply in different circumstances".[86]

Nevertheless, the concurrent extraterritorial applicability of IHRL and IHL is widely supported by international jurisprudence, State practice and legal scholarship.[87] The ICJ has established that an Occupying Power's duty under Hague Regulations Article 43 to ensure public order and civil life "comprised the duty to secure respect for the applicable rules of international human rights law".[88] The Human Rights Committee (HRC) has concluded that the applicability of IHL "in a situation of occupation, does not preclude the application of the [ICCPR]", and that Covenant provisions "apply to the benefit of the population of the occupied territories … with regard to all conduct by the State party's authorities or agents in those territories".[89] The applicability of IHRL to Israel's conduct in the oPt was affirmed in the ICJ's Wall Opinion.[90]

85 ICRC, above note 70, p. 29.
86 Fifth Periodic Submitted by Israel Report Under Article 40 of ICCPR, UN Doc. CCPR/C/ISR/5, 30 October 2019, paras. 22–6.
87 Noam Lubell, "Human Rights Obligations in Military Occupation", *International Review of the Red Cross*, Vol. 94, No. 885, 2012, p. 318.
88 ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, *ICJ Reports 2005*, para. 178.
89 HRC, Concluding Observations on the Third Periodic Review of Israel, UN Doc. CCPR/C/ISR/CO/3, 3 September 2010, para 5.
90 ICJ, above note 58, para. 106.

Applying international humanitarian law and international human rights law concurrently

An Occupying Power's deployment of FRTs is therefore governed by both IHL and IHRL which apply concurrently. Though these legal frameworks often complement each other, sometimes they "point in diverse – perhaps contradictory – directions".[91] In such situations, consideration must be paid to how such conflicts may be resolved.

In its Wall Opinion, the ICJ considered "both … human rights law and, as *lex specialis*, international humanitarian law".[92] The *lex specialis* principle provides that in the event of a conflict between legal norms, the more specific rule (*lex specialis*) overrides the more general one.[93] In this case, the Court indicated that IHL, as the legal framework specifically governing contexts of belligerent occupation, applies as *lex specialis*. In its Nuclear Weapons opinion, the Court found that the right to life under ICCPR Article 6 is applicable during hostilities, but that "whether a particular loss of life … is to be considered an arbitrary deprivation of life contrary to Article 6" could only be "decided by reference to the law applicable in armed conflict, and not deduced from the terms of the Covenant itself".[94] Thus the Court indicated that, though conflicts between IHRL and IHL norms cannot be resolved by the wholesale transposition of one body of law over another, IHL will take primacy in this circumstance.

The HRC, however, has eschewed the *lex specialis* principle when considering contexts of armed conflict where IHL and IHRL apply concurrently, asserting that while certain IHL rules "may be especially relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive".[95] As discussed above, where IHL rules are general or incomplete, they may need to be interpreted by reference to concurrently applicable specific rules of IHRL. The International Criminal Tribunal for the former Yugoslavia (ICTY), for example, used the detailed definition of torture taken from IHRL (Convention Against Torture Article 1) as an "interpretive guide" for the prohibition of torture in customary IHL and Article 3(a) common to the four Geneva Conventions, where no definition is provided.[96] The Tribunal cautioned, however, that "notions developed in the field of human rights can be transposed in international humanitarian law only if they take into consideration the specificities of the latter body of law".[97]

As Prud'homme highlights, the *lex specialis* principle "is silent as to what is specific and what bears a general character", concluding that "the vagueness of the

91 Y. Dinstein, above note 54, p. 95.
92 ICJ, above note 58, para. 106.
93 Y. Dinstein, above note 54, p. 95.
94 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, *ICJ Reports 1996*, para. 25.
95 HRC, General Comment No. 31, UN Doc. CCPR/C/21/Rev.1/Add.13, 26 May 2004, para. 11.
96 ICTY, *Prosecutor v. Kunarac, Kovac and Zukovic*, Case No. ICTY-96-23-T, Judgment (Trial Chamber), 22 February 2001, paras. 465–97.
97 *Ibid*., para. 471.

lex specialis maxim, and its consequential broad scope, allows the theory to be interpreted in all directions".[98] Indeed, in the present case IHL is the more specific body of law as regards contexts of belligerent occupation, whereas IHRL provides more specific guidance regarding States' obligations toward privacy.

In such instances it may be advisable to take a harmonizing approach which "brings international humanitarian law and international human rights law closer while acknowledging the specificities of each discipline".[99] This is consistent with the requirement of the Vienna Convention on the Law of Treaties that treaty provisions be interpreted in light of "any relevant rules of international law applicable in the relations between the parties".[100] As Prud'homme asserts, such an approach "underscores the fact that the two disciplines are already involved together inasmuch as they are both inspired by a common objective – the protection of humanity – and apply concomitantly".[101] Assessing the ICJ's Nuclear Weapons Opinion, Ben-Naftali and Shany find that "the emphasis the Court placed on the humanitarian considerations that inform IHL, underscores the purpose and underlying principles common to both regimes as the rationale for their co-application", with the effect that:

> each affects the interpretation of the other's norms: international humanitarian law may be used to interpret a human right rule, and human rights law influences the proper application of IHL in tilting the balance between military considerations and humanitarian concerns in favor of the latter.[102]

Following a harmonizing approach in the present case, IHRL obligations regarding the right to privacy should be read through the prism of IHL, as the body of law that specifically governs the conduct of an Occupying Power. At the same time, as IHL provides only general or incomplete guidance as regards protecting the privacy of protected persons, the proportionality of the Occupying Power's measures of control and security under GC IV Article 27 should be assessed in light of the more specific rules of IHRL relating to the rights upon which they impinge.

Face recognition technologies and the right to privacy

The human rights implications of FRTs depend on the specific nature of a given technology and the circumstances of its use. ID verification at checkpoints, the construction of biometric databases and watchlists, and LFR surveillance, all raise varied human rights challenges.[103] Here, focus is placed on the right to privacy,

98 Nancie Prud'homme, "*Lex Specialis*: Oversimplifying a More Complex and Multifaceted Relationship?", *Israel Law Review*, Vol. 40, No. 2, 2007, pp. 382–3.

99 *Ibid.*, p. 387.

100 Vienna Convention on the Law of Treaties, 115 UNTS 331, 23 May 1969 (entered into force 27 January 1980), Art. 31(2)(c).

101 N. Prud'homme, above note 98, p. 387. See also Orna Ben-Naftali and Yuval Shany, "Living in Denial: The Application of Human Rights in the Occupied Territories", *Israel Law Review*, Vol. 37, No. 1, 2003, pp. 56–7.

102 *Ibid.*, p. 56.

103 P. Fussey and D. Murray, above note 27.

as the right most directly interfered with by FRTs, and, in particular, Israel's reported deployment of LFR surveillance in the West Bank.

ICCPR Article 17 provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence", and that "[e]veryone has the right to the protection of the law against such interference or attacks".[104] Though definitions of "privacy" vary, it broadly encompasses:

> the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[105]

While, historically, interferences with privacy by States have primarily delved into private spaces and communications (e.g. home searches, or interception of correspondence), LFR surveillance typically takes place in public spaces. The HRC has established that information available in public areas may still be protected by Article 17.[106] The UN High Commissioner for Human Rights has outlined:

> the right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station … The public sharing of information does not render its substance unprotected.[107]

The European Court of Human Rights (ECtHR) has correspondingly concluded that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'",[108] and that while simple monitoring of individuals in public spaces (e.g. through CCTV) does not *per se* interfere with the right to privacy, "the recording of the data and systematic or permanent nature of the record may give rise to such considerations".[109]

The automated identification of individuals, and collection, storage and processing of sensitive personal biometric information in public spaces, whether or not they are on a watchlist, therefore constitutes an interference with the right to privacy. Moreover, as outlined above, covert identification of individuals through FRTs can enable access to a significant amount of personal data stored in private sources, such as national intelligence databases, or open sources, such as social media. Consequently, the deployment of these technologies is regulated by ICCPR Article 17.

104 ICCPR, 999 UNTS 171, 16 December 1966 (entered into force 23 March 1976), Art. 17.
105 Report of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/39/29, 3 August 2018, para. 5.
106 HRC, Concluding Observations on the Seventh Periodic Review of Colombia, UN Doc. CCPR/C/COL/7, 17 November 2016, para. 32.
107 UN High Commissioner for Human Rights, above note 105, para. 6.
108 ECtHR, *Peck v. The United Kingdom*, App. No. 44647/98, Judgment, 28 January 2003, para. 57.
109 *Ibid*., para. 59.

Permitted limitations on the right to privacy

Article 17 does not contain a limitation clause. The HRC, however, has established that interferences with the right to privacy "can only take place on the basis of law" and, to be non-arbitrary, must "be in accordance with the provisions, aims and objectives of the Covenant and … reasonable in the particular circumstances".[110] The HRC has interpreted reasonableness to mean that interferences with privacy "must be proportional to the end sought and be necessary in the circumstances of any given case".[111]

In General Comment 31, the HRC asserted that in imposing restrictions on Covenant rights, "States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims".[112] Interferences with privacy must therefore comply with the cumulative requirements of legality, legitimate aims, necessity and proportionality.[113]

As outlined above, when considering the application of ICCPR Article 6 in situations of armed conflict, the ICJ interpreted the term "arbitrary" in line with relevant rules of IHL. More broadly, Ben-Naftali and Shany assert that in contexts where IHRL and IHL apply concomitantly, "[e]xplicit limitation clauses found in human rights instruments … should also be applied in line with IHL".[114] Consistent with a harmonizing approach, the implicit requirements for the permissibility of limitations for the right to privacy under Article 17 must likewise be interpreted by reference to IHL.

Legality

A State's interference with the right to privacy "can only take place on the basis of law, which must itself comply with the provisions, aims and objectives of the Covenant".[115] National laws delineating permitted interferences with privacy "must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances".[116] To prevent arbitrary interferences with privacy, legal safeguards on surveillance should articulate, "the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided".[117]

110 HRC, General Comment 16: Article 17 (Right to Privacy), UN Doc. HRI/GEN/1/Rev9, 8 April 1988, paras. 3–4.
111 HRC, *Toonen v. Australia*, Communication No. 488/1992, Views, UN Doc. CCPR/C/50/D/488/1992, 31 March 1994, para. 8.3.
112 HRC, above note 95, para. 6.
113 Office for the High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 30 June 2014, para. 23.
114 O. Ben-Naftali and Y. Shany, above note 101, p. 105.
115 HRC, above note 110, para. 3.
116 OHCHR, above note 113, para. 23.
117 Frank La Rue, Report of the Special Rapporteur on the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 81.

An individual need not know, in all circumstances, when their privacy is being interfered with, as this would render sometimes-necessary covert surveillance impossible. Instead, the ECtHR has determined that laws must be sufficiently precise to enable individuals "to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[118] An individual must therefore be able to anticipate what conduct (e.g. engaging in serious crime) may result in them being placed under surveillance and their privacy interfered with, and adjust their behaviour accordingly.

Though an Occupying Power is generally restricted from enacting new legislation in the occupied territory under IHL under Article 43 of the Hague Regulations, failing to provide sufficiently clear criteria and limitations for restricting the rights of protected persons – for example through its military orders – is arguably also contrary to the requirement that an Occupying Power "restore … civil life",[119] particularly in contexts of prolonged occupation.

As discussed above, key provisions of IHL do permit an Occupying Power to undertake security measures, including surveillance, in the interests of public order, civil life, and its own security. These general IHL provisions do not by themselves, however, clearly and precisely delineate the circumstances in which such measures may be taken, nor provide legal safeguards against abuses.

Contrary to what is the case in East Jerusalem (the latter being considered to have been annexed by Israel), Palestinians in the West Bank are not subject to Israeli domestic laws, but to Israeli military orders. These orders do not establish criteria under which Palestinians may be targeted by LFR surveillance, nor place clear limits on these measures. Furthermore, the military orders laying out criminalized actions – which may potentially cause protected persons to be selected for surveillance – are "written so broadly that they violate the obligation … to clearly spell out conduct that could result in criminal sanction".[120]

Israel has not published policies outlining where its forces are permitted to deploy LFR surveillance in the oPt, who may be targeted, how that data is stored and processed, or who may access it. Reservists from Israel's military intelligence Unit 8200 have made allegations, reported by the press, claiming that it surveilled innocent people, making "no distinction between Palestinians who are, and are not, involved in violence".[121] If this is true, it underscores the broad discretionary power of surveillance afforded to Israeli authorities in the oPt.

As the OHCHR has established, "secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of 'law'".[122] Palestinians have no reasonable "foreseeability" regarding any use of LFR surveillance by Israel. They cannot know what actions may cause them to be

118 ECtHR, *The Sunday Times v. The United Kingdom*, App. No. 6538/74, Judgment, 26 April 1979, para. 49.
119 Hague Regulations, above note 50, Art. 43; GC IV, above note 65, Art. 64.
120 HRW, above note 47, p. 2.
121 The Guardian, "Israeli Intelligence Veterans' Letter to Netanyahu and Military Chiefs – In Full", 12 September 2014, accessible at: https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-veterans-letter-netanyahu-military-chiefs.
122 OHCHR, above note 113, para. 29.

placed on a watchlist, nor are they afforded opportunities to adjust their behaviour to avoid having their faces scanned in public spaces and thus their privacy invaded.

Legitimate aim

ICCPR Article 17 does not specify for which aims the right to privacy may legitimately be limited, though these may be inferred from the limitation clauses to other qualified Convention rights as laid out in HRC General Comment 27: "to protect national security, public order (*ordre public*), public health or morals and the rights and freedoms of others".[123]

The prevention of terrorism and serious crime may therefore constitute legitimate aims for surveillance, including through FRTs.[124] These aims are broad, however, with States often using "an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights" through surveillance.[125] LFR surveillance, and the adding of individuals to a watchlist, should thus only be considered for the most serious criminal offences.[126]

Considering the concurrent applicability of IHL, the Occupying Power's duty to ensure public order and civil life for the occupied population encompasses the same legitimate aims for security measures, including surveillance. The right of the Occupying Power to deploy "measures of control and security" under GC IV Article 27 means that these aims should also be expanded to include the protection of its own legitimate security interests. Allegations from Unit 8200 whistle-blowers that Israeli military surveillance practices are "used for political persecution" raise concerns that LFR surveillance may, however, be used for illegitimate aims.[127]

Necessity and proportionality

The HRC has specified that limitations on qualified rights must be "necessary in a democratic society" and "conform to the principle of proportionality".[128] UN special procedures have applied "necessary in a democratic society" as the standard of necessity for limitations on the right to privacy under ICCPR Article 17.[129] The European Convention on Human Rights (ECHR) similarly prohibits interferences with the right to privacy "except such as is … necessary in a democratic society".[130] This standard for necessity is stricter than that presented

123 HRC, General Comment 27: Article 12 (Freedom of Movement), UN Doc. CCPR/C/21/Rev1/Add9, 1 November 1999, para. 11. This reflects similar limitations clauses of, for example, Art. 19 (freedom of expression) and Art. 21 (peaceful assembly).
124 OHCHR, above note 113, para. 24.
125 F. La Rue, above note 117, para. 60.
126 D. Kaye, above note 28, para. 50; P. Fussey and D. Murray, above note 27, p. 55.
127 The Guardian, above note 121.
128 HRC, above note 123, paras. 11 and 14.
129 Joseph Cannataci, Report of the Special Rapporteur on the Right to Privacy, UN Doc. A/HRC/40/63, 27 February 2019, paras. 11–21; F. La Rue, above note 117, para. 29.
130 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 213 UNTS 222, 3 September 1953, Art. 8(2).

for security measures in IHL under GC IV Article 27 ("necessary as a result of the war"). As the context under consideration is one of belligerent occupation – where the normal democratic function of a state may be temporarily suspended – this is one area where harmonization is required and the greater contextual specificity of IHL recognized. Thus the concept of necessity must be widened to permit interferences with right to privacy to both uphold the "pressing social needs"[131] of the local population, and to meet the Occupying Power's military exigencies, including the protection of its forces and materiel from threats arising in the territory.

A proportionate balance must also be struck between these needs and the severity of a given interference with privacy.[132] HRC General Comment 27 establishes that, to be proportionate, limitations on ICCPR rights must be "appropriate to achieve their protective function"; "the least intrusive instrument amongst those which might achieve the desired result"; and "proportionate to the interest to be protected".[133] For surveillance technologies, then:

> …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.[134]

GC IV Article 27(4) also does not provide *carte blanche* to the Occupying Power's security measures, which "may not exceed what is reasonably required to achieve a legitimate security purpose in the circumstances".[135] The ICJ invoked the HRC's necessity and proportionality tests in its Wall Opinion, concluding that the route of Israel's separation wall was not "necessary to attain its security objectives" and that the infringements on Palestinians' rights caused by the wall and its associated administrative regime "cannot be justified by military exigencies or by the requirements of national security or public order".[136]

For a given means to be the "least intrusive" available, its limitations on privacy must not exceed what is necessary to achieve the legitimate aim. The HRC has established that interferences with privacy should only be permitted "on a case-by-case basis".[137] In *S. and Marper v. UK*, the ECtHR found that the "blanket and indiscriminate" power to retain DNA and biometric data of individuals suspected, but not convicted, of a criminal offence, "fail[ed] to strike a fair balance between the competing public and private interests" and was therefore disproportionate.[138] UN special procedures have assessed that mass

131 ECtHR, *Sunday Times v. UK*, above note 118, para. 59.
132 Ben Emmerson, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc. A/69/397, 23 September 2014, para. 51.
133 HRC, above note 123, para. 14. See also OHCHR, above note 113, paras. 23–5.
134 OHCHR, above note 113, para. 25.
135 Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, ICRC, Geneva, 2016, p. 225.
136 ICJ, above note 58, paras. 136–7.
137 HRC, above note 110, paras. 6–8.
138 ECtHR, *S. and Marper v. The United Kingdom*, App. Nos. 30562/04 and 30566/04, Judgment, 2008, para. 125.

digital surveillance "constitutes a potentially disproportionate interference with the right to privacy".[139]

It is sometimes claimed that LFR surveillance is minimally invasive due to the lack of physical search involved.[140] Where deployed in public spaces, however, these systems involve interferences with the privacy of all individuals whose faces are scanned, not only those on a watchlist. Such "widespread and bulk monitoring, collection, storage, analysis or other use" of biometric data may be considered "indiscriminate mass surveillance".[141]

Furthermore, the accuracy of these technologies is hotly contested, and "false-positives", where people are wrongly identified, potentially expose innocent individuals to unnecessary searches, ID checks, detention and further rights interferences. For example, police tests of LFR technologies have reported as many as 95% of matches as "false-positives".[142] Fussey and Murray have thus argued for a "broader proportionality analysis" that "takes into account the rights impact of those not on the watchlist".[143] As with mass interception of internet communications, assessments of the proportionality of LFR surveillance should therefore "also take account of the collateral damage to collective privacy rights".[144] These issues have led some to assert that LFR systems are "inherently disproportionate".[145]

As established above, Pictet similarly asserts that measures of control and security under GC IV Article 27 should not suspend rights "in a general manner", with personal freedoms remaining "in general unimpaired".[146] IHL and IHRL are therefore in agreement that LFR surveillance technologies used in public spaces in occupied territory, constituting mass, indiscriminate surveillance, are likely to constitute disproportionate limitations on the right to privacy of protected persons.

Finally, although the concept of belligerent occupation contains an "implicit assertion that military control is temporary",[147] Israel's control has persisted for fifty-four years. The duration of an occupation should also factor into balancing the interests of the local population and the Occupying Power when determining proportionality.[148] Benvenisti, for example, asserts that, "as hostilities subside, and security considerations permit, the occupant is expected to restore civil and political rights".[149] The Israeli Supreme Court has also recognized "the needs of the local population gain weight in a long-term military

139 B. Emmerson, above note 132, para. 18.
140 K. A. Gates, above note 4, p. 46.
141 Amnesty International, *The Right to Peaceful Assembly: Submission to the UN Human Rights Council*, London, March 2019, p. 25.
142 Big Brother Watch, above note 12, p. 15.
143 P. Fussey and D. Murray, above note 27, pp. 60–1.
144 B. Emmerson, above note 132, para. 52.
145 Equality and Human Rights Commission, *Civil and Political Rights in Great Britain*, London, March 2020, p. 64.
146 J. Pictet, above note 68, p. 202.
147 A. Roberts, above note 55, p. 45.
148 O. Ben-Naftali and Y. Shany, above note 101, p. 97; A. Roberts, above note 55, p. 71.
149 E. Benvenisti, above note 49, p. 75.

occupation".[150] The general lack of hostilities in the West Bank and prolonged nature of Israel's occupation should further tilt the balance of proportionality in favour of the right to privacy of Palestinians.

Corollary human rights impacts

As established above, in domestic contexts, FRTs have been used in ways which consolidate abusive control over securitized populations by restricting movement and clamping down on dissent. The possibility similarly exists that, by inhibiting the enjoyment of privacy by protected persons, these technologies may facilitate the entrenchment of an Occupying Power's control over occupied territory and populations in ways which violate broader individual and collective rights.

Freedom of assembly, association and expression

The enjoyment of the ICCPR rights to freedom of peaceful assembly (Article 21), association (Article 22) and expression (Article 19) are often contingent on the enjoyment of the right to privacy and anonymity in public spaces. These rights are not only important individual rights, but are also essential to express legitimate collective grievances and motivate the peaceful development of societies.[151] As UN Special Rapporteur David Kaye described:

> In environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise rights to freedom of expression [and] association.[152]

The HRC's General Comment 37 outlines that state surveillance at assemblies "must strictly conform to applicable international standards, including on the right to privacy, and may never be aimed at intimidating or harassing participants or would-be participants in assemblies".[153] LFR surveillance, however, challenges anonymity, potentially permitting security forces to identify individual protesters and subject them to harassment or detention.

For the duration of its prolonged occupation, Israel has placed significant restrictions on these rights. In the West Bank, Military Order 101, issued in 1967, prohibits *inter alia* assemblies of ten or more persons where "a speech is being made on a political subject" and authorizes "every soldier … to use the degree of force necessary" to prevent violations of this order.[154] Breaches are punishable by

150 *Jamayat Askan v. Commander of the IDF in Judea and Samaria*, HCJ 393/82 (1983), para. 22.
151 HRC, General Comment 37: Article 21 (Right of Peaceful Assembly), UN Doc. CCPR/C/GC/37, 17 September 2020, para. 1.
152 D. Kaye, above note 28, para. 21.
153 HRC, above note 151, para. 61.
154 Legal Advisor for Judea and Samaria Region, *Israeli Defense Forces Order No. 101: Regarding Prohibition of Incitement and Hostile Propaganda Actions* (Translated by B'Tselem), 27 August 1967, available at: https://www.btselem.org/download/19670827_order_regarding_prohibition_of_incitement_and_hostile_propaganda.pdf.

ten years' imprisonment and a fine. UN special procedures and human rights organizations have opposed Israel's restrictions on freedom of assembly, expression and association, and called for the repeal of Military Order 101.[155] Israel's digital surveillance has documented a "chilling" effect on the free political expression of Palestinian activists and journalists online.[156]

The use of LFR surveillance in public spaces may thus deter Palestinians from attending peaceful public demonstrations demanding change from an Occupying Power that they have no democratic control over, for fear of being identified, detained or suffering reprisals. Pervasive interferences with privacy permitted by FRTs may ultimately reduce pressure on an Occupying Power to change its policies, grant further rights to the population, or withdraw.

Freedom of movement

Privacy and control of movement are also inextricably linked. The freedom of movement of Palestinians is controlled, not only by physical barriers such as checkpoints and the separation wall, but also by administrative and legal controls which require their identification, and the collection, processing and storage of their personal data. This includes "more than a dozen different travel permits, each allowing different categories of persons to travel to different categories of space",[157] and Israel's control over the Palestinian population registry and IDs.[158]

In its Wall Opinion, the ICJ determined not only that the construction of the wall beyond the Green Line was contrary to international law, but so too was its associated administrative regime of permits and ID cards issued to Palestinians living in, or seeking to enter, the "closed area" between the wall and the Green Line.[159] These measures together were found to "impede the liberty of movement of the inhabitants of the Occupied Palestinian Territory" and to "impede the exercise by the persons concerned of the right to work, to health, to education and to an adequate standard of living".[160] As described below, the Court held that these measures create a "*fait accompli*", imposing permanent rather than temporary impediments to Palestinians' rights.[161]

As Weizman observes, the separation wall and its checkpoints are "not only an instrument of partition, but also of observation and control".[162] Interferences with privacy, through the mass collection and processing of Palestinians' facial data, comprise an increasingly integral part of Israel's administrative regime, consolidating its control over the lives – and movements – of Palestinians.

155 See HRW, above note 47, p. 8; Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/20/17/Add2, 11 June 2012, para. 102.
156 HRW, above note 47, p. 7.
157 Eyal Weizman, *Hollow Land: Israel's Architecture of Occupation*, Verso, London, 2007, p. 146.
158 E. Zureik, above note 72, p. 14.
159 ICJ, above note 58, para. 85.
160 *Ibid*., para. 134.
161 *Ibid*., para. 121.
162 E. Weizman, above note 157, p. 153.

Self-determination

The primary advantages of FRTs for an Occupying Power are efficiency and scale – more individuals can be monitored and their movements controlled with fewer resources. Installed at checkpoints, automated ID checks further reduce physical interactions between Palestinians and border guards, limiting points of potential "friction".[163] LFR systems enhance the scope of surveillance and potential to target individuals for arrest or application of force, while reducing the need for human monitoring of CCTV, or the physical presence of soldiers in occupied territory.

Weizman observes, however, that Israel has sought to render the occupation increasingly "invisible" in order "to absolve itself of the responsibilities it has assumed as the occupying power" – including the maintenance of the humanitarian needs of the population – "without losing overall 'security control'".[164] In 2005, for example, Israel removed its troops and settlements from inside Gaza, while retaining control over Gaza's airspace, land crossings, territorial waters, population registry and ability to conduct frequent military incursions.[165] As Scobbie highlights: "Given the high-tech means of surveillance and attack employed by Israel, this was an attempt to deny responsibility for the territory while reaping the benefits of effective, albeit remote, control."[166]

AI-powered technologies – including FRTs, predictive policing and digital surveillance – may render Israel's control not only more "invisible" and "remote", but also increasingly automated. Through these systems, security threats can be identified and neutralized earlier and with fewer boots on the ground, and resistance and protest can be nullified both directly and indirectly through self-censorious behaviour of those fearing repercussions. The population under occupation, meanwhile, may endure increasing humanitarian costs as their privacy disappears, their movement reduces and civil life erodes. Increasing automation may entrench an Occupying Power's control while reducing the pressure on it to withdraw, thus prolonging what is intended to be a temporary situation.

As Ben-Naftali, Sfard and Viterbo assert, "if an occupation could continue indefinitely, the interests it is designed to protect would all become meaningless" including "the inhabitants' interest in regaining control over their life and exercising their right to self-determination".[167] Israel's obligation to respect the Palestinian people's collective right to self-determination and thus "freely determine their political status and freely pursue their economic, social and

163 *Ibid.*, p. 150.
164 *Ibid.*, pp. 156–9.
165 Julia Grignon, "The Geneva Conventions and the End of Occupation", in A. Clapham, P. Gaeta and M. Sassòli (eds), above note 84, p. 1592.
166 Ian Scobbie, "Gaza", in Elizabeth Wilmshurst (ed.), *International Law and the Classification of Conflicts*, Oxford University Press, Oxford, 2012, p. 314.
167 Orna Ben-Naftali, Michael Sfard and Hedi Viterbo, *The ABC of the OPT: A Legal Lexicon of the Israeli Control Over the Occupied Palestinian Territory*, Cambridge University Press, Cambridge, 2018, p. 17.

cultural development"[168] was affirmed by the ICJ in its Wall Opinion.[169] The Court, finding that the construction of the wall and other measures impede Palestinians' enjoyment of their economic, social and cultural rights, reflected fears that these measures "will prejudge the future frontier between Israel and Palestine" and thus "create a '*fait accompli*' on the ground that could well become permanent".[170] The measures, contravening the assumption of temporariness in an Occupying Power's control, were therefore found to "severely [impede] the exercise by the Palesitnian people of its right to self-determination".[171]

Israel's use of FRTs should be considered in light of not only the half-century duration of its occupation, but also what UN Special Rapporteur Michael Lynk has termed a failure to govern the oPt in "good faith" as "measured by the criteria of substantive compliance with United Nations resolutions or by the satisfaction of its obligations as occupier under the framework of international law".[172] The "avaricious" nature of its occupation should also be considered, as demonstrated by "the expanding settlement enterprise, the annexation of territory, the confiscation of private and public lands, the pillaging of resources, [and] the publicly-stated ambitions for permanent control over all or part of the Territory".[173]

Just as Israel's separation wall engenders the risk of imposing permanent control over occupied territory and alterations to its demographic composition,[174] the use of FRTs and related technologies may also facilitate the prolonging of an Occupying Power's control over an occupied population – particularly if it is governing in bad faith – and thus inhibit the exercise of their collective right to self-determination. As Lubell explains:

> The expectation that the occupation should be a temporary affair, and that sovereignty … is not transferred to the Occupying Power, requires rules designed to minimize the possibility of the occupier creating changes that would endanger these assumptions.[175]

The broader impacts on Palestinians' collective right to self-determination should therefore also be considered when assessing the proportionality, and permissibility, of these measures.

Conclusion

Despite their increasing ubiquity and implications for the rights and freedoms of people in areas of conflict and occupied territories, there has been scant academic

168 ICCPR, above note 104, Art. 1.
169 ICJ, above note 58, paras. 88 and 149.
170 *Ibid*., para. 121.
171 *Ibid*., paras. 134 and 122.
172 Michael Lynk, Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied Since 1967, UN Doc. A/72/43106, 23 October 2017, para. 62.
173 Michael Lynk, Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied Since 1967, UN Doc. A/HRC/37/75, 15 March 2018, para. 64.
174 ICJ, above note 58, para. 122.
175 N. Lubell, above note 87, p. 329. See also E. Benvenisti, above note 49, p. 349.

or judicial exploration of the legal implications of military uses of FRTs. This reflects both the newness of these technologies, and the covert nature of their use.

Though these technologies were unforeseeable to the drafters of the core IHL treaties, the law of occupation is flexible, adapting to a broad array of modern scenarios and technologies. Where deployed within an Occupying Power's measures of control and security, FRTs sit at the fulcrum of the law of occupation's central balance between the Occupying Power's security interests and the humanitarian interests of protected persons. IHL provides only general guidance, however. Assessing the humanitarian impacts of an Occupying Power's uses of FRTs, and thus their proportionality, requires reference to overlapping IHRL obligations, particularly regarding the right to privacy. Under IHRL, interferences with privacy are permissible so long as they satisfy the cumulative requirements of legality, legitimate purpose, necessity and proportionality.

Although a thorough examination is limited by the secrecy surrounding Israel's deployment of LFR surveillance in the oPt, its documented uses appear *prima facie* not to satisfy these criteria, even where they are harmonized with the framework of IHL which specifically concerns the conduct of belligerent occupation. In particular, it lacks adequate basis in law, and the indiscriminate mass interference with privacy caused by the unfettered use of LFR surveillance in public spaces would constitute a disproportionate interference with Palestinians' right to privacy.

Furthermore, pervasive interferences with the right to privacy engendered by FRTs may have corollary impacts on the rights to freedom of movement, expression, assembly and association. FRTs, and related technologies, may reduce the costs of occupation while simultaneously rendering the occupant's exercise of authority less visible, more remote and increasingly automated, thus entrenching its control. In the context of Israel's already-prolonged occupation they thus engender risks to the Palestinians' exercise of their collective right to self-determination. Additional study is warranted into these issues, particularly regarding the challenge posed to the very concept of "occupation" and the task of determining the existence of an occupation under Hague Regulations Article 42 where the Occupying Power's control is increasingly automated and remote.

Further examination of the international legal implications of these technologies is imperative. While FRTs, and other AI-powered security technologies, touch the lives of more and more people around the world, the governments and corporations at the vanguard of developing, deploying and exporting them also influence the norms governing their uses. Should such technologies be increasingly used without the essential safeguards of international humanitarian and human rights law, a spectre of digital authoritarianism lies ahead.