



FACULTY OF LAW

LUND UNIVERSITY

Andria Lillieroth Charalambous

Biometric Surveillance and the Law of Occupation

Privacy in the Age of Military Panopticons

JAMM07 Master Thesis

International Human Rights Law

30 higher education credits

Supervisor: Alberto Rinaldi

Term of graduation: Spring 2026

Summary

The last two decades have seen considerable advancements in biometric technology, and consequently its use as a surveillance measure during occupation. The increasingly invasive and omniscient nature of biometric surveillance technologies means they constitute a considerable infringement on the private sphere of occupied populations, and consequently an interference with their right to privacy. This thesis examines the rules of international humanitarian law, international human rights law and data protection law to ascertain what protections exist for the biometric privacy of those living under occupation. A particular focus is placed on the phenomenon of prolonged occupation and its far-reaching implications for the privacy of occupied persons.

While much of legal scholarship has been dedicated to evaluating the impact of various biometric technologies on armed conflict, the focus of existing research is overwhelmingly on technologies used for targeting. Despite its undeniable legal relevance in the present day, the international law of occupation continues to be a neglected and underdeveloped area of international humanitarian law. Also neglected in the context of armed conflict is the question of privacy, an important human right made increasingly relevant as surveillance technologies using biometric data continue to advance in scope and capabilities. Endeavouring to fill this gap in legal scholarship, this thesis examines international treaties, jurisprudence, legal commentary and literature on occupation, the right to privacy and data protection, bringing them together in search of a cohesive legal framework.

To guide the research, this thesis evaluates what provisions and principles govern biometric surveillance in three core areas where the Occupier and the occupied interact: public spaces in the occupied territory, military checkpoints and places of internment and detention. The provisions and principles are then tested by conducting a case study of two existing prolonged occupations. The research finds that while persistent legal gaps remain, there is an emerging trend of convergence of international humanitarian law, international human rights law and data protection law on the right to biometric privacy.

Preface

This thesis marks the end of my time as a law student at Lund university, and I wish first and foremost to thank the many passionate and engaging scholars and lecturers who have shaped my time here. I extend my most sincere gratitude to my supervisor Alberto Rinaldi for his excellent guidance and untiring encouragement.

This journey would have been considerably more challenging without the support and encouragement of my friends and family. I would especially like to thank Tereza, Niusha, Sara, Chloe and my sister Daniella for always lending me an ear when I needed it.

Table of contents

Summary	1
Preface.....	2
Abbreviations	5
1 INTRODUCTION	6
1.1 Background.....	6
1.2 Purpose and research question.....	7
1.3 Method and material.....	7
1.4 Delimitations and clarifications.....	8
1.5 Outline	9
2 A GENEALOGY OF OCCUPATION AND SURVEILLANCE	11
2.1 Introduction	11
2.2 The Lieber Code of 1863.....	12
2.3 The Hague Regulations of 1899 and 1907	12
2.4 The 1949 Geneva Convention IV	14
2.5 Post-1949 developments.....	15
3 THE LAW OF OCCUPATION AND BIOMETRIC SURVEILLANCE OF THE OCCUPIED.....	17
3.1 General framework of operation	18
3.2 Biometric surveillance of the occupied	24
3.2.1 Public spaces	25
3.2.2 Checkpoints.....	27
3.2.3 Internment and detention.....	27
4 THE RIGHT TO PRIVACY UNDER INTERNATIONAL HUMAN RIGHTS LAW IN OCCUPATION SETTINGS	30
4.1 Concurrent application of international human rights law in occupation settings.....	30
4.2 The right to privacy under international human rights law .	32
4.2.1 Article 17 of the International Covenant on Civil and Political Rights.....	33
4.2.2 Article 8 of the European Convention on Human Rights	35
4.3 Jurisprudence of the European Court of Human Rights.....	37
4.3.1 Public spaces	38
4.3.2 Checkpoints.....	39
4.3.3 Internment and detention.....	40
4.4 Devising a test for the use of biometric surveillance	41
4.4.1 Requirement (1): Legality	42
4.4.2 Requirement (2): Legitimate purpose	43

4.4.3	Requirement (3): Necessity.....	43
4.4.4	Requirement (4): Proportionality	44
4.5	Reconciling IHL and IHRL	45
5	DATA PROTECTION PRINCIPLES IN OCCUPATION SETTINGS	
	47	
5.1	Current state of law	48
5.2	Council of Europe.....	49
5.2.1	Convention 108+	49
5.2.2	Recommendation No. (87) 15	51
5.3	European Union.....	52
5.3.1	Charter of Fundamental Rights of the European Union..	52
5.3.2	Law Enforcement Directive	52
5.4	Data protection principles during occupation.....	54
6	CASE STUDIES: PRIVACY AND PROLONGED OCCUPATION	
	IN UKRAINE AND PALESTINE	55
6.1	Ukraine	56
6.1.1	Checkpoints.....	57
6.1.2	Internment and detention.....	57
6.1.3	Public spaces	58
6.1.4	Analysis.....	59
6.2	Palestine.....	62
6.2.1	Public spaces	62
6.2.2	Checkpoints.....	64
6.2.3	Internment and detention.....	64
6.2.4	Analysis.....	65
6.3	Towards a panoptic military future?.....	68
7	Concluding remarks.....	69
	Bibliography	72

Abbreviations

AI	Artificial Intelligence
AP I	Additional Protocol I to the Geneva Conventions
CCTV	Closed-Circuit Television
CFR	Charter of Fundamental Rights of the European Union
CoE	Council of Europe
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FRT	Facial Recognition Technology
GCIV	The Fourth Geneva Convention of 1949
GDPR	General Data Protection Regulation
HRC	Human Rights Council
HRW	Human Rights Watch
LFRT	Live Facial Recognition Technology
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
IHRL	International Human Rights Law
UN	United Nations

1 INTRODUCTION

1.1 Background

The last two decades have seen considerable advancements in biometric technology, resulting in its increased application in armed conflicts and consequently its accelerating use as a means of surveillance in occupation settings. The increasingly invasive and omniscient nature of biometric surveillance technologies enables an Occupying Power to exert authority over the occupied despite diminished physical presence in an occupied territory.¹ Through the collection and processing of facial images, fingerprints, palm prints, body language and numerous other biometric identifiers, Occupying Powers can now track and monitor occupied persons *en masse* on an unprecedented scale.²

These developments raise pressing questions related to the privacy protections of occupied populations, perhaps especially those living under prolonged occupation. The conduct of Occupying Powers is governed by the international law of occupation, a subset of international humanitarian law (IHL). Despite its inarguable legal relevance in the present day, codification of the law of occupation has remained stagnant since 1977. However, the concurrent application of international human rights law (IHRL) in armed conflict has brought the right to privacy of occupied persons to the forefront of discussions on surveillance during occupation. The collection and processing of biometric data directly interfere with the right to privacy under international human rights law and involves forms of personal data increasingly recognised as particularly sensitive under modern data protection re-

¹ Goodfriend, Sophia, ‘Algorithmic State Violence: Automated Surveillance and Palestinian Dispossession in Hebron’s Old City’ (2023) 55(3) *International Journal of Middle East Studies* 461–478 p. 465-469.

² Amnesty International, *Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT* (2 May 2023) p. 42-47; Dwoskin, Elizabeth, ‘Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank’ *The Washington Post* (5 November 2021).

gimes. Against this background, this thesis examines how international humanitarian law, international human rights law and emerging principles of data protection law regulate the use of biometric surveillance technologies by Occupying Powers, with particular focus on prolonged occupation.

1.2 Purpose and research question

Advancements in the field of technology have significant implications for occupation and the laws of war. Most legal scholars who assess the impact of new biometric technologies in the theatre of war have focused on the emerging use of so-called ‘killer robots’ and FRT systems used for targeting. This singular focus has left a blind spot in scholarship regarding what effect the same technologies have on occupation and the rights of the occupied, particularly their right to privacy. Thus, the overarching aim of this thesis is to address this existing research gap by examining how the law of occupation, a subset of IHL, and other legal regimes protect privacy when biometric surveillance is deployed on the civilian population by an Occupying Power.

The research conducted in this thesis is centred on the following research question:

- What limitations do international humanitarian law, international human rights law and data protection law place on the use of biometric surveillance technologies by Occupying Powers against occupied populations?

1.3 Method and material

This thesis uses the doctrinal legal method to identify current law and answer the research question posed above. Through the doctrinal legal method, current law is established by evaluating generally accepted sources of law.³ The relevant sources of law for this thesis are those prescribed in Article 38(1) of

³ Kleineman, Jan, ‘Rättsdogmatisk metod’ in Nääv, Maria and Zamboni, Mauro (eds), *Juridisk Metodlära* (2nd Edition, Studentlitteratur 2021) 21–46 p. 21-31.

the Statute of the International Court of Justice (ICJ). The provision is considered to apply broadly to international law and defines its three primary sources: international conventions, international custom and the general principles of law. As subsidiary means, it further provides that judicial decisions and publications of highly qualified publicists may also be used to determine the rules of law.⁴

The research material used in this thesis consists of international treaties and judicial decisions by international and regional courts and tribunals, as well as relevant commentary by courts, human rights bodies and international organisations. Additionally, publications by legal scholars are used as subsidiary means for determining law, and reports issued by reputable human rights organisations are used to provide a factual basis for a legal assessment of occupations that exist today.

Considerable challenges arise when researching the factual circumstances of ongoing armed conflicts and occupations. The research conducted for the case studies in Chapter 6 of this thesis relies on verified, publicly available information found in reports by human rights non-governmental organisations, as well as in news articles and literature. It neither purports to nor intends to provide an exhaustive account of the underlying facts of either occupation.

1.4 Delimitations and clarifications

The topic of this thesis is the use of biometric surveillance technology in occupation settings and its relationship to the right to privacy under human rights law. The thesis does not examine the legality of biometric surveillance in domestic settings, e.g. as part of national law enforcement operations, except to the limited extent that case law on that topic may assist in determining what protections apply during occupation. Also outside the scope of this thesis is the question of what effect biometric surveillance has on human rights

⁴ Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 33 UNTS 993 art 38(1)d.

other than the right to privacy. The thesis also excludes questions of discrimination and machine bias in relation to surveillance technologies that use Artificial Intelligence (AI).

The research question focuses on the use of various forms of biometrics to surveil the population of an occupied territory on a mass scale. Beyond the scope of the research question is the role of biometrics in the targeting of military combatants and military objectives, and any IHL or IHRL concerns that may arise from that practice. The thesis does not include the use of biometric technology to identify the deceased or to distribute humanitarian aid during armed conflicts. Also delineated are the duties of non-state parties, such as military contractors and private corporations, in relation to biometrics and privacy.

In addition to examining the contents of international humanitarian law and international human rights law, applicable to all armed conflicts, this thesis evaluates relevant parts of Council of Europe (CoE) and European Union (EU) data protection law. Neither CoE nor EU regulations can themselves be said to apply directly to all instances of occupation, as they are limited to conduct falling within the jurisdiction of the State parties. They do not apply directly to the occupations of Ukraine and Palestine, which are the subject of the case study in Chapter 6. These regulations are instead assessed analogously to test the application of biometric data protection principles that may amount to customary law either presently or in the future. Due to limitations in time and scope, the thesis does not examine other regimes of data protection law. It similarly does not examine the right to privacy under other regional human rights systems other than the European Convention on Human Rights (ECHR) and its jurisprudence.

1.5 Outline

The first chapter of this thesis introduces the subject of research. It provides the factual background, research question and scope, as well as the method and materials used. Chapter 2 provides a brief historical outline of the emergence of the law of occupation, alongside examples of surveillance practices

used by Occupying Powers at various points in recent history. Following this, Chapter 3 examines the provisions under IHL that regulate the conduct of Occupying Powers. It discusses what protections they offer in terms of privacy and what limitations they place on the use of biometric surveillance. Chapter 4 examines the right to privacy in relation to biometric surveillance in occupation settings by looking at the provisions, jurisprudence and commentary of the International Covenant on Civil and Political Rights (ICCPR)⁵ and the European Convention on Human Rights (ECHR).⁶ Chapter 5 reviews what data protection law says about biometrics and identifies key general and biometric data protection principles that may be relevant in occupation settings.

Lastly, Chapter 6 tests the research findings by evaluating the use of biometric surveillance technologies and their impacts on the right to privacy in two current prolonged occupations: Ukraine and Palestine. The concluding remarks provide a legal doctrinal examination of the law and its implications for both the present and future.

⁵ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

⁶ European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953) ETS No 5.

2 A GENEALOGY OF OCCUPATION AND SURVEILLANCE

2.1 Introduction

The international law of occupation governs the relationship between an Occupying Power and the State, territory and population it occupies. Rooted in centuries-old laws and customs of war, occupation law gradually came to evolve from military practice into a codified branch of modern international humanitarian law. The protection of privacy, initially manifested as the sanctity of the home, family, property and honour of civilians, has been a recurring feature of occupation law as it has emerged in codified form over the past 150 years. Beginning with the Lieber Code of 1863,⁷ and continuing through the Hague Conventions of 1899⁸ and 1907⁹ (Hague Regulations), the drafting of the 1949 Geneva Conventions in the immediate aftermath of World War II¹⁰ and the 1977 Additional Protocol I to the Geneva Conventions (AP I),¹¹ a recurring pattern of protections for the private sphere of occupied civilians has emerged. While further codification of the law of occupation has remained stagnant since 1977, interpretation of privacy and the rights of the occupied in the context of modern warfare continues to evolve through commentary and legal scholarship.

Biometrics and surveillance have fundamentally altered the nature of occupation. This chapter provides a brief historical overview of privacy, surveillance and occupation. It will outline the emergence of relevant provisions under

⁷ Instructions for the Government of Armies of the United States in the Field (Lieber Code) (24 April 1863) General Orders No 100. (Lieber Code)

⁸ Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900). (1899 Hague Regulations)

⁹ Convention (IV) respecting the Laws and Customs of War on Land and annexed Regulations (adopted 18 October 1907, entered into force 26 January 1910) 205 CTS 277. (1907 Hague Regulations)

¹⁰ International Committee of the Red Cross, *Documentation préliminaire pour la révision et l'établissement de Conventions ayant trait à la Croix-Rouge* (Circular No 368, Geneva, 15 February 1945).

¹¹ Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 art 75.

occupation law alongside historical examples illustrating the parallel evolution of surveillance. In addition to provisions related to privacy, the chapter will also highlight key aspects of occupation law that make possible the prolonged, technology-driven military occupations seen today in the territories of Ukraine and Palestine.

2.2 The Lieber Code of 1863

The Lieber Code of 1863 (Lieber Code) was one of the earliest attempts to codify the laws of war. It was an important precursor to modern international humanitarian law, including the law of occupation. Adopted during the American Civil War, the Lieber Code established legal guidelines intended to regulate the conduct of armed forces and to ensure the humane treatment of civilian populations in occupied territory.¹²

Notably, the Lieber Code established a general rule of protection for the private sphere of civilians. It asserted that soldiers must protect ‘the inoffensive citizen of the hostile country’, and that ‘privation and disturbance of private relations’ was an exceptional measure permitted only in certain circumstances.¹³

Occupations of the period nevertheless frequently involved intrusive forms of surveillance. During the American Civil War, Union forces occupying Confederate territories engaged in practices such as house searches, imposed systems of travel passes to restrict civilian movements and intercepted correspondence of those suspected of covertly supporting the Confederacy.¹⁴

2.3 The Hague Regulations of 1899 and 1907

¹² Nabulsi, Karma: *Traditions of War: Occupation, Resistance, and the Law* (Oxford University Press 1999) p. 5.

¹³ Lieber Code art 24. See also Lubin, Asaf, ‘The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law’ in Kolb, Robert; Gaggioli, Gloria and Kilibarda, Pavle (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (Edward Elgar Publishing 2022) 463–492 p. 463.

¹⁴ Neely, Mark E Jr, *The Fate of Liberty: Abraham Lincoln and Civil Liberties* (Oxford University Press 1991) p. 30-36, 53-58, 81-85.

The earliest international codification of the law of occupation is found in the Hague Regulations of 1899 and 1907. The Regulations were the result of an effort by the European sovereigns of the 19th century to regulate the conduct of occupying armies, as part of a broader effort to codify the laws of war.¹⁵ The Regulations established two core obligations of any Occupying Power.¹⁶ The first obligation is to protect the inhabitants of the occupied territory. This obligation was not derived from conceptions of human rights as such, but rather from the distinction made between combatant and non-combatant. The distinction also separated the sovereign ruler from 'the unarmed citizens' within a given territory.¹⁷ This meant that the private property and private sphere of civilians were to be left intact when territory came under occupation. The property of the State, on the other hand, could pass in title to the Occupying Power, who was at this time not only an occupier but also a conqueror.¹⁸

The second obligation of an Occupying Power was to respect the rights of the ousted sovereign ruler, at least until such time that a formal transfer of power could occur.¹⁹ Occupation and conquest were at this time intertwined but not identical: the 1815 Congress of Vienna had established a prohibition on unilateral annexation, separating the question of control from that of sovereign rights. This emerging understanding of sovereignty meant that occupation did not equate to conquest but still constituted a means to achieve it. Once occupied, territory could become subject to peace negotiations which would eventually lead to the ceding of territory by the ousted ruler. But since sovereign rights could no longer be ceded by force, the obligation to respect the rights

¹⁵ Benvenisti, Eyal, *The International Law of Occupation* (2nd Edition, Oxford University Press 2012) p. 20.

¹⁶ Mansoor, Nimra, *The Evolution of the Law of Occupation* (Conflict Law Centre, Research Society of International Law Pakistan 2023) p. 8-10.

¹⁷ *Ibid* p. 10-11.

¹⁸ de Vattel, Emmerich, *The Law of Nations* (1758 Chitty, Joseph ed. and transl., Philadelphia 1852), Vol. 2 Book 3 p. 195: 'One sovereign makes war against another sovereign, and not against the unarmed citizens.' See Benvenisti (2012) p. 23-24 and note 10.

¹⁹ Benvenisti (2012) p. 27-30.

of the ousted ruler required the Occupying Power to maintain the laws already in force, unless absolutely prevented from doing so.²⁰

While the 1899 and 1907 Hague Regulations placed limitations on the conduct of an Occupying Power, both neglected to set any temporal limits on occupation.²¹ The nature of occupation was viewed as inherently temporary, lasting for the interim period between a military victory and the subsequent formal concession of territory through a peace treaty. This deficiency laid the basis for the future problem of prolonged occupation.

Parallel to this, occupations of the first half of the twentieth century saw increased reliance on bureaucratic systems of surveillance. During the German occupation of Belgium in World War I, the occupying administration monitored correspondence, required civilians to carry identity documents and restricted civilian movement in the occupied territory through imposing pass systems. During World War II, Occupying Powers became even more dependent on censuses, population registries, identity cards and other forms of systematic documentation to track occupied populations.²²

2.4 The 1949 Geneva Convention IV

Following the Hague conferences and two World Wars, there was a push for further international codification of IHL.²³ The insufficiency of the Hague Regulations in regulating the conduct of the World War II Occupying Powers, and the subsequent weakening of the Regulations' normative power, brought about the drafting of a new regulatory instrument: the Geneva Convention relative to the Protection of Civilian Persons in Time of War (GCIV).²⁴ The Fourth Geneva Convention furthered the obligations first codified in the

²⁰ Mansoor (2023) p. 8-12, 16-19; 1899 Hague Regulations arts 44, 46.

²¹ 1907 Hague Regulations art 42; Kalandarishvili-Mueller, Natia, *Occupation and Control in International Humanitarian Law* (Routledge 2021) p. 92, 94.

²² Torpey, John, *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge University Press 2000) p. 93-116.

²³ Nabulsi (1999) p. 13.

²⁴ Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

Hague Regulations, establishing an extensive bill of rights for occupied populations, with mirroring duties placed on Occupying Powers. It also set further limitations on the legislative power of the occupying administration. However, just as it is sometimes said that history is written by the victors, so indeed were many legal instruments of the postwar period. The Allied powers, being then themselves the occupiers of defeated Axis states, wanted to secure continued leeway in their role as Occupying Powers. The Occupier's duty towards the occupied under GCIV still contained a number of caveats which enabled an Occupying Power broad discretion in the administration of occupied territories.²⁵

The Fourth Geneva Convention also neglected to introduce any temporal limit on occupation. Occupations in the Hague era were conceived as a naturally transitional stage that preceded legal annexation, making temporal limitations obsolete. This changed with the understanding of territorial sovereignty that emerged in the twentieth century. The prohibition on annexation meant that the annexation of occupied territory was no longer possible under international law.²⁶ The (perhaps intended, perhaps unintended) result of the continued lack of a temporal scope for occupation was that while Occupying Powers could no longer formally annex the occupied territory, they could nonetheless extend their occupation indefinitely. This legal loophole enabled, and continues to enable, Occupying Powers to place territories under prolonged occupation, becoming eventually a form of *de facto* annexation.

2.5 Post-1949 developments

From the second half of the twentieth century until today, the nature of occupation has undergone significant change. Surveillance technology has become a core feature of military operations in the modern age, with occupations of the twenty-first century engaging in widespread biometric data collection.²⁷ Biometrics is increasingly used not only as a tool in the 'toolbox'

²⁵ Benvenisti (2012) p. 98-100; GCIV arts 64-67.

²⁶ Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 2(4).

²⁷ Shehabi, Omar Yousef, 'Emerging Technologies, Digital Privacy and Data Protection in Military Occupation' in Buchan, Russell and Lubin, Asaf (eds), *The Rights to Privacy and*

of occupying military forces, but as a partial or full substitute for their physical presence in occupied territories.²⁸ While Article 42 of the 1907 Hague Regulations established that occupation requires the presence of military forces in the territory, the need for Occupying Powers to have ‘boots on the ground’ in order to exercise authority or institute measures of control and order over occupied populations has decreased considerably in modern warfare. The biometric surveillance technologies deployed in the occupations of the present day perform many of the same functions as occupying soldiers. Using only the biometric data extracted from a photograph or video recording, they can utilise live video feeds to identify and track individuals throughout urban neighbourhoods or cities.²⁹

It is in the context of modern technological developments that the stagnated nature of the law of occupation is most urgently felt. While increasingly sophisticated surveillance systems are deployed against civilians in occupied territories, the law of occupation, and IHL more broadly, offers comparatively little guidance on the legal limits of surveillance in occupation settings. The following chapter seeks to clarify those limits.

Data Protection in Times of Armed Conflict (NATO CCDCOE Publications 2022) 87–112. p. 88. See also Estrin, Daniel, ‘Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, but Raises Concerns’ *NPR* (22 August 2019); Dwoskin (2021); Asher-Schapiro, Avi and Osseiran, Nazih, ‘Why Does the US Still Retain the Biometrics of Millions of Iraqis?’ *Reuters* (16 March 2023); Robins-Early, Nick, ‘How Israel Uses Facial-Recognition Systems in Gaza and Beyond’ *The Guardian* (19 April 2024).

²⁸ Goodfriend (2023) p. 468-470.

²⁹ Talbot, Rohan, ‘Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory’ (2020) 102(914) *International Review of the Red Cross* 823–849 p. 836. See also Chapter 6 below.

3 THE LAW OF OCCUPATION AND BIOMETRIC SURVEILLANCE OF THE OCCUPIED

The development of highly advanced surveillance technologies capable of gathering and processing large amounts of biometric data has provided military forces with tools for tracking and monitoring the private lives and movements of occupied populations *en masse*. Since at least the Second Iraq War, large-scale biometric identification systems have been used by militaries in occupation settings to collect and process the biometric data of occupied persons.³⁰ The technologies continue to develop at an accelerating pace, with AI-powered and multimodal surveillance technologies enabling Occupying Powers to intrude into the private sphere of the occupied population on a mass scale.³¹

Black-letter IHL does not specifically address the right to privacy of the occupied or place explicit limitations on biometric surveillance. The fact that technological evolution has outpaced the codification of IHL should not, however, be interpreted as amounting to inherent permission.³² Through examining key provisions of the Hague Regulations and the Fourth Geneva Convention alongside commentary from the International Committee of the Red Cross (ICRC) and other sources, this chapter will examine to what extent biometric surveillance against an occupied population is permissible under international humanitarian law. Focusing specifically on the use of biometric

³⁰ Asher-Schapiro & Osseiran (2023); Zwanenburg, Marten, 'Legal Issues Arising from the Military Use of AI-Supported Biometrics' (2026) 107 *International Law Studies* 152–183 p. 153 and note 111.

³¹ Robins-Early (2024); Human Rights Watch, *'We Had No Choice': 'Filtration' and the Crime of Forcibly Transferring Ukrainian Civilians to Russia* (2022); Amnesty *Automated Apartheid* Report (2023) p. 41-42.

³² Lubin, Asaf and Shehabi, Omar Yousef, 'The New Frontlines: Digital Rights Protection in Contemporary Armed Conflicts' in Ducheine, Paul; Gill, Terry; Pijpers, Peter and Zwanenburg, Marten (eds), *A Research Agenda for Military Law* (Edward Elgar Publishing 2026) 115–125 p. 115.

surveillance in public spaces, at checkpoints and during internment, the chapter will outline what limitations and protections IHL provides for the privacy of the occupied.

3.1 General framework of operation

Occupation is established once the hostile army of a State takes effective control of territory outside of its own borders.³³ It is important to note that, as the laws of occupation are rules *in bello*, the *jus ad bellum* character of underlying hostilities has no bearing on the existence or lawfulness of occupation itself, or on the legal obligations of an Occupying Power.³⁴ Once an occupation factually exists and for as long as it continues, whether formally recognised or not, the Occupying Power is obligated to abide by the applicable rules of IHL. As observed by Vaivos Koutroulis, ‘the scope of application *ratione temporis* of these rules is aligned to their scope of application *ratione materiae*.’ Even when active military operations are no longer being conducted in the territory, as is often the case during prolonged occupation, the rules of IHL will continue to apply.³⁵

The provisions of the Hague Regulations and the Fourth Geneva Convention together outline the general framework of operation for an Occupying Power. A core provision is found in Article 43 of the 1907 Hague Regulations. The provision is recognised as a rule of customary international law,³⁶ and often

³³ 1907 Hague Regulations art 42. While this is most often the territory of another state, occupation may also occur on disputed or contested territory, see Arai-Takahashi, Yutaka, *The Law of Occupation: Continuity and Change of International Humanitarian Law, and Its Interaction with International Human Rights Law* (Martinus Nijhoff Publishers 2009) p 8.

³⁴ Arai-Takahashi (2009) p. 46.

³⁵ Koutroulis, Vaivos, ‘The application of international humanitarian law and international human rights law in situation of prolonged occupation: only a matter of time?’ (2012) 94(885) *International Review of the Red Cross* 165–205 p. 172-174. Koutroulis further notes that while GCIV Article 6(3) would indicate that there is a one-year expiry date on a number of Convention rules, the provision is widely viewed as having been rendered irrelevant. This is supported by Article 3(b) of AP I and by state practice.

³⁶ See, for example, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136 paras 89, 124.

referred to as an expression of the ‘conservationist’ principle. It places a general obligation on the Occupying Power to preserve order and safety in the occupied territory:

The authority of the legitimate power having in fact passed into the hands of the occupant, the latter shall take all the measures in his power to restore and ensure, as far as possible, public order and safety, while respecting, unless absolutely prevented, the laws in force in the country.

The provision can be characterised as a ‘general guideline’ for occupation, requiring that any legislative measure, order or other act undertaken by the Occupying Power must first be filtered through it.³⁷ It is perhaps most easily understood as outlining two separate but interlocked duties of an Occupying Power. Firstly, to ‘take all measures in his power to restore and ensure, as far as possible, public order and safety’. Secondly, to do so while ‘respecting, unless absolutely prevented, the laws in force in the country’. As noted by Rohan Talbot, the first duty of an Occupying Power under Article 43 is to protect the local population from the collapse of security and general safety, and to safeguard public order and civil life. The expression ‘civil life’ does not appear expressly in the English translation of the 1907 Hague Regulations, but is derived from the phrase *la vie publique* used in the French text.³⁸ Widely used as a reference point by legal scholars when determining the scope of the Occupying Power’s obligations under Article 43, ‘civil life’ denotes ‘the social functions [and] ordinary transactions which constitute daily life’³⁹ for any population. It has also been described as encompassing ‘the whole social, commercial and economic life’ of a community.⁴⁰ For an Occupying Power, this first duty is to take measures both to *restore* and *ensure*, meaning an Occupying Power may both act to *restore* disrupted public order or civil life, and to take preventative measures to *ensure* them in the face of future risks.⁴¹ While this may appear to ensure the occupied population far-

³⁷ Benvenisti (2012) p. 69.

³⁸ Talbot (2020) p. 832 and note 60.

³⁹ Schwenk, Edmund Heinz, ‘Legislative Power of the Military Occupant under Article 43, Hague Regulations’ (1945) 54(2) *Yale Law Journal* 393–416 p. 398.

⁴⁰ Koutroulis (2012) p. 178 and note 68.

⁴¹ Schwenk (1945) p. 398.

reaching protections, it is worth noting that the provision does not require an Occupying Power to factually deliver this outcome. It only requires that the Occupying Power acts ‘as far as possible’ towards this end, using all measures ‘within its power’. In practice, the leeway created by these caveats enables the Occupying Power to balance its obligations towards the occupied civilian population with its own military interests,⁴² often entirely at its own discretion.

A similar issue emerges in the practical realisation of the second duty under Article 43. When administering the occupied territory, the Occupying Power is required to respect the laws already in place, ‘unless absolutely prevented’ from doing so. The traditional interpretation provides that an Occupying Power should keep domestic law, meaning the law of the ousted sovereign, intact. However, the legal landscape has changed considerably in the time since the drafting of the Hague Regulations. Many States are now parties to international human rights conventions. This raises the question of whether the meaning of domestic law has evolved to include the international human rights obligations of an ousted government. Regardless of whether the meaning of ‘laws in force’ is interpreted narrowly or broadly, practical application of the second duty is effectively left in the hands of the Occupying Power. As observed by Marco Sassòli,⁴³ Occupying Powers have historically used the ambiguity of Article 43 to their own benefit. The duty to ‘restore and ensure’ has, alongside Article 64(2) of the Fourth Geneva Convention, been invoked as a justification for imposing broad legislative measures on populations,⁴⁴ often at the expense of their rights. On the other hand, the duty to respect local laws ‘unless absolutely prevented’ has been used by Occupying Powers to

⁴² Talbot (2020) p. 832.

⁴³ Sassòli, Marco, ‘Legislation and Maintenance of Public Order and Civil Life by Occupying Powers’ (2005) 16(4) *European Journal of International Law* 661–694 p. 663.

⁴⁴ See, for example, the case HCJ 393/82 *Jam’iat Iscan Al-Ma’almoun Al-Ta’awuniya Al-Mahdouda Al-Masouliya Cooperative Society v Commander of IDF Forces in the Judea and Samaria Region* [1983] IsrSC 37(4) 785, referenced by Koutroulis (2012) p. 181-182 and note 9.

skirt their obligation to ensure the welfare and continued civil life of the occupied population by neglecting to introduce legislation even in the face of pressing social needs.⁴⁵

In cases of prolonged occupation, some legal scholars take the view that the Occupying Power is granted more leeway in its legislative powers over the occupied territory, allowing it to institute more extensive and permanent changes.⁴⁶ Such legislative changes can have both positive and negative results for the occupied population. Protracted occupations may go on for several years or decades. If no legal changes are introduced by the Occupying administration, the population may be left living under a stagnant, outdated legal system or with inadequate development or legal protections. Yet at the same time, an Occupying Power that institutes wide-spanning legislative changes may violate the sovereignty of the occupied territory while the changes will not necessarily be those that benefit the occupied population. The Occupying Power will first and foremost be concerned with the protection of its military forces and installations, not with the privacy rights of the occupied. Therefore, as Koutroulis argues, a faithful interpretation of Article 43 means understanding the full provision in the context of safeguarding civil life. In this light, a prolonged occupation will place a further duty on the Occupying Power to ensure that the population can return to normalcy. The longer an occupation lasts, the less acceptable it becomes for an Occupying Power to suggest there are ‘no measures in its power’ to restore and safeguard the rights of the occupied.⁴⁷ Otherwise, occupied populations risk being forced to live indefinitely under restrictive and intrusive military orders.⁴⁸

Another core provision of the law of occupation is found in Article 27 of the Fourth Geneva Convention. The provision further defines an Occupying Power’s obligations towards the occupied population. Article 27(1) of the

⁴⁵ Sassóli (2005) p. 663.

⁴⁶ Koutroulis (2012) p. 176-178.

⁴⁷ *Ibid* p. 183.

⁴⁸ In its 2019 report *Born Without Civil Rights: Israel’s Use of Draconian Military Orders to Repress Palestinians in the West Bank*, Human Rights Watch (HRW) similarly contends that the Occupying Power’s obligation to restore civil life ‘increases in a prolonged occupation, where the occupier has more time and opportunity to develop more narrowly tailored responses to security threats that minimize restrictions on rights.’

Convention establishes the central humanitarian principle that governs all provisions related to the protection of fundamental rights. It asserts that civilians under occupation

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. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity.⁴⁹

This echoes an earlier provision, found in Article 46 of the 1907 Hague Regulations:

Family honour and rights, the lives of persons, and private property, as well as religious convictions and practice, must be respected.⁵⁰

In its 1958 Commentary to the GCIV, the International Committee of the Red Cross (ICRC) asserts that the right to respect for the person should be interpreted in the broadest sense. According to the Commentary, it must be understood to cover ‘all the rights of the individual’ and ‘includes, in particular, the right to physical, moral and intellectual integrity’.⁵¹ The 1958 Commentary asserts that one aspect of the right to ‘moral and intellectual integrity’ of persons is that their ‘names or photographs, or aspects of their private life must not be given publicity’.⁵² The specific protection against ‘publicity’ does not entail privacy in a broad or all-encompassing sense, however. It refers specifically to the collection and dissemination of images and various forms of private information with the intention of exposing or humiliating occupied persons.⁵³ The requirement of ‘respect for honour’ of the person is more expansive, protecting against not only libel, slander and insult but also ‘any viola-

⁴⁹ GCIV art 27(1).

⁵⁰ 1907 Hague Regulations art 46. See also Convention relative to the Treatment of Prisoners of War (adopted 27 July 1929, entered into force 19 June 1931) 118 LNTS 343 art 14(1).

⁵¹ Pictet, Jean (ed), *Commentary on the Geneva Conventions of 12 August 1949, Volume IV: Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (International Committee of the Red Cross 1958) p. 201.

⁵² *Ibid.* See also Talbot (2020) p. 853.

⁵³ Shehabi (2022) p. 98.

tion of a personal nature'. In its 2025 Commentary, the ICRC goes on to identify new surveillance technologies as entailing risks specifically to the right to respect for 'persons and their honour'.⁵⁴

As a counterpoint to the humanitarian obligations of Article 27(1), however, Article 27(4) authorises an Occupying Power to 'take such measures of control and security in regard to protected persons as may be necessary as a result of the war'. What control and security measures an Occupying Power may enact under this provision is not further specified, and the 'choices of means' are therefore largely left to the Occupying Power itself.⁵⁵ This allows it to undertake a wide array of measures that serve its military interests.⁵⁶ The 1958 ICRC Commentary provides a non-exhaustive list with examples of possible measures, ranging from requirements that the occupied carry identity cards or other documents, to restrictions of their movement, or even assigned residence and internment.⁵⁷ There is no mention of the deployment of surveillance technology or biometrics; neither the parties drafting the Fourth Geneva Convention in 1949 nor the authors of the ICRC Commentary in 1958 could feasibly anticipate the nature, scale and capability of the surveillance technologies used in occupation settings today. But in its updated 2025 Commentary to the GCIV, the ICRC makes particular note of the development of new technologies for surveillance, including technologies using automated biometric data processing and artificial intelligence.⁵⁸ Discussing the right to respect for the person, the 2025 Commentary states:

Depending on the circumstances, surveillance and (biometric) data collection may infringe upon the dignity of protected persons, expose them or make them more vulnerable to ill-treatment or suffering and violate the right of respect for their persons and honour. [...] Any collection and processing of personal data of protected persons must adhere to applicable data protection standards.⁵⁹

⁵⁴ International Committee of the Red Cross, *Commentary on the Fourth Geneva Convention: Convention (IV) Relative to the Protection of Civilian Persons in Time of War* (2nd Edition, ICRC 2025) para 2224. See also Shehabi (2022) p. 97.

⁵⁵ 1958 ICRC Commentary p. 207.

⁵⁶ Talbot (2020) p. 833.

⁵⁷ 1958 ICRC Commentary p. 207.

⁵⁸ 2025 ICRC Commentary para 2224 and note 83.

⁵⁹ *Ibid* para 2224.

Against this background, the following section examines what limitations IHL places on the use of biometric surveillance technologies in occupied territory.

3.2 Biometric surveillance of the occupied

While provisions found in both the Hague Regulations and GCIV permit Occupying Powers to adopt measures of control and security, such measures remain subject to the protections afforded to occupied populations under IHL. This section therefore examines under what conditions biometric surveillance practices may be reconciled with IHL, and consequently the extent to which Occupying Powers may lawfully deploy such surveillance measures.

Looking first to the leeway given to Occupying Powers under Article 43 of the 1907 Hague Regulations, it follows that the duty to restore and ensure general safety, public order and civil life for the occupied can justify deploying biometric surveillance technology in a similar manner to the use of the same technology by law enforcement authorities in domestic settings. Measures that can feasibly be permitted under the provision include the collection of the biometric data of those partaking in hostilities. It can also include the use of biometric identification methods at military checkpoints to limit the movements of individuals suspected of engaging in resistance activities, or to identify and detain known combatants.⁶⁰ The need to ensure the ‘civil life’ of the occupied in the face of threats from within the territory has often been a justification invoked by Occupying Powers such as Russia and Israel for the collection of biometric data and the implementation of various other means of biometric surveillance.⁶¹

⁶⁰ Talbot (2020) p. 833.

⁶¹ Written Statement of the State of Israel, *Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem* (Written Proceedings, 27 July 2023) p. 3; B’Tselem, *Playing the Security Card: Israeli Policy in Hebron as Means to Effect Forcible Transfer of Local Palestinians* (2019) p. 14-15; HRW *We Had No Choice* Report (2022).

Measures instituted under Article 43 of the 1907 Hague Regulations must be intended to safeguard the occupied population. As such, they cannot be enacted for the sole purpose of serving the security interests of the Occupying Power. However, an Occupying Power may still enact measures to ensure its own security under Article 27(4) of the GCIV. By invoking its discretion under Article 27(4), an Occupying Power can deploy biometrics as ‘measures of control and security’ in the service of military interests. It is important to note that while there are a wide range of means permitted under 27(4), the discretion provided under the provision is not unlimited. Any deployment of biometric surveillance must be balanced against the obligation to treat the occupied population humanely and with respect for their persons and should not affect their fundamental rights.⁶² The Occupying Power is thus required to weigh its own security interests against the consequences experienced by the occupied.

The following three subsections examine the legality under IHL of biometric surveillance in three key settings where the technology has frequently been utilised by Occupying Powers:⁶³ public spaces, military checkpoints and places of internment.

3.2.1 Public spaces

Public spaces in occupied territories, such as streets, marketplaces, train stations, public transportation systems and other forms of public infrastructure, are essential to the civil life of the occupied population. The continued functioning of social, commercial and economic life within occupied territories, which constitutes a core obligation of the Occupying Power,⁶⁴ necessarily depends on civilians’ access to and use of these public spaces.

Provided there is a legitimate reason under either Article 43 of the 1907 Hague Regulations or 27(4) of GCIV, IHL permits an Occupying Power to institute legislative measures to monitor and restrict the public movements of

⁶² 1958 ICRC Commentary p. 207.

⁶³ See Chapter 5.

⁶⁴ See Section 3.1.

the occupied population. Traditional measures have included limiting access to public areas, or requiring the carrying of identity cards or other documents.⁶⁵ Technological advancements over the last two decades have also made a variety of highly sophisticated automated and non-automated FRT tools available to Occupying Powers that seek to monitor the public spaces of occupied territories *en masse*.

Tools for automated biometric surveillance include live facial recognition technology (LFRT). LFRT can be integrated into existing closed-circuit television (CCTV) feeds. Its capabilities include providing automated facial recognition by scanning live video feeds of public spaces and matching persons seen on the feeds to databases of existing biometric records. The deployment of LFRT-enabled surveillance systems mean Occupying Powers can remotely and covertly identify subjects and track their movements throughout areas of the public. Many LFRT-systems are AI-enabled, and the speed and efficiency of their automated identification capabilities far exceeds the capacity of humans performing the same tasks.⁶⁶

As Rohan Talbot describes, the use of FRTs to monitor the public movements of civilians sits at ‘the fulcrum’ of interests IHL seeks to balance. Even when deployed with the intent to capture enemy combatants or protect military installations, both constituting legitimate purposes under IHL, they may nonetheless diminish civil life and constitute a form of indiscriminate mass surveillance incompatible with the requirements under GCIV Article 27.⁶⁷ In this context it is worth noting that the use of CCTV and automated biometric processing tools, both including and excluding AI-technology, are measures which the 2025 ICRC Commentary views as posing a risk to the dignity and honour of occupied persons under Article 27(1).⁶⁸ While IHL offers no conclusive guidance on when they may or may not be used, the ICRC Commentary indicates that their use should at least be restrictive.

⁶⁵ 1958 ICRC Commentary p. 207.

⁶⁶ Talbot (2020) p. 825-827.

⁶⁷ *Ibid* p. 834.

⁶⁸ 2025 ICRC Commentary para 2224 and notes 84-85.

3.2.2 Checkpoints

Military checkpoints, including roadblocks and other forms of ID controls, are a measure that the Occupying Power may establish in the occupied territory.⁶⁹ The installation of checkpoints is permitted under IHL provided they are necessary for security purposes and proportional in their scope and duration. Occupying Powers may use checkpoints to restrict access to areas of the occupied territory, and conduct identity checks to ensure that only those permitted access can pass.⁷⁰ Under IHL, an Occupying Power may continue to maintain checkpoints even after the general close of military operations, provided that this is justified by military exigencies.⁷¹

Both IHL and associated commentaries by the ICRC provide little guidance on how biometrics may be deployed at checkpoints. In its 2004 Advisory Opinion, the ICJ found that Israel's separation wall and its 'associated regime' of administrative measures, including its system of checkpoints, permits and ID cards, constituted a grave infringement on the rights of the Palestinians.⁷² In the years since, Israel has expanded its West Bank checkpoint regime to include both verification through biometric IDs and LFRT-enabled CCTV surveillance.⁷³ In light of this, the findings of the 2024 Advisory Opinion that Israel's practice of using checkpoints to impose indiscriminate restrictions on all Palestinians 'are disproportionate to any legitimate public aim and cannot be justified with reference to security'⁷⁴ may have implications for at least the more invasive or prolonged uses of biometrics at checkpoints.

3.2.3 Internment and detention

In occupation settings, internment is the forcible placement of occupied subjects in facilities where they are deprived of liberty. Article 78 of GCIV per-

⁶⁹ Shehabi (2022) p. 104.

⁷⁰ *The Wall AO* paras 136-137; *Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem* (Advisory Opinion) [2024] ICJ Rep 753 para 205; 2025 ICRC Commentary paras 2349-2350, 2352.

⁷¹ *The Wall AO* para 135.

⁷² *Ibid* paras 133-137; Talbot (2020) p. 834.

⁷³ See Section 5.2.

⁷⁴ *Policies and Practices AO* paras 201-206.

mits the Occupying Power to place occupied subjects in internment in exceptional circumstances when it is imperative for reasons of security.⁷⁵ Alongside assigned residence, internment constitutes the harshest measure an Occupying Power may institute against the civilian population.⁷⁶ In addition to internment, an Occupying Power may also arrest and detain civilians for criminal offences when enforcing either local laws or laws instated by the Occupying Power itself.⁷⁷ Occupied subjects are protected by Article 27(1), requiring respect for their person(s) ‘in *all* circumstances’, and their humane treatment ‘at *all* times’ – including when deprived of liberty.⁷⁸ In its 2025 Commentary, the ICRC notes specifically that the risk of suffering violations to the right to respect for their person through surveillance and biometric data collection is particularly exacerbated for occupied subjects who are interned or otherwise detained under the Occupying Power.⁷⁹

Discussing the use of various measures of surveillance to maintain order in a place of internment,⁸⁰ the ICRC observes that ‘a certain reduction in privacy’ is an inherent feature of internment. However, any infringements in privacy must be justified by legitimate grounds, such as security reasons, and also proportional to them.⁸¹ Identifying the use of CCTV as ‘pervasive’ in detention settings and other holding places, the 2025 ICRC Commentary states that ‘[l]imited, well-regulated and well-managed video surveillance’ is not in principle prohibited under either of GCIV Articles 27(1) or 100. In fact, the Commentary finds that it may in *specific* circumstances be an appropriate measure of surveillance, if paired with adequate safeguards.⁸² However, the Commentary identifies several risks associated with the use of highly advanced ‘omniscient’ surveillance technologies that collect, store and process the biometric data of internees in an automated manner, such as through automated

⁷⁵ 2025 ICRC Commentary para 2346.

⁷⁶ GCIV arts 27(4), 78; 1958 ICRC Commentary p. 201.

⁷⁷ GCIV arts 64-66, 71-76.

⁷⁸ GCIV art 27(1); 2025 ICRC Commentary para 4195.

⁷⁹ 2025 ICRC Commentary paras 2224, 5053.

⁸⁰ GCIV art 100.

⁸¹ 2025 ICRC Commentary paras 5051-5052. The commentary refers to all surveillance, meaning both surveillance by automated means (such as CCTV) and non-automated means (such as direct observation by guards).

⁸² *Ibid* paras 2744, 5051-5052, 5054.

FRTs, AI-integration or a combination of the two. In particular, the risk that biometric data is abused means that any collection and processing of it in internment settings must be ‘proportionate to a legitimate purpose’ and ‘subject to a degree of protection, confidentiality and security’ that reflects its heightened sensitivity.⁸³

In light of this, the 2025 Commentary further discusses what surveillance measures can constitute violations of the internees’ rights under GCIV. Though the Commentary makes no definitive statement on legality, it states that all measures must be weighed against other, less intrusive alternatives that would achieve the same legitimate purpose. Due to the highly intrusive nature of biometric surveillance systems, and the continuous identification and tracking they expose the occupied subject to, it follows that the threshold of justification for collecting biometric data and using biometric surveillance is correspondingly higher. The ICRC Commentary also emphasises that if other means of surveillance are available, occupied subjects should not be exposed to pervasive monitoring environments where they cannot avoid video surveillance at all. Additionally, the ICRC states that instituting blanket measures on an indiscriminate basis, without individual assessment, risks violating requirements of necessity and proportionality. Furthermore, interned subjects should be informed of the video surveillance, and data collected from the surveillance systems must be used and managed in compliance with ‘applicable data protection requirements’.⁸⁴

⁸³ *Ibid* para 5053.

⁸⁴ *Ibid* para 5054.

4 THE RIGHT TO PRIVACY UNDER INTERNATIONAL HUMAN RIGHTS LAW IN OCCUPATION SETTINGS

When an Occupying Power implements biometric surveillance measures in the occupied territory, their actions are not only subject to the rules of IHL but also to the larger international legal system. This means that whether an Occupying Power invokes their obligation to ensure public order and civil life for the occupied under Article 43 of the 1907 Hague Regulations, or the safeguarding of its own military and security needs under Article 27(4) of the Fourth Geneva Convention, or both, IHL alone is insufficient for determining the legality of the measures in question.⁸⁵

Today, many States across the world have ratified IHRL treaties on the international and regional level and formally made human rights law part of their domestic legal systems. The right to privacy in occupation may therefore apply in a number of ways. It may apply as customary international law, owing to its universality. It may apply extraterritorially, emanating from the Occupying Power's own legal system. It may also apply as local law in the occupied territory, which the Occupying Power is bound to respect.⁸⁶

Given that international human rights law applies concurrently with IHL, a legal evaluation of the occupying army's use of biometrics must therefore consider not only the humanitarian principles of IHL but also the occupied population's right to privacy under IHRL.

4.1 Concurrent application of international human rights law in occupation settings

Developments in jurisprudence over the past decades have made it clear that international humanitarian law does not displace international human rights

⁸⁵ International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (Report to the 33rd International Conference of the Red Cross and Red Crescent, Geneva, 12 December 2019) p. 21; Talbot (2020) p. 836.

⁸⁶ 1907 Hague Regulations art 43 *in fine*.

law in situations of occupation. While IHL applies exclusively in armed conflict, IHRL is not its ‘mirror-opposite’. Rather, IHRL is an overarching legal framework that applies both in war and peacetime,⁸⁷ and that is often necessary for ascertaining the specific contents of the rights of the occupied.⁸⁸ This has been made evident many times over in the practice of the International Court of Justice (ICJ). The Court has on several occasions established that both bodies of law apply concurrently by asserting that ICCPR and other major human rights treaties continue to apply alongside IHL in an occupation setting,⁸⁹ and that an Occupying Power’s obligation to ensure ‘public order and civil life’ under Article 43 of the 1907 Hague Regulations includes respecting the applicable rights under IHRL.⁹⁰ Both the ICJ and regional human rights courts such as the European Court of Human Rights (ECtHR) demonstrate this by continuously evaluating the conduct of occupying armies through IHRL as well as IHL.⁹¹ Concurrent application of both legal regimes during occupation is largely considered unchallenged, except by the United States and Israel.⁹²

Though there is near-consensus on the concurrent application of the two legal regimes, international law provides no precise guidance on how they should be balanced against each other when they come into a conflict of norms. In *The Wall AO*, the ICJ asserted that human rights law applies generally to the occupied territory of Palestine, but that IHL was the *lex specialis* in situations of armed conflict.⁹³ A similar assertion has been made by the International Criminal Tribunal for the former Yugoslavia, which stated that human rights

⁸⁷ Lubell, Noam, ‘Human rights obligations in military occupation’ (2012) 94 (885) *International Review of the Red Cross* 317-337 p. 318.

⁸⁸ McCarthy, Conor, ‘Legal Reasoning and the Applicability of International Human Rights Standards During Military Occupation’ in in Arnold, Roberta and Quéniwet, Noëlle (eds), *International Humanitarian Law and Human Rights Law: Towards a New Merger in International Law* (Martinus Nijhoff Publishers 2008) 101–118 p. 121.

⁸⁹ *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 para 240; *The Wall AO* para 106.

⁹⁰ *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168 para 178; Talbot (2020) p. 836.

⁹¹ Gross, Aeyal, *The Writing on the Wall: Rethinking the International Law of Occupation* (Cambridge University Press 2017) p. 338. See, for example, *The Wall AO* para 134. See also the case of *Loizidou v. Turkey* (Judgment) App no 15318/89 (ECtHR, 23 March 1995) para 52, where the ECtHR found that ECHR applies to occupied Cyprus.

⁹² Benvenisti (2012) subsection 1.3.2.

⁹³ *The Wall AO* para 106.

can be transposed ‘only if they take into consideration’ the specificities of IHL.⁹⁴ This would indicate that, while both legal regimes should be read together, IHL takes primacy should they collide. The UN Human Rights Committee, on the other hand, has rejected the *lex specialis* argument and has asserted that the two bodies of law are complementary, not mutually exclusive.⁹⁵ The Human Rights Committee has further asserted that in situations of occupation, the applicability of IHL ‘does not preclude’ the application of the ICCPR. The Committee asserts specifically that the provisions of ICCPR apply ‘to the benefit of the population of the occupied territories’.⁹⁶

Even if one were to subscribe to the *lex specialis* approach to concurrent application, this does not necessarily devalue the role of IHRL. As Talbot points out, *lex specialis* can be argued two ways. While IHL is indeed the more specific body of law for military occupation settings generally, IHRL provides the *lex specialis* guidance on States’ obligations to respect the privacy of individuals.⁹⁷

4.2 The right to privacy under international human rights law

The right to privacy is a fundamental human right enshrined in Article 12 of the Universal Declaration of Human Rights⁹⁸ and made enforceable through Article 17 of the International Covenant on Civil and Political Rights,⁹⁹ Article 8 of the European Convention on Human Rights¹⁰⁰ and other regional and international human rights instruments.¹⁰¹ It also makes up part of customary

⁹⁴ *Prosecutor v Kunarac, Kovač and Vuković* (Trial Judgment) IT-96-23-T & IT-96-23/1-T (ICTY, Trial Chamber, 22 February 2001) para 471.

⁹⁵ Human Rights Committee, *General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant* (29 March 2004) UN Doc CCPR/C/21/Rev.1/Add.13 para 11.

⁹⁶ Human Rights Committee, *Concluding Observations of the Human Rights Committee: Israel* (29 July 2010) UN Doc CCPR/C/ISR/CO/3 para 5.

⁹⁷ Talbot (2020) p. 838.

⁹⁸ Universal Declaration of Human Rights, UNGA Res 217 A(III) (10 December 1948) (UDHR) art 12.

⁹⁹ ICCPR art 17.

¹⁰⁰ ECHR art 8.

¹⁰¹ See, for example, Charter of Fundamental Rights of the European Union [2000] OJ C364/1 (CFR) arts 7 and 8(1), discussed in Chapter 5.

international law.¹⁰² The right to privacy protects individuals from ‘unlawful and arbitrary interference’ with their privacy,¹⁰³ and requires that any State interference with this right meets the standard of legality, legitimate purpose, necessity and proportionality.¹⁰⁴ In a surveillance context, the collection and processing of biometric data may interfere with individuals’ privacy in several dimensions, affecting both their bodily and informational privacy.¹⁰⁵

4.2.1 Article 17 of the International Covenant on Civil and Political Rights

Article 17 of the ICCPR asserts that ‘no one shall be subjected to arbitrary or unlawful interference’ with their privacy, and that ‘everyone has the right to protection of the law against such interference’.¹⁰⁶ At the core of this right is the concept of individual liberty and autonomy; the right to exist freely and to both partake in public life and to withdraw into one’s own private sphere. This private sphere traditionally consisted of the features mentioned explicitly in Article 17(1): family, home and correspondence. Individual existence, such as appearance, identity, name and genetic code are various dimensions of the right to privacy. Advancements in technology and society have expanded upon the traditional understanding of privacy to include personal data and biometric information.¹⁰⁷ Furthermore, privacy as it is understood in the Covenant, is not limited to what an individual wishes to keep hidden from the public. Secrecy is only one aspect of privacy. The right to privacy also protects against arbitrary and unlawful interference with the private acts of individuals that are conducted in public spaces.¹⁰⁸

Article 17(2) asserts that individuals have the right to legal protection against arbitrary or unlawful interference. This provision creates a positive obligation

¹⁰² Lubin (2022) p. 471.

¹⁰³ ICCPR art 17(1).

¹⁰⁴ UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* UN Doc A/HRC/39/29 (3 August 2018) paras 38-39.

¹⁰⁵ *Ibid* paras 6-7.

¹⁰⁶ ICCPR art 17(1-2).

¹⁰⁷ Nowak, Manfred, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd Revised Edition, N.P. Engel Verlag 2005) p. 378, 387.

¹⁰⁸ *Ibid* p. 377-379.

on the part of States to institute regulatory measures safeguarding privacy, an obligation which extends especially to persons detained or otherwise deprived of liberty, as well as those in vulnerable positions.¹⁰⁹

The right to privacy is not absolute. In contrast to other derogable provisions of the ICCPR,¹¹⁰ Article 17 does not contain a derogation clause allowing for restriction of privacy under certain conditions, such as for national security or public order.¹¹¹ Instead, the provision allows State interference so long as the interference is conducted lawfully and non-arbitrarily, and prohibits it only when it fails to meet either one of the two standards.

Looking first at the meaning of ‘unlawful interference’, this is generally understood to mean interference in violation of provisions under the domestic legal system. However, a State cannot circumvent its obligation to respect the right to privacy by neglecting to legislate for the protection of privacy. The positive obligation under Article 17(2) means that legal protection is in of itself part of the right to privacy.¹¹²

Looking next at the meaning of ‘arbitrary’ interference, this means any act of interference with the privacy of individuals that may be lawful under the domestic legal system, but that is nevertheless either unjust, unpredictable or unreasonable. When evaluating whether a specific act of interference by a State is arbitrary or not, the assessment must take into account whether the act has a purpose that is legitimate under the Covenant in its entirety,¹¹³ whether it is predictable and whether it is proportional (i.e. reasonable) in relation to the purpose or the specific circumstances.¹¹⁴

¹⁰⁹ *Ibid* p. 380.

¹¹⁰ See, for example, the derogation clauses in ICCPR arts. 12(3), 18(3), 19(3), 21 and 22. See also ECHR art 8(2).

¹¹¹ Nowak (2005) p. 381.

¹¹² *Ibid* p. 382-383.

¹¹³ This includes the ‘purposes, aims and objectives’ of the Covenant. See, for example, *Canepa v. Canada* Communication No 558/1993, UN Doc CCPR/C/59/D/558/1993 (HRC, 3 April 1997) para 11.4.

¹¹⁴ Nowak (2005) p. 381, 383-384. Purposes may be, *inter alia*, public order, security or protecting the rights of others.

4.2.2 Article 8 of the European Convention on Human Rights

Article 8(1) of the ECHR provides that each person has the right to respect for their private life. While the phrase ‘private life’ differs from ‘privacy’, the two provisions carry essentially the same meaning in the context of biometric surveillance. The right to respect for private life protects individuals from interference with their physical and psychological integrity, as well as from unwanted access to and collection of information.¹¹⁵ While the provision itself makes no reference to biometric data or surveillance, the position taken by the European Court of Human Rights is that the notion of ‘private life’ under ECHR must be interpreted broadly, and that it is not possible to provide a singular or exhaustive definition.¹¹⁶ It includes the protection of biometric data, considering it ‘of fundamental importance’ to the enjoyment of the right to respect for private life.¹¹⁷

Just as with the right to privacy under the ICCPR, the right to respect for private life under ECHR is not absolute. Article 8(2) establishes that there are instances where public authority can limit this right, provided that such limitations are lawful and ‘necessary in a democratic society’ in the interest of, *inter alia*, ‘national security, public safety’ or crime prevention.¹¹⁸ There is also the possibility of derogation under Article 15 of the ECHR in time of war or other emergencies. However, the mere fact that Article 8(2) gives States discretionary allowances to limit the right to respect for private life in certain conditions should not be interpreted as permitting the ‘annihilation’ of privacy.¹¹⁹

¹¹⁵ Ovey, Clare and White, Robin C.A., *The European Convention on Human Rights* (5th Edition, Oxford University Press 2010) p. 357.

¹¹⁶ *Niemietz v. Germany* App no 13710/88 (ECtHR, 16 December 1992) para 29.

¹¹⁷ *Glukhin v. Russia* App no 11519/20 (ECtHR, 4 July 2023) para 75.

¹¹⁸ ECHR art 8(2).

¹¹⁹ *Bărbulescu v. Romania* App no 61496/08 (ECtHR [GC], 5 September 2017) para 80. See also Argren, Rigmor, ‘Protection of biometric private life under the European Convention on Human Rights and the law of armed conflict’ (2024) 61(1) *The Military Law and the Law of War Review* 61–88 p. 71.

Article 8 has seen considerable legal development through case law,¹²⁰ and contains the most central right in the context of surveillance and data retention.¹²¹ In adjudicating cases regarding the right to private life, the European Court of Human Rights has established extensive jurisprudence on how States must balance the conflicting interests of individuals of their right to private life versus the States' interest in surveillance and other privacy interferences. Particularly relevant to occupation is the general obligation contained in Article 1 of the ECHR, that requires its member States to 'secure to everyone within their jurisdiction the rights and freedoms' of the convention. The ECtHR has consequently developed a doctrine of extraterritorial jurisdiction,¹²² extending the territorial scope of ECHR convention obligations beyond the borders of the member States. The jurisprudence of the ECtHR is therefore particularly useful when looking at privacy in the context of military surveillance operations, as it has found that 'in many situations in which armed forces would make use of biometrics abroad, the ECHR will apply'.¹²³ The extraterritorial application of the ECHR would not inherently constitute a guarantee of privacy for the occupied, however. As previously mentioned, the right to private life under ECHR is not an absolute right. It is a so-called 'limitation right', meaning the language Article 8 itself permits States to limit the right. Additionally, Article 8 is derogable - though, as Rigmor Argren notes, what additional derogation could feasibly be necessary beyond what is already permitted is unclear. At present, no State has expressly derogated from ECHR in situations where they have jurisdiction outside of their territorial borders.¹²⁴

¹²⁰ Schabas, William, *The European Convention on Human Rights: A Commentary* (Oxford University Press 2015) p. 358.

¹²¹ European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights: Data Protection* (28 February 2026) p. 7. See also *Glukhin v. Russia* App no 11519/20 (ECtHR, 4 July 2023) para 75.

¹²² Argren (2024) p. 71. See also Zwanenburg, Marten and van de Put, Steven, 'The Use of Biometrics in Military Operations Abroad and the Right to Private Life' in Pijpers, Peter; Voskuil, Mark and Beeres, Robert (eds), *Towards a Data-Driven Military: A Multidisciplinary Perspective* (Leiden University Press 2022) 283–302 p. 286-289 on the question of extraterritorial application.

¹²³ Argren (2024) p. 72.

¹²⁴ *Ibid.*

4.3 Jurisprudence of the European Court of Human Rights

The case law of the ECtHR has dealt extensively with the use of biometrics and surveillance in law enforcement operations on the domestic level. Evaluating this case law is relevant for two reasons. Firstly, the extraterritorial application of Convention rules means that Occupying Powers that are parties to the ECHR would be subject to its provisions when operating in occupied territory. Even in cases where the ECHR is not directly applicable, ECtHR jurisprudence may still speak to the contents of the right to privacy under ICCPR or IHRL more generally. Secondly, in many prolonged military occupations where there are no longer active hostilities, the Occupying Power's administration of the territory will closely resemble that of a domestic government. An analogy to domestic law enforcement operations can therefore help ascertain the legality of biometric surveillance measures deployed against the occupied.

Just as the UN High Commissioner for Human Rights has asserted that the right to privacy applies even in public settings,¹²⁵ the ECtHR has concluded that the protected private sphere of individuals extends to some degree into their public life.¹²⁶ Consequently, while the use of CCTV to monitor public spaces does not *per se* constitute interference with the right to privacy, 'the recording of the data and systematic or permanent nature of the record may give rise to such considerations'.¹²⁷ On the question of biometrics, the ECtHR consistently aligns itself with the standard set out in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+),¹²⁸ defining biometric data as a special category of data that may only be processed if there are heightened legal safeguards in place.

¹²⁵ HRC *Right to Privacy in the Digital Age* Report (2018) para 38.

¹²⁶ *Glukhin v. Russia* para 64.

¹²⁷ *Peck v. United Kingdom* App no 44647/98, (ECtHR, 28 January 2003) para. 57; *Glukhin v. Russia* para 66.

¹²⁸ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data as amended by the Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No 223 art 6(2).

4.3.1 Public spaces

In the case of *Glukhin v. Russia*, law enforcement collected digital images of the applicant and used its LFRT-equipped CCTV surveillance system of the Moscow underground to locate the applicant based on his biometric data. The applicant was subsequently arrested with the intent of charging him with an administrative offence. The ECtHR found that both the use of FRT technology to identify the applicant based on digital images *and* the real-time deployment of it to locate and apprehend him while he was in public constituted a violation of the applicant's right to private life. The Court asserted that interference under Article 8(2) must be lawful, must pursue a legitimate aim and must be 'necessary in a democratic society'. The Court characterized the use of LFRT as a 'particularly intrusive' interference with private life and found that the deployment of LFRT surveillance in public spaces requires 'the highest level of justification'.¹²⁹

The case of *Big Brother Watch and Others v. the United Kingdom* did not deal directly with the surveillance of public spaces, but instead with the bulk interception of data. The ECtHR judgment is nonetheless interesting for the former, as the Court characterised the interaction between mass surveillance and privacy rights as a 'sliding scale' of infringement. This meant that beginning with the initial interception of data, the degree of infringement on privacy would increase when the data was stored and automatically processed and increase even further when the data was examined by an analyst.¹³⁰ The Court found that the practice of bulk interception constituted a violation of Article 8. It came to a different conclusion in the *Centrum for Rättvisa v. Sweden* case, the difference being that Sweden was deemed to have instituted adequate legal safeguards against 'arbitrariness and the risk of abuse'.¹³¹ Particularly relevant for the question of extraterritorial application during occupation is that in both cases, neither the ECtHR nor the parties challenged the

¹²⁹ *Glukhin v. Russia* paras 37, 68, 78, 86.

¹³⁰ Shehabi (2022) p. 90-91; *Big Brother Watch and Others v. the United Kingdom* Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR [GC], 25 May 2021) para 329.

¹³¹ *Big Brother Watch and Others v. the United Kingdom* para 2; *Centrum för Rättvisa v. Sweden* App no 35252/08 (ECtHR [GC], 25 May 2021) para 181.

Convention's scope of application, instead leaving it uncontested that the ECHR applied to foreign mass surveillance operations.¹³²

4.3.2 Checkpoints

While there is no direct parallel to a military checkpoint in a domestic setting, a comparative environment could potentially be a police station, such as in the case of *Perry v. the United Kingdom*. In *Perry v. the United Kingdom*, the applicant had refused to participate in a police lineup. Law enforcement officers subsequently arranged for the applicant to be covertly filmed while he was brought to a police station for identification and questioning purposes. Although the CCTV camera in the custody area was permanently operating, it had been specifically adjusted to obtain clear images of the applicant. The footage was later used to create a video lineup shown to witnesses. The applicant had not consented to the video recording and was not informed that the captured images would be used in this manner.¹³³ The ECtHR held that the covert recording and subsequent use of CCTV footage constituted an interference with the applicant's right to private life, emphasizing that the systematic recording and processing of identifiable images by law enforcement engages privacy protections even in spaces not ordinarily considered private. Specifically, the Court found that the officers had contravened domestic law by failing to ask for the applicant's consent, failed to inform him of the creation of the video lineup and his right to view it and object to its contents. As their conduct was not compliant with the legal safeguards under domestic law, the interference was unlawful and therefore in violation of ECHR Article 8.¹³⁴

The case may function as an analogy to military checkpoints, where individuals are similarly compelled to pass through controlled spaces operated by Occupying authorities where they are subjected to covert or systematic biometric surveillance. Additionally, when military checkpoints form an una-

¹³² Lubin (2022) p. 470-471.

¹³³ *Perry v. the United Kingdom* App no 63737/00 (ECtHR 17 July 2003) paras 13-15.

¹³⁴ *Ibid* paras 46-49.

voidable part of the public environment in an occupied territory, the jurisprudence on public spaces outlined in the section above would also become relevant.

4.3.3 Internment and detention

In the 2008 case of *S. and Marper v. the United Kingdom*, the two applicants had been suspects detained in criminal investigations and had their fingerprints and DNA samples collected as a result. Though neither were later convicted, the United Kingdom police retained their fingerprints, cellular samples and DNA profiles in a national database where they would be kept permanently and regularly processed by automated means.¹³⁵ In its judgment, the ECtHR found a violation of the right to private life and emphasised that States that pioneer new technologies in law enforcement must strike an appropriate balance between the potential benefit of using the technology against ‘important private-life interests’. Furthermore, the Court condemned the blanket, indiscriminate and open-ended retention practices, concluding that the practice ‘overstepped any acceptable margin of appreciation’ in terms of proportionality.¹³⁶ The Court came to the same conclusion in the 2020 case of *Gaughran v. the United Kingdom*, finding that the indefinite retention of fingerprints, photographs and DNA samples of an applicant convicted of a minor criminal offence constituted disproportionate interference with the right to respect for private life.¹³⁷

In the case of *Ukraine and the Netherlands v. Russia*, the Court discussed the administrative practices of the Russian occupying forces at so-called ‘filtration sites’ established on occupied territory in Ukraine.¹³⁸ The Court particularly noted that the screening procedures associated with the ‘filtration’ regime, which included the collection of biometric data, had not been limited

¹³⁵ *S. and Marper v. the United Kingdom* Apps nos 30562/04 and 30566/04 (ECtHR 4 December 2008) para 86.

¹³⁶ *Ibid* paras 86, 120, 125.

¹³⁷ *Gaughran v. the United Kingdom* App no 45245/15 (ECtHR 13 February 2020) paras 96-97.

¹³⁸ Further discussed in Chapter 6 below.

to combatants but also used on civilians, including children. Citing their invasive and indiscriminate nature, and the lack of legal predictability and adequate safeguarding, the Court found them in violation of the right to respect for private life.¹³⁹

4.4 Devising a test for the use of biometric surveillance

It has been made clear that individuals belonging to an occupied population retain their right to respect for privacy, whether through international human rights law, the application of the ECHR or through some other regional or international treaty. There is consequently a corresponding obligation to respect the right placed on Occupying Powers, to be applied concurrently with the rules under IHL. However, as mentioned in Section 4.2 above, both the ICCPR and ECHR provide that the right is limited to unlawful and arbitrary biometric surveillance. An invocation of a state of emergency (such as in times of war) would additionally permit an Occupying Power to place further limitations on the right to privacy of the occupied through derogation.¹⁴⁰ However, the state of emergency exception cannot be invoked as a ‘blanket rule’, nor can it be invoked in situations of prolonged occupation. It requires a clear and immediate threat to ‘the life of a nation’. In most instances of occupation, the right to privacy will therefore apply alongside IHL.¹⁴¹

In its jurisprudence, neither the HRC, the ECtHR or other human rights courts provide precise and definitive answers on what the permissible interferences with privacy are. This determination is instead done on a case-by-case basis. However, case law has set a consistent standard through principles, establishing that interferences with privacy must be (1) lawful and non-arbitrary, (2) in pursuit of legitimate aims, (3) necessary and (4) proportional.¹⁴² These four

¹³⁹ *Ukraine and the Netherlands v. Russia* Apps nos 8019/16, 43800/14, 28525/20 and 11055/22 (ECtHR [GC], 9 July 2024) section (5)(c)(vi).

¹⁴⁰ ICCPR art 4(1); ECHR art 15.

¹⁴¹ Koutroulis (2012) p. 201, 204.

¹⁴² UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* UN Doc HRI/GEN/1/Rev.1 (8 April 1988) paras 3-4; Talbot (2020) p. 840.

requirements are used below to construct a four-step ‘test’ for assessing the legality of biometric surveillance measures under IHRL.

4.4.1 Requirement (1): Legality

First, as outlined in Sections 4.2 and 4.3, any interference with the privacy of an occupied subject must fulfil the requirement of legality. This means the interference must be both *lawful* and *non-arbitrary*. To be lawful, the interference must be done on the basis of law, and the law must itself be compliant with the ‘provisions, aims and objectives’ of IHRL.¹⁴³ If legislative measures instituted by an Occupying Power permit interferences with privacy, the legal provisions must be ‘sufficiently accessible, clear and precise’ so that an occupied subject can look at the law and ascertain who is authorised to conduct the surveillance and under what circumstances.¹⁴⁴ Lawfulness does not require that the Occupying Power inform the individual subject that their biometric privacy has been infringed upon, but the legal provisions must be sufficiently clear that the subject can ‘foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.’¹⁴⁵ The individual must be able to foresee what conduct will result in interferences with their biometric privacy, and there must exist a possibility for the individual to adjust their behaviour to avoid this interference.¹⁴⁶

To be non-arbitrary, the legal provisions must also outline the ‘nature, scope and duration’ of the surveillance measures, ‘the grounds required’ to conduct such surveillance, what authority will ‘authorize, carry out and supervise’ the surveillance and ‘the kind of remedy provided’ to those affected.¹⁴⁷

¹⁴³ UN Human Rights Committee *General Comment No. 16* (1988) para 3.

¹⁴⁴ HRC *Right to Privacy in the Digital Age* Report (2021) para 23.

¹⁴⁵ *The Sunday Times v. the United Kingdom* App no 6538/74 (ECtHR, 26 April 1979) para 49.

¹⁴⁶ Véliz, Carissa, *The Ethics of Privacy and Surveillance* (Oxford University Press 2024) p. 143.

¹⁴⁷ UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue* UN Doc A/HRC/23/40 (17 April 2013) para 81.

4.4.2 Requirement (2): Legitimate purpose

Any interference with the right to privacy of an occupied subject must be done in the pursuit of a legitimate purpose. Guidance on what constitutes a legitimate purpose can be found in the limitation clauses of other rights under the ICCPR, and in Article 8(2) of the ECHR. Together they provide that the protection of national security, public order, public safety and the prevention of crime can constitute legitimate reasons for States' interference with privacy.¹⁴⁸ Given the duty of Occupying Powers under IHL to guarantee public order and civil life, these same reasons can likely be invoked by them to legitimise biometric surveillance, including the use of FRTs.¹⁴⁹

In an occupation context, the broad scope of legitimate purpose is not without its problems. It can easily be abused by Occupying Powers through invoking 'amorphous' concepts of national security to justify all-encompassing and invasive surveillance measures against the occupied, with the support of GCIV Article 27(4). However, use of biometric surveillance measures that does not correspond to an *authentic* threat to security would not fulfil the requirement of legitimate purpose.¹⁵⁰

4.4.3 Requirement (3): Necessity

The biometric measures deployed by the Occupying Power must not exceed what is necessary to achieve the legitimate purpose.¹⁵¹ Under IHRL, the requirement of necessity is tied to what limitations of privacy can be constituted as necessary 'in a democratic society'.¹⁵² This requirement of necessity is considerably stricter than the requirement provided under Article 27(4) of the GCIV. The latter requires only that the surveillance measures are 'necessary

¹⁴⁸ UN Human Rights Committee, *CCPR General Comment No. 27: Article 12 (Freedom of Movement)* (2 November 1999) CCPR/C/21/Rev.1/Add.9 para. 11. Note that the listed example of legitimate aims is not exhaustive. The ECHR also lists reasons such as the economic wellbeing of the country.

¹⁴⁹ Talbot (2020) p. 842.

¹⁵⁰ *Ibid.*

¹⁵¹ *The Wall AO* paras 136-137.

¹⁵² UN Human Rights Committee *CCPR General Comment No. 27* para. 11; ECHR art 8(2); Talbot (2020) p. 842-843.

as a result of the war'. Given the unique setting of occupation, where democracy will (at least temporarily) be superseded by the military rule of the Occupying Power, the requirement of necessity must here be interpreted using the more contextually relevant body of law that is IHL. A complementary reading of IHL provides that biometric surveillance measures must either be necessary for restoring and ensuring the civil life, interests and rights of the occupied population,¹⁵³ or for securing military interests, such as protecting the 'forces and materiel' of the Occupying Power from threats in the occupied territory.¹⁵⁴ Biometric surveillance measures that are deployed in response to threats from the occupied must be limited to what is necessary for the specific legitimate purpose. The fact that the Occupying Power may safeguard its own interests does not provide blanket permission to institute unnecessary surveillance measures.¹⁵⁵

4.4.4 Requirement (4): Proportionality

Finally, biometric surveillance measures that infringe on the right to privacy of the occupied are subject to the requirement of proportionality under IHRL.¹⁵⁶ The requirement of proportionality provides that surveillance measures must strike a proportionate balance between the interests of the Occupying Power and the rights and interests of the occupied. Even where a measure is (1) lawful, (2) legitimate and (3) necessary, it may still violate the right to privacy if it is disproportionately intrusive in relation to its purpose.

In its General Comment No. 27, the HRC asserted that restrictions on ICCPR rights must be 'appropriate to achieve their protective function', constitute 'the least intrusive instrument amongst those which might achieve the desired result', and be 'proportionate to the interest to be protected'.¹⁵⁷ In an occupa-

¹⁵³ 1907 Hague Regulations art 43.

¹⁵⁴ Talbot (2020) p. 842-843.

¹⁵⁵ *The Wall AO* paras 136-137.

¹⁵⁶ The requirement of proportionality under IHRL will concern the effect the biometric measures have on the rights of the targeted subjects themselves. This is different from the proportionality requirement of targeting under IHL, which is concerned with the effects on those who are *not* the target.

¹⁵⁷ UN Human Rights Committee, *General Comment No. 27* para 14.

tion setting, this means that biometric surveillance measures must remain limited in scope and intensity to what is required for the specific security or public order interest pursued. Blanket or indiscriminate biometric surveillance directed broadly at the occupied population is therefore unlikely to satisfy the requirement of proportionality.¹⁵⁸

The existence of adequate safeguards also forms part of the proportionality assessment. Data security and sensitivity requirements minimise the risk of arbitrary or unauthorised processing of biometric data and thereby reduce the severity of the interference with privacy. As demonstrated in cases such as *S. and Marper v. UK* and *Ukraine and the Netherlands v. Russia*, the absence of such safeguards weighs against the legality of biometric surveillance measures under IHRL.¹⁵⁹

4.5 Reconciling IHL and IHRL

The concurrent application of IHL and IHRL in occupation settings means that biometric surveillance measures deployed by an Occupying Power cannot be evaluated solely through the lens of the laws of war. While the law of occupation grants Occupying Powers broad discretion to restore and ensure public order and civil life, and to take measures of control and security, these powers remain limited by the occupied population's right to privacy under IHRL. The collection and processing of biometric data therefore require a balancing act between the security interests of the Occupying Power and the privacy rights and freedoms of the occupied population.

This balancing becomes particularly significant in situations of prolonged occupation. As occupation increasingly resembles long-term governance rather than temporary military control, the role of IHRL correspondingly strengthens.¹⁶⁰ As noted in jurisprudence and scholarship, prolonged occupation complicates attempts to distinguish sharply between the application of IHL and

¹⁵⁸ *S. and Marper v. the United Kingdom* paras 103, 119-125; *Ukraine and the Netherlands v. Russia* section (5)(c)(vi).

¹⁵⁹ Basri, Nahide, 'Regulating surveillance during occupation through core data protection principles' (2026) *The International Journal of Human Rights*, 1–31 p. 7.

¹⁶⁰ Sassóli (2005) p. 663-665; McCarthy (2008) p. 122-124.

IHRL, as long-term administration of a territory inevitably creates the expectation that human rights norms associated with peaceful governance will apply. In this context, supervisory mechanisms and judicial guarantees under IHRL may increasingly supersede the more permissive framework of IHL where necessary, in order to safeguard the fundamental rights of the occupied population. Although the Occupying Power may continue to invoke military exigency and security concerns under IHL, and active hostilities may ‘re-activate’ considerations of legitimate purpose and necessity,¹⁶¹ prolonged occupation cannot justify open-ended or indiscriminate systems of biometric surveillance directed broadly at the civilian population. The requirement to ensure civil life under Article 43 of the 1907 Hague Regulations must also be understood to include the guarantee of relevant human rights.

Biometric surveillance is therefore not prohibited *per se* under either IHL or IHRL. Occupying Powers may lawfully employ biometric technologies for legitimate security and administrative purposes, including at checkpoints, in public spaces and in places of detention. However, the legality of such measures depends on whether they comply with the four-step test of legality, legitimate purpose, necessity and proportionality. In practice, the more indiscriminate and technologically intrusive the surveillance becomes, the more difficult it is to reconcile with the right to privacy as it is afforded to occupied populations.

¹⁶¹ Koutroulis (2012) p. 194, 197-198 and notes 160-161, 182.

5 DATA PROTECTION PRINCIPLES IN OCCUPATION SETTINGS

When examining the use of biometric surveillance against civilians under occupation, a pressing question is to what extent data protection law applies to the conduct of Occupying Powers. In its 2025 Commentary to the Fourth Geneva Convention, the ICRC asserts that any collection and processing of biometric data of occupied populations must adhere to applicable data protection standards. When discussing specifically the holding of internees, the Commentary further states that biometric data extracted from the interned must be used and managed in accordance with applicable data protection requirements.¹⁶²

International humanitarian law itself offers little guidance on emerging surveillance technologies and data protection, and on the international level data protection law remains fragmented and relatively weak.¹⁶³ When it comes to protecting the data of occupied civilians, human rights law and regional data protection regimes have evolved more rapidly and are more adequately posed to address these challenges.¹⁶⁴ A challenge that presents itself specifically in the context of occupation is that occupied territories may not necessarily have data protection regulation in place prior to occupation, and an Occupying Power may not always have extraterritorial obligations that have been established through binding regional or international treaties. Through evaluating regional human rights instruments and the vast jurisprudence of human rights treaty bodies and regional courts, it nonetheless becomes possible to glean the emerging core principles of data protection that may have broader application beyond the regulatory instruments they are currently realised through. In light of the ICRC's assertions that the processing of biometric data of the occupied requires at least some degree of adherence to data protection principles, this chapter therefore examines what principles may govern biometric surveillance during occupation by examining Council of Europe (CoE) and EU data

¹⁶² 2025 ICRC Commentary paras 2224, 5054.

¹⁶³ Shehabi (2024) p. 101 and note 77, 80. See also Lubin (2022) p. 472.

¹⁶⁴ Lubin (2022) p. 466.

protection law. The chapter also discusses what implications the emerging data protection principles have for the conduct of Occupying Powers.

5.1 Current state of law

It is easy to conceive of data privacy and data protection as modern conceptions, born from the emergence of today's highly advanced communications- and information-gathering technology, such as the various biometrics that are the subject of this thesis. But data protection and data privacy began to be a subject of international discussion as early as the 1960's, with the 'first generation' of legal instruments and domestic legislation dating back to the 1970's.¹⁶⁵ Among those legal instruments were the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (No. 108), the predecessor of today's Convention 108+.

Data protection is generally understood as a facet of the right to privacy, protecting the right of individuals to determine 'when, how and to what extent information about them is communicated to others'.¹⁶⁶ In General Comment No. 16, the HRC asserts that the right to privacy entails that any gathering of personal data in databases or by other digital means conducted by public authorities must be regulated by law, and never used for purposes 'incompatible with the Covenant'.¹⁶⁷ However, Asaf Lubin also identifies a growing trend of data protection emerging as a standalone right, referring to its separate protection under Article 8 of the Charter of Fundamental Rights of the European Union (CFR) and its separate constitutional protection in many domestic legal systems.¹⁶⁸

¹⁶⁵ *Ibid* p. 472 and note 59.

¹⁶⁶ *Ibid* p. 472 and note 64.

¹⁶⁷ UN Human Rights Committee *General Comment No. 16* (1988) para 10.

¹⁶⁸ Lubin (2022) p. 471–473.

At present, the rapid development of intrusive technologies capable of collecting, storing and processing categories of sensitive data, such as biometrics, has sparked new regulatory initiatives in response.¹⁶⁹ The following sections of this chapter will outline key regulations on biometrics and discuss their implications for the obligations of Occupying Powers.

5.2 Council of Europe

In addition to the ECHR, the Council of Europe has also drafted a treaty and issued commentary specifically on the subject of data protection. While the CoE's data protection regulation is only binding for States who have acceded to the treaty, the treaty contains an authoritative definition of biometrics frequently referenced by legal scholars and courts. Additionally, other regional and national legislations often mirror its provisions, indicating that it reflects a common understanding of data protection standards.¹⁷⁰

5.2.1 Convention 108+

The Council of Europe's Convention 108, originally drafted in 1981, is the only legally binding international treaty that regulates the automated processing of personal data.¹⁷¹ The Convention regards protection of personal data as a facet of the right to privacy, and as necessary for the safeguarding of human dignity.¹⁷² Its amended version (Convention 108+) aims at responding to the emergence of new technologies capable of 'algorithmic deduction, control or surveillance'.¹⁷³ A key feature of Convention 108+ is that it applies to all actors that engage in data processing, including law enforcement authorities, military forces and intelligence services. In its amended version, the Con-

¹⁶⁹ Argren, Rigmor, 'What Militaries Need to Know about Data Protection and the Right to Digital Privacy/Private Life' (2025) 107(928) *International Review of the Red Cross* 2–18 p. 6.

¹⁷⁰ *Ibid.*

¹⁷¹ The Convention regulates data protection both for member States of the Council of Europe and for several State parties outside of Europe, such as Uruguay, Senegal, Morocco and Mexico.

¹⁷² Convention 108+ preamble and Article 1.

¹⁷³ de Terwangne, Cécile, 'Council of Europe convention 108+: A modernised international treaty for the protection of personal data' (2021) 40 *Computer Law & Security Review* p. 1-3.

vention's scope is no longer limited to the territory of each State party. Instead, it applies to all data processing subject to the State Party's jurisdiction.¹⁷⁴ This expanded scope indicates that Convention 108+ may apply extraterritorially, at least in exceptional circumstances.¹⁷⁵

Convention 108+ provides a catalogue of core principles that must be respected in all data processing, mirroring the IHRL requirements of lawfulness, legitimate purpose, necessity and proportionality. The Convention classifies biometric data as a special category of data that may only be processed if there are safeguards protecting against risks to the interests and rights of the data subject.¹⁷⁶ In 2021, the CoE released its Guidelines on facial recognition as a complement to Convention 108+. The Guidelines assert the uniquely sensitive nature of biometric data and the risk of FRTs seriously infringing on the right to privacy.¹⁷⁷

Article 6 of Convention 108+ regulates the use of biometrics. It provides that the processing of biometric data requires that the State has 'appropriate legal safeguards' enshrined in law. Article 6(2) stipulates that the legal safeguards must specifically protect against any risk that the processing poses to the interests and rights of the individual, and against any disproportionate interference with their fundamental rights.¹⁷⁸ The requirement of appropriate legal safeguards means it is not sufficient that States' use of biometric surveillance is lawful under domestic law. Legislation that authorises 'vast surveillance of individuals' still risks violating the right to respect for private life under ECHR,¹⁷⁹ therefore potentially violating Article 6(2). The CoE Guidelines

¹⁷⁴ Compare Convention 108 (1981) art 1 and Convention 108+ (2018) art 3. See also the Explanatory Report of the Council of Europe, featured in *Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data* 15-33 paras 25-26.

¹⁷⁵ Council of Europe, *Draft Explanatory Report – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No 108) para 24 and note 9, referencing *Issa and Others v. Turkey* App no 31821/96 (ECtHR 16 November 2004) para 68.

¹⁷⁶ Convention 108+ art 6(2). See also Argren (2024) p. 69; Argren (2025) p. 7.

¹⁷⁷ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition* (Council of Europe 2021) p. 5-8.

¹⁷⁸ Convention 108+ art 6; Council of Europe *Guidelines on Facial Recognition* (2021) p. 7; de Terwangne p. 6.

¹⁷⁹ Council of Europe *Guidelines on Facial Recognition* (2021) p. 5.

further state that some uses, including intrusive use of LFRT in public and ‘quasi-public’ places should be heavily regulated, and so-called emotion recognition technology should be prohibited outright.¹⁸⁰

5.2.2 Recommendation No. (87) 15

In 1987, recognising the need to balance States’ interest in the maintenance of public order and the suppression of crime with the individual’s right to privacy,¹⁸¹ the CoE issued its Recommendation No. (87) 15 on regulating the use of personal data in the context of law enforcement. Principle 2 of the Recommendation lays down a core requirement of necessity and proportionality, intended to prevent ‘open-ended, indiscriminate collection of data’ by police.¹⁸² It states that collection of personal data for police purposes should as a rule be limited to only what ‘is necessary for the prevention of real danger’ and the suppression of ‘a specific criminal offence’. For data collected through surveillance or other automated means, such collection should be governed by specific dedicated provisions provided under national law.¹⁸³

When it comes to categories of sensitive data, that today includes biometrics,¹⁸⁴ the Recommendation takes the view that the collection and storage of such data should be restricted. It finds that while limited collection of certain sensitive data may at times be necessary, such data should ‘under no circumstances’ be collected by law enforcement simply ‘to compile a file on certain minority groups whose behaviour or conduct is within the law’.¹⁸⁵

¹⁸⁰ *Ibid* p. 8-9 and note 9.

¹⁸¹ Council of Europe Committee of Ministers, *Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector* (adopted 17 September 1987 at the 410th meeting of the Ministers’ Deputies) preamble.

¹⁸² Council of Europe Committee of Ministers, *Explanatory Memorandum to Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector* (17 September 1987) para 43.

¹⁸³ Council of Europe *Recommendation No. (87) 15* (1987) principle 2.1, 2.3.

¹⁸⁴ Council of Europe *Guidelines on Facial Recognition* (2021) p. 5.

¹⁸⁵ Council of Europe *Explanatory Memorandum* (1987) para 48.

5.3 European Union

The European Union (EU) has an extensive regime of data protection regulations, including regulations that govern the public sector of its member States. This section examines provisions on data protection in the Charter of Fundamental Rights of the European Union and the EU Directive 2016/680 on data processing in law enforcement operations.

5.3.1 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union, binding for all EU Member States, has two provisions regulating privacy and data protection respectively. Article 7 enshrines the right to respect for private life, while Article 8 separately enshrines the right to protection of personal data, including sensitive data such as biometrics. Under CFR data protection is constructed as a separate and distinct right, existing independently of the right to privacy or private life.¹⁸⁶ CFR's Article 8 is based on Convention 108, requiring that personal data is processed either on the basis of consent or another legitimate and lawful basis. Further specification on what the right to data privacy under CFR entails for biometrics requires an assessment of relevant EU regulatory instruments.¹⁸⁷

5.3.2 Law Enforcement Directive

The EU Directive 2016/680 (Law Enforcement Directive)¹⁸⁸ regulates data processing related to law enforcement operations, an area excluded from the scope of the General Data Protection Regulation (GDPR).¹⁸⁹ The directive

¹⁸⁶ Argren (2025) p. 8 and note 36.

¹⁸⁷ Kranenborg, Herke, 'Art 8 – Protection of Personal Data' in Peers, Steve, Hervey, Tamara, Kenner, Jeff and Ward, Angela (eds), *EU Charter of Fundamental Rights: A Commentary* (2nd Edition, Bloomsbury Publishing 2021) 231–290 p. 256; CFR art 8(2).

¹⁸⁸ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

¹⁸⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and

addresses data protection done by any actor who exercises public authority in the context of crime and threats to public security,¹⁹⁰ but excludes national security activities as these fall outside the ambit of EU law.¹⁹¹ It is nevertheless interesting to examine what standards are established through the Law Enforcement Directive, and their potential implications for Occupying Powers. As previously mentioned, the Occupying Power's administration of territory during prolonged occupation may closely resemble domestic law enforcement operations.

In line with CFR, the directive views data protection as a fundamental right and sets a minimum standard for how this right should be safeguarded by EU member States.¹⁹² The processing of biometric data is regulated in Article 10 of the directive, containing similar heightened protections as those of Convention 108+. Article 10 of the Law Enforcement Directive stipulates that biometric data may only be processed when it is strictly necessary and subject to appropriate safeguards guaranteeing the rights of the individual. Furthermore, the processing of biometric data must also either be authorised by law, intended to protect the vital interest of affected individuals or other natural persons, or relate to data 'manifestly made public' by individuals themselves.¹⁹³

The directive specifically identifies both biometric data and the processing of 'large amount[s] of personal data' affecting 'a large number of data subjects' as two forms of processing that constitute a particular risk to the right to protection of personal data guaranteed under Article 8 CFR.¹⁹⁴ The Guidelines on the use of FRT by law enforcement issued by the European Data Protection Board emphasise that any derogations from, or limitations of, the rights to privacy and data protection are only applicable 'when strictly necessary'. The necessity requirement means that when less intrusive means are available,

on the Free Movement of Such Data, and repealing Directive 95/46/EC [2016] OJ L119/1 art 2(2)d.

¹⁹⁰ Law Enforcement Directive preamble paras 11-12, art 1.

¹⁹¹ *Ibid* preamble para 14.

¹⁹² *Ibid* preamble paras 1, 15.

¹⁹³ *Ibid* art 10.

¹⁹⁴ *Ibid* preamble para 51.

they should be given priority over FRTs. Discussing the question of proportionality, the Guidelines emphasise that a ‘general interest of effectiveness in fighting serious crimes cannot in itself justify’ the processing of vast amounts of data that have been collected indiscriminately.¹⁹⁵

5.4 Data protection principles during occupation

While the international law of occupation lacks explicit provisions regulating data protection, the 2025 ICRC Commentary suggests that there are still a number of data protection principles that govern the conduct of Occupying Powers. In this respect, the Martens Clause originating with the 1899 Hague Regulations provides that the ‘legal silence’ of IHL in the face of rapid social and technological development should not be viewed as ‘inherently permissive’.¹⁹⁶ Through identifying the common threads that run through existing regulations on the collection and processing of biometric data, it becomes possible to identify a number of principles that may constitute ‘emerging norms’ of data protection for Occupying Powers.¹⁹⁷ There are firstly the general requirements, principles which are applied to all data processing: lawfulness,¹⁹⁸ legitimate purpose, necessity, proportionality, transparency and data minimisation.¹⁹⁹ In the context of biometric surveillance, the regulations examined in this chapter converge into two distinct norms. Firstly, the collection and processing of biometric data is associated with a specific lawfulness requirement, indicating that the use of biometrics must be authorised by specific provisions in law.²⁰⁰ Secondly, the law must contain safeguards dedicated to ensuring the fundamental rights of the individual data subject.²⁰¹

¹⁹⁵ European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement* (European Union 26 April 2023) p. 17, 51–52; Argren (2024) p. 70.

¹⁹⁶ Lubin & Shehabi (2026) p. 115.

¹⁹⁷ Lubin (2022) p. 473–474.

¹⁹⁸ This includes consent.

¹⁹⁹ See, for example, Convention 108+ arts 5, 7–10; Law Enforcement Directive arts 4, 20. See also Lubin (2022) p. 473–474 for further discussion on emerging norms.

²⁰⁰ Council of Europe *Recommendation No. (87) 15* principle 2.3; Law Enforcement Directive art 10(a).

²⁰¹ Convention 108+ art 6(2); Law Enforcement Directive art 10; CFR art 8(1).

6 CASE STUDIES: PRIVACY AND PROLONGED OCCUPATION IN UKRAINE AND PALESTINE

This chapter consists of two case studies of biometric surveillance and the right to privacy during prolonged occupation. The case studies will examine the biometric surveillance measures deployed by Russia in territories of Ukraine and Israel in the West Bank of Palestine and conduct an analysis of their legality under international law. The measures instituted by the Occupying Powers will be evaluated using the concurrent application of relevant provisions of IHL, the four-step ‘test’ on interferences with privacy under IHRL and the emerging data protection principles outlined in the previous chapter.

Both the occupation of Ukraine and the occupation of Palestine fall outside the ambit of some binding protections. While the ECtHR has found that the ECHR could be applied to conduct by the Russian military in the occupied territories of Ukraine up until September of 2022,²⁰² neither the ECHR nor other regional human rights conventions have direct applicability on the occupied territories of Palestine. Neither Russia nor Israel have ratified the amended Convention 108+ or other data protection regulations with extraterritorial application. However, the purpose of this case study is simply to test the protections accorded by the concurrent application of these bodies of law against existing prolonged occupations.

It is additionally worth noting that the ICJ has repeatedly asserted that the protections offered by international human rights conventions continue to apply to occupied populations,²⁰³ just as the 2025 ICRC Commentary asserts that Occupying Powers must abide by applicable data protection standards.²⁰⁴ Yet, as Koutroulis observes, in practice the Occupying Powers may when convenient neglect to implement legislative measures that benefit occupied

²⁰² *Ukraine and the Netherlands v. Russia* paras 328, 361. Note that Russia ceased to be a party to the ECHR on 16 September 2022.

²⁰³ *The Wall AO* paras 106, 107, 111-113; *Policies and Practices AO* paras 216, 224-225.

²⁰⁴ 2025 ICRC Commentary paras 2224, 5523.

populations.²⁰⁵ In prolonged occupation, this renders occupied populations unable to keep pace with developments in human rights and data protection law as a way of solidifying their right to privacy. As the occupied populations cannot themselves modernise the ‘local laws’ that Occupying Powers are bound to protect under Article 43 of the 1907 Hague Regulations, they are left without binding protections.

6.1 Ukraine

In February of 2014, Russia invaded and began its military occupation of the Ukrainian peninsula of Crimea.²⁰⁶ In March of 2014, annexation was formalised through an addition in the Russian constitution, listing Crimea as Russian territory.²⁰⁷ On February 24, 2022, in a further escalation of the conflict, Russia launched a full-scale military invasion of mainland Ukraine. In addition to Crimea, the regions of Donetsk, Luhansk, Zaporizhzhia and Kherson are as of 2026 under Russian military occupation.²⁰⁸ While Russia has continuously refused to formally acknowledge its status as Occupying Power over the territories,²⁰⁹ this is of little relevance to the legal status of the territory. The existence of occupation is determined through factual criteria, not formal recognition by the Occupant.

After the capture of territories in mainland Ukraine in 2022, Russian armed forces began subjecting Ukrainian civilians to so-called ‘filtration’. ‘Filtration’ is a compulsory screening process involving invasive body searches, interrogations and the forcible collection of biometric data,²¹⁰ including fingerprints and front and side facial images.²¹¹ Civilians who ‘fail’ the filtration process report being forcibly transferred to detention facilities either in Russia

²⁰⁵ Koutroulis (2012) p. 172-174.

²⁰⁶ Anischchuk, Alexei, ‘Putin Admits Russian Forces Were Deployed to Crimea’ *Reuters* (17 April 2014).

²⁰⁷ Tsvetkova, Maria and Gutterman, Steve, ‘Russia's lower house votes to bring Crimea into Russia’ *Reuters* (20 March 2014).

²⁰⁸ BBC Visual Journalism Team, ‘Ukraine in Maps: Tracking the War with Russia’ *BBC News* (24 February 2026).

²⁰⁹ *Ukraine and the Netherlands v. Russia* para 220.

²¹⁰ UN Office of the High Commissioner for Human Rights (OHCHR), *The Situation of Human Rights in Ukraine in the Context of the Armed Attack by the Russian Federation, 24 February to 15 May 2022* (29 June 2022) p. 2, 19-21.

²¹¹ HRW *We Had No Choice* Report (2022).

or Russian-occupied areas of Ukraine, as did some who were ‘cleared’ by the screening.²¹² The following subsections will discuss ‘filtration’ as a biometric surveillance measure instituted by Russian armed forces against occupied subjects.

6.1.1 Checkpoints

Reports from September 2022 describe Ukrainian civilians being subjected to ‘filtration’ at military checkpoints established by Russia.²¹³ According to Human Rights Watch (HRW), thousands of Ukrainian civilians fleeing hostilities were stopped and detained at checkpoints and forced to undergo compulsory security screenings. The screening process involved body searches, the search of personal belongings, and interrogations that appear to be intended to ascertain their political views and affiliations with Ukrainian soldiers or civil authorities. HRW describes the screening process as typically involving the collection of the civilians’ biometric data, including ‘fingerprints and front and side facial images’. Nearly all civilians, including children, were indiscriminately subjected to the screening process. Many civilians reported being stopped and made to undergo new security screenings at multiple checkpoints. Civilians who ‘failed’ the filtration process, or some who were unable to arrange their own transport to Ukraine-controlled areas, report being subsequently transferred to either Russia or Russian-occupied areas of Ukraine. Those who were transferred across the border into Russia report undergoing yet another ‘filtration’ process at military checkpoints located along the Russian border.²¹⁴

6.1.2 Internment and detention

According to two independent reports,²¹⁵ the ‘filtration’ regime instituted by Russian armed forces also involved the internment of Ukrainian civilians, both while awaiting the security screening and in some instances also after

²¹² *Ibid.*

²¹³ OHCHR *The Situation of Human Rights in Ukraine* Report (2022) p. 2, 19-21.

²¹⁴ HRW *We Had No Choice* Report (2022).

²¹⁵ *Ibid.*; OHCHR *The Situation of Human Rights in Ukraine* Report (2022).

having completed it. It is reported that in addition to screening fleeing civilians at checkpoints, Russian armed forces also rounded up Ukrainian civilians for screening by removing them from their homes or shelters and transporting them to ‘filtration centres’. There, they were kept in crowded facilities while waiting for their turn to undergo screening, with the waiting period ranging from a few hours to several days or weeks.²¹⁶ In other instances, Ukrainian civilians volunteered for security screenings at the filtration centres with the understanding that the screening process was required in order to be allowed to leave areas with active hostilities or travel on roads controlled by Russian forces.²¹⁷

Similar to the screening process described by civilians stopped at military checkpoints, the security screening at filtration camps is reported to involve interrogations, the search of their electronics and the collection of biometric data. Civilians interviewed by HRW described Russian forces collecting fingerprints, palm prints and facial images, and additionally state that they were not asked for consent before their biometric data was collected, and that they were not told what purpose it had been collected for.²¹⁸

6.1.3 Public spaces

Ukrainian civilians have described having their biometric data collected during ‘filtration’ screenings and subsequently being transferred to resettle either in Russian-occupied areas of Ukraine or Russia.²¹⁹ While this research has found little publicly available information about the Russian authorities’ use of biometric surveillance in the Russian-occupied areas of Ukraine,²²⁰ the use of LFRT-enabled CCTV surveillance to monitor public spaces in Russia is well-documented.²²¹ It is plausible that Ukrainian civilians that have had their

²¹⁶ HRW *We Had No Choice* Report (2022).

²¹⁷ *Ibid.*

²¹⁸ *Ibid.*

²¹⁹ *Ibid.*

²²⁰ A 2022 proposal suggests Russia intends to deploy FRT-enabled surveillance in Crimea, see Gofman, Mikhail I and Villa, Maria, ‘Identity and War: The Role of Biometrics in the Russia-Ukraine Crisis’ (2023) 5(1) *International Journal on Engineering, Science and Technology* 89–111 p. 98.

²²¹ *Gluhkin v. Russia* para 33; Amnesty International, ‘Russia: Intrusive facial recognition technology must not be used to crackdown on protests’ (31 January 2020); Human Rights

biometric information collected prior to being relocated to Russia risk being subjected to tracking and surveillance in public spaces, enabled by Russia's pre-existing extensive system of biometric video surveillance.²²²

6.1.4 Analysis

According to HRW, the 'filtration' regime has enabled Russian authorities to collect vast amounts of biometric data belonging to Ukrainian civilians. While there are no conclusive numbers on how many Ukrainians have undergone 'filtration', testimonies given to HRW suggest that filtration sites may have processed the biometric information of somewhere between several hundreds and tens of thousands of Ukrainians.²²³ It goes without saying that the biometric surveillance practices employed by the Russian military in connection with its 'filtration' regime engage the concurrent application of all three bodies of law that are the subject of this thesis: IHL, IHRL and data protection principles relevant for occupation.

Looking first to the Russian army's collection of biometric data at checkpoints within the occupied territory, IHL permits the general use of checkpoints and identity controls to limit the movements of an occupied population and to identify enemy combatants, even in areas where there are little or no active hostilities. While the collection and processing of biometric data at checkpoints is not categorically prohibited under IHL, as a measure of control and security it must serve either a legitimate civilian or military interest. It must also be proportionately balanced to the infringement of rights it results in for the occupied. Given reports that the interrogations of Ukrainian civilians centred around their personal affiliations to Ukrainian armed forces or their political opposition to the Russian invasion, it would appear that the 'filtration' screenings were implemented at least partially to safeguard the military interests of Russia as an Occupying Power over Ukraine. However, even

Watch, 'Russia Expands Facial Recognition Despite Privacy Concerns: Lack of Accountability, Oversight, Data Protection' (2 October 2020); Human Rights Watch, 'Russia: Broad Facial Recognition Use Undermines Rights' (15 September 2021).

²²² Gofman & Villa (2023) p. 97-98.

²²³ HRW *We Had No Choice* Report (2022).

without engaging IHRL and data protection standards, the categorically indiscriminate, invasive, excessive and repetitive nature of the biometric data collection would render it disproportionate to *any* military aim, let alone a legitimate one. The ICRC's assertion in its 2025 Commentary that practices involving biometric data collection pose heightened risks to the rights of the occupied under GCIV 27(1) only serves to reinforce this conclusion.

Looking next to the biometric data collection of Ukrainian civilians held in places of internment, the practice raises similar concerns under IHL. While the general framework of operation for Occupying Powers under IHL can permit placing civilians in internment, it constitutes an exceptionally harsh measure permitted only when lesser means cannot suffice. The collection and processing of biometric data of the interned similarly requires a heightened degree of justification, especially as it exposes the individual to future risks of identification and tracking through biometric surveillance systems. Russia is bound by its obligation under GCIV 27(1) to always treat the occupied humanely, including during internment. Consequently, the holding of Ukrainian civilians in filtration centres for the specific purpose of facilitating the mass collection of their biometric data²²⁴ finds no support under IHL. As made evident by the Court's findings in *Ukraine and the Netherlands v. Russia*, the 'filtration' measures also lack both the foreseeability and the adequate safeguards against arbitrariness and abuse required to fulfil the (1) legality requirement under IHRL. The indiscriminate, mass application of the measure also fails to strike a (4) proportionate balance against the right to private life of Ukrainians under occupation. The failure to fulfil the legality requirement is relevant also for the question of data protection. According to the testimony of Ukrainian civilians, the data collection was not preceded by any request for consent, nor any transparency regarding its future use. This would render it non-compliant with general data protection principles. On the specific subject of biometric surveillance, data protection regulations also increasingly converge to form two further requirements. They provide that Russia's data

²²⁴ As well as other forms of personal data.

collection must not only be authorised under law; the law must also contain safeguards for the right to privacy of the Ukrainian population.

Looking finally at the deployment of biometric surveillance technologies to monitor Ukrainians *en masse* in public spaces in either Russian-occupied Ukraine or Russia, the research cannot conclusively determine if any such practices currently exist. The analysis will therefore evaluate this only as a theoretical possibility. An assessment under the rules of IHL requires accounting for the importance of the public spaces of occupied Ukraine to the continued civil life of Ukrainians under occupation, and the damage that mass biometric surveillance may cause to the civil life of communities over time. The forced resettlement of Ukrainians to Russia, constituting itself a separate violation under IHL, does not remove from them the protections they are accorded under GCIV Article 27(1). In both scenarios, the concurrent application of IHL and IHRL is required to account fully for their privacy rights under law. While IHL provides little guidance on surveillance of public spaces, IHRL has vast jurisprudence of the same. Especially relevant is the *Glukhin v. Russia* case, which provides that the tracking of persons through LFRT-enabled CCTV surveillance, a technology widely deployed in public spaces in Russia, constitutes a particularly intrusive interference with privacy. As such, it should only be used in exceptional circumstances. The case of *Big Brother Watch and Others v. UK* is also relevant, as it provides that the interference with privacy would be of increased severity if the biometric data of Ukrainians was not only collected at ‘filtration’, but also subsequently processed through the use of surveillance FRTs.

Drawing on this jurisprudence, the use of collected biometric data to implement surveillance measures against occupied or forcibly displaced Ukrainians would (similar to the general practice of ‘filtration’) not fulfill the requirement of (1) legality, as it lacks legal foreseeability for the affected persons; (2) legitimate purpose, which cannot be all-encompassing, ‘amorphous’ security concerns; (3) necessity, given that the invasive nature of such a measure would require the highest degree of justification, and (4) proportionality as it fails both to account for the interests of Ukrainians and provide them the

adequate safeguards necessary under IHRL and emerging data protection norms.

6.2 Palestine

Since June 7, 1967, the West Bank and Gaza Strip have been under Israeli military occupation.²²⁵ For Palestinian civilians residing in the West Bank, the ensuing six decades of occupation have resulted in the fragmentation of the territory through illegal settlements, the disruption of daily life through an unpredictable regime of checkpoints and restrictions on movement, and extensive infringements of their privacy.²²⁶ While Israel has continuously objected to the application of international human rights in the occupied territories, the ICJ has established twice over that the provisions of IHRL apply to Palestinians, alongside the rules of IHL.²²⁷ Israel monitors the West Bank using ‘an ecosystem of surveillance’ that includes biometric checkpoints, LFRT-enabled CCTV networks and vast databases storing biometric information collected from occupied persons.²²⁸ The precise nature of Israel’s various biometric surveillance systems in the West Bank, and how they interact with each other, remains opaque. The evaluation will focus almost exclusively on the surveillance regimen Israel has deployed in the West Bank city of Hebron, sometimes described as a military panopticon,²²⁹ other times as one of the most heavily surveilled cities in the world.²³⁰

6.2.1 Public spaces

Israel has deployed LFRT-enabled CCTV surveillance technologies throughout the West Bank,²³¹ reportedly with the intention of spotting and monitoring ‘potential Palestinian assailants’. The CCTV cameras have been installed in

²²⁵ HRW *Born Without Civil Rights* Report (2019).

²²⁶ Amnesty *Automated Apartheid* Report (2023).

²²⁷ *The Wall AO* paras 106-107, 111. *Policies and Practices AO* paras 97-100. The Advisory Opinions establish the applicability of ICCPR to both the West Bank and the Gaza Strip.

²²⁸ Shehabi (2022) p. 88-89.

²²⁹ Goodfriend (2023) p. 462.

²³⁰ Dwoskin (2021).

²³¹ Shehabi (2022) p. 92; Talbot (2021) p. 830; Dwoskin (2021).

cities and on roads and intersections, and in some places the surveillance covers up to 95% of all public areas.²³² One biometric technology widely reported to have been integrated into the CCTV network combines facial and body recognition technology with AI capabilities, purportedly to identify ‘suspicious behaviour’. This AI-powered and LFRT-enabled surveillance network is able to track a single subject across multiple cameras, ‘extract, analyse and store face images’ of any individual who passes ‘within a camera’s view’. It can also perform ‘historic video analysis’ of an individual by matching them biometrically to previously recorded footage.²³³ Palestinians in the West Bank have described the extensive surveillance regime they are subjected to as having a chilling effect on public life, creating discomfort and uncertainty and leaving them feeling stripped of ‘the last vestiges of their privacy’.²³⁴

In addition to the use of LFRT-enabled CCTV surveillance, the biometric data of Palestinians is also collected by non-automated means. In a 2023 report, Amnesty International detailed the Israeli army’s use of an app-based surveillance system called Blue Wolf to register the facial images of ‘as many Palestinians as possible’ in the city of Hebron.²³⁵ Israeli soldiers patrolling the streets were instructed to photograph Palestinian civilians they encountered, sometimes by force, and upload the pictures to the app. In many cases, the photograph matched an existing profile in the system, which made the app flash either yellow, red or green to indicate whether the person should be detained, arrested immediately or allowed to pass.²³⁶ The app also featured a ranking system based on the number of Palestinian faces captured by each unit. Rewards would be given to the battalion with the highest ranking.²³⁷ In their report on surveillance in the West Bank, Amnesty International contends

²³² Shehabi (2022) p. 93; Talbot (2021) p. 830.

²³³ Shehabi (2022) p. 92-93.

²³⁴ Amnesty *Automated Apartheid* Report (2023) p. 47; Dwoskin (2021).

²³⁵ Amnesty *Automated Apartheid* Report (2023) p. 6, 42-43.

²³⁶ Dwoskin (2021).

²³⁷ Amnesty *Automated Apartheid* Report (2023) p. 43.

that it is likely that the app is connected to Wolf Pack,²³⁸ a vast Israeli database described as the Israeli army's 'Facebook for Palestinians' and said to contain profiles on 'virtually every Palestinian' residing in the West Bank.²³⁹

6.2.2 Checkpoints

Israel has utilised various forms of biometrics at its military checkpoints in the West Bank for more than two decades, beginning with the use of biometric work permits as early as 2005.²⁴⁰ In 2019, the Israeli authorities instituted a biometric verification system using FRT at checkpoints that controlled access from the West Bank to East Jerusalem and Israel. Palestinians wishing to cross the checkpoints were required to provide facial images and fingerprints that would be connected to electronic ID cards and stored in Israel's biometric databases.²⁴¹

In connection to the checkpoints that control movement between different neighbourhoods in the city of Hebron, the Israeli army has deployed an FRT surveillance system called Red Wolf. The system photographs the face of every Palestinian that passes its cameras and stores their biometric data. When Palestinians enter the checkpoint, they are biometrically identified through the cameras before they have even presented their ID cards.²⁴² If a person passing by the checkpoint does not already have a 'biometric entry' tied to their ID in the Red Wolf system, soldiers stationed at the checkpoint can biometrically enrol them in the Red Wolf database using the data captured by the surveillance cameras. Palestinians are not asked for consent prior to enrolment, nor are they informed that their biometric data has been collected in the database or told what the data is used for.²⁴³

6.2.3 Internment and detention

²³⁸ *Ibid* p. 45.

²³⁹ Dwoskin (2021).

²⁴⁰ Shehabi (2022) p. 90.

²⁴¹ Talbot (2021) p. 829; Estrin (2019).

²⁴² Dwoskin (2021).

²⁴³ Amnesty *Automated Apartheid* Report (2023) p. 42; Goodfriend (2023) p. 462.

Palestinians in the occupied West Bank²⁴⁴ live under Israeli military law, which includes the use of ‘administrative detention’. Israel’s administrative detention regime involves the arbitrary detention of civilians, without charge or trial, in prison facilities.²⁴⁵ Palestinians from Gaza have also been detained and interned in prison facilities, including in conditions where they are provided with virtually no privacy and kept under constant surveillance by guards.²⁴⁶ While biometric surveillance systems like Blue Wolf and Red Wolf may instruct occupying soldiers to detain civilians,²⁴⁷ the research conducted for this thesis has not established to what (if any) degree those detained and interned continue to be subjected to biometric data collection and biometric surveillance once inside detention facilities.

6.2.4 Analysis

The case study of biometric surveillance in the West Bank of Palestine reveals a vast and potentially interconnected network of surveillance with direct impacts on many aspects of public and private life. Looking first at the use of LFRT-enabled and AI-powered technologies to monitor public spaces and checkpoints, these exist at ‘the fulcrum’ between diverging IHL interests described by Talbot.²⁴⁸ While IHL alone does not offer conclusive guidance on their use, the concurrent application of IHRL and emerging data protection norms tips the scales in the favour of the occupied. Under IHRL, the deployment of LFRT-enabled surveillance in public areas of the West Bank would require that Israel instituted legislative measures in the territory that provide Palestinians with (1) legal foreseeability, so that they may alter their behaviour to avoid interferences with privacy. Such legislation must also outline on what grounds and to what extent Israel may deploy the surveillance. The legality of the LFRT-surveillance deployed at Hebron’s checkpoints falls at this

²⁴⁴ Excluding East Jerusalem, where Israel applies its own civil law.

²⁴⁵ Amnesty International, *Starved of Justice: Palestinians Detained Without Trial by Israel* (5 June 2012) p. 14-20; Gunter, Joel, ‘How Israel Jails Hundreds of Palestinians without Charge’ *BBC News* (15 December 2023).

²⁴⁶ Kingsley, Patrick and Bilal Shbair, ‘Inside the Base Where Israel Has Detained Thousands of Gazans’ *The New York Times* (6 June 2024).

²⁴⁷ Amnesty *Automated Apartheid* Report (2022); Dwoskin (2021).

²⁴⁸ See Section 3.2.1.

first requirement. Their placement in core parts of Hebron means that Palestinians must cross them in order to access education, health care, shops and workplaces; core aspects of civil life. To avoid their interference, Palestinians would have to give up the ‘ordinary transactions that constitute daily life’.²⁴⁹

Israel’s use of LFRT-surveillance must also correspond to (2) a legitimate purpose. Legitimate purposes can include, *inter alia*, the protection of national security, public order or civil life. In the context of the West Bank, however, the ICJ has found that Israel cannot impose indiscriminate control and security measures against Palestinians if the measures are meant to protect its own encroaching illegal settlements. This is because the existence of the Israeli settlements is itself contrary to international law.²⁵⁰ Their protection can therefore not constitute a legitimate purpose. Israel’s use of LFRT-enabled surveillance is also governed by the requirements of (3) necessity and (4) proportionality under IHRL. A concurrent reading of IHRL and IHL provides that even if the measures were intended to safeguard legitimate military or civil life-interests, this would still not provide Israel with a *carte blanche* to deploy mass surveillance. The surveillance measures must also strike a proportionate balance between Israel’s security interests and the privacy rights of the occupied Palestinians. The existence of appropriate safeguards forms part of the proportionality assessment under IHRL, and also part of the emerging norms on biometric data protection. The lack of consent, transparency or any other safeguards under law for the biometric data of Palestinians renders the surveillance incompatible with both the right to privacy under IHRL and biometric data protections.

Looking next at the non-automated collection of biometric data through Blue Wolf, Article 27(1) of GCIV entitles the occupied to ‘respect for their persons’ and provides for their humane treatment. That Palestinians in Hebron may at any time, simply by virtue of existing in public, be subjected to forced photographing by occupying soldiers seeking to collect their biometric data, is hardly in compliance with this provision nor with the Occupying Power’s

²⁴⁹ See Section 3.1.

²⁵⁰ *Policies and Practices AO* para 205.

obligations on data protection established in the ICRC's 2025 Commentary. Furthermore, the (1) legality requirement of IHRL requires both that the data collection is lawful and that it is not contrary to the overarching 'provisions, aims and objectives' of IHRL. Arbitrary interferences with privacy go directly against both the ICCPR Article 17 and the ECHR Article 8 protections of privacy. The use of Blue Wolf would also require (2) legitimate purpose. In this respect, the 'gamified'²⁵¹ nature of the app, constructed to incentivise soldiers to collect as much biometric data as possible, severely discounts any claims of legitimacy. Military units patrolling the public while competing in the forceful collection of biometric data from passing Palestinians functions to destabilise public order and civil life, rather than ensure them. That the app was deployed as a (3) necessary measure protecting some legitimate military interest can also be discounted. If that were the case, it would hardly necessitate indiscriminate data collection, including from children and the elderly.²⁵² An assessment of (4) proportionality similarly finds no support for Israel's Blue Wolf surveillance. Proportionality requires that surveillance measures are 'limited in scope and intensity' to only what is required for a given objective. That the Blue Wolf app contains built-in ranking features to incentivise soldiers to collect as much biometric data as possible runs contrary in every sense to considerations of proportionality.

Lastly, an analysis of the biometric surveillance measures deployed by Israel in the West Bank requires not only the application of IHL, IHRL and data protection as outlined in the previous chapters, but also an understanding of what legal consequences may result specifically from a prolonged occupation numbering six decades. Israel's duty as an Occupying Power to restore and ensure a functioning civil life for the occupied Palestinian population increases over time. Correspondingly, the caveat under Article 43 of the 1907 Hague Regulations that limits Israel's duty to only the measures within its power, shrinks.²⁵³ The wholesale stripping of Palestinians of their right to privacy, and the legislative stagnation in Palestinian territories that results

²⁵¹ Amnesty *Automated Apartheid* Report (2023) p. 6.

²⁵² Dwoskin (2021).

²⁵³ See Section 3.1. See also HRW *Born Without Civil Rights* Report (2019).

from Israel's reluctance to implement protective legislation safeguarding the rights of Palestinians in the face of ever-evolving biometric privacy risks, cannot be justified with reference to either protection of civil life, military need or national security.

6.3 Towards a panoptic military future?

The two case studies illustrate the ways that biometric surveillance has become an entrenched and central feature of contemporary occupation. In both the occupied territories of Palestine and those of Ukraine, surveillance practices extend far beyond proportion to facilitate the continuous monitoring, identification and control of civilian populations. Through the integration of facial recognition technology, biometric databases, satellite imagery, data scraping and real-time monitoring systems, Occupying Powers are now capable of exercising pervasive forms of control over occupied populations even as they reduce their physical presence on the ground. The development of these technologies therefore raises broader questions about the future of occupation and the extent to which existing legal frameworks are capable of regulating technologically enabled forms of domination and control.

The codified provisions of the law of occupation provide Occupying Powers with the discretion to implement increasingly intrusive measures of control and security in occupied territory, without adequately safeguarding the right to privacy or protecting against the collection and processing of biometric information. In this sense, they demonstrate the vastly different technological context from which they emerged. When applied in isolation, the law of occupation risks providing insufficient safeguards against arbitrary or disproportionate interference with the privacy of the occupied. As surveillance technology continues to push occupation towards the filtration regimes of Russia, or the military panopticon of Hebron, the right to privacy becomes increasingly essential for the occupied's enjoyment of all other rights.

7 Concluding remarks

This thesis has examined what limitations international humanitarian law, international human rights law and data protection law place on the use of biometric surveillance technologies by Occupying Powers against occupied populations. Through analysing the law of occupation, the right to privacy under international human rights law and emerging principles of data protection law, the thesis has sought to identify what legal protections exist for the biometric privacy of occupied persons in the age of increasingly pervasive and sophisticated military surveillance.

Beginning with the historical emergence of international codifications on the law of occupation, various representations of the private sphere of persons have enjoyed protection from Occupying Powers. These protections have never been absolute, however, making possible ever-increasing degrees of interference with privacy in the modern history of armed conflict. The historical development of occupation and surveillance demonstrates that systems of monitoring, identification and movement control have consistently formed part of military occupation, evolving from pass systems and population registries into the technologically advanced biometric surveillance systems deployed today. At the same time, surveillance technology has developed considerably faster than occupation law itself. As a result, while IHL continues to place humanitarian limitations on the conduct of Occupying Powers, it provides only limited guidance on the permissible scope of modern biometric surveillance practices directed at occupied populations.

International humanitarian law permits Occupying Powers to deploy biometric surveillance technologies in occupied territory for purposes connected to security, public order and civil life. Article 43 of the 1907 Hague Regulations and Article 27(4) of GCIV may therefore justify the use of biometric surveillance in the three core areas examined in this thesis: public spaces, military checkpoints and places of internment or detention. At the same time, the discretion afforded to Occupying Powers under IHL is not unlimited.

Measures of biometric surveillance remain subject to humanitarian protections under the Hague Regulations and GCIV, including humane treatment, proportionality and respect for the person, honour and dignity of occupied persons. The commentary of the ICRC, read alongside the jurisprudence of the ICJ, further demonstrates increasing recognition of the risks posed by pervasive biometric surveillance and automated data processing to the dignity and private sphere of occupied populations.

The concurrent application of IHRL alongside IHL further demonstrates that occupied populations retain the right to privacy during occupation. The protections of Article 17 of the ICCPR and Article 8 of the ECHR both extend to the collection, retention and processing of biometric data, including in public spaces. The jurisprudence of the ECtHR demonstrates that biometric identification systems, facial recognition technologies and the storage of biometric data constitute interferences with the protected private sphere of individuals. Such interferences must satisfy the four-step test of (1) legality, (2) legitimate purpose, (3) necessity and (4) proportionality. While security, public order and military necessity may justify certain surveillance measures during occupation, broad, indiscriminate or permanent forms of biometric surveillance risk violating the right to privacy, particularly in situations of prolonged occupation where surveillance becomes integrated into the ordinary administration and governance of civilian life.

An analysis of data protection law demonstrates an increasing convergence of principles governing biometric data under Council of Europe and European Union law. Biometric data is increasingly recognised as particularly sensitive personal data requiring heightened protection and safeguards against abuse. Principles such as legality, purpose limitation, proportionality and data minimisation therefore function as important complements to both IHL and IHRL. In addition, the requirement of appropriate safeguards, and specifically safeguards protecting the rights of the data subject, demonstrates the increasing importance of data protection law in regulating biometric surveillance practices during occupation.

The case studies of Ukraine and Palestine demonstrate the practical risks of existing legal deficiencies in situations of prolonged occupation. They illustrate how biometric surveillance has become an increasingly central feature of contemporary occupation, enabling Occupying Powers to monitor, identify and restrict civilian populations on a mass scale through facial recognition systems, biometric databases, CCTV surveillance and other forms of automated data processing. The case studies further demonstrate that prolonged occupation fundamentally alters the relationship between the Occupying Power and the occupied population. As occupations increasingly resemble long-term governance rather than temporary military control, the protection of privacy and biometric data correspondingly becomes more difficult to separate from ordinary human rights protections afforded in peacetime. Ultimately, the findings of this thesis demonstrate an emerging convergence between IHL, IHRL and data protection law on the protection of biometric privacy during occupation. While biometric surveillance is not prohibited per se under international law, increasingly pervasive, indiscriminate and technologically intrusive forms of surveillance become progressively more difficult to reconcile with the humanitarian protections afforded to occupied populations and their right to privacy.

Bibliography

i. Academic literature

Arai-Takahashi, Yutaka, *The Law of Occupation: Continuity and Change of International Humanitarian Law, and Its Interaction with International Human Rights Law* (Martinus Nijhoff Publishers 2009).

Argren, Rigmor, 'Protection of biometric private life under the European Convention on Human Rights and the law of armed conflict' (2024) 61(1) *The Military Law and the Law of War Review* 61–88.

Argren, Rigmor, 'What Militaries Need to Know about Data Protection and the Right to Digital Privacy/Private Life' (2025) 107(928) *International Review of the Red Cross* 2–18.

Basri, Nahide, 'Regulating surveillance during occupation through core data protection principles' (2026) *The International Journal of Human Rights*, 1–31.

Benvenisti, Eyal, *The International Law of Occupation* (2nd Edition, Oxford University Press 2012).

de Terwangne, Cécile, 'Council of Europe convention 108+: A modernised international treaty for the protection of personal data' (2021) 40 *Computer Law & Security Review*.

de Vattel, Emmerich, *The Law of Nations* (1758 Chitty, Joseph ed. and transl., Philadelphia 1852) Vol. 2 Book 3.

Gofman, Mikhail I and Villa, Maria, 'Identity and War: The Role of Biometrics in the Russia-Ukraine Crisis' (2023) 5(1) *International Journal on Engineering, Science and Technology* 89–111.

Goodfriend, Sophia, 'Algorithmic State Violence: Automated Surveillance and Palestinian Dispossession in Hebron's Old City' (2023) 55(3) *International Journal of Middle East Studies* 461–478.

Gross, Aeyal, *The Writing on the Wall: Rethinking the International Law of Occupation* (Cambridge University Press 2017).

Kalandarishvili-Mueller, Natia, *Occupation and Control in International Humanitarian Law* (Routledge 2021).

Kleineman, Jan, 'Rättsdogmatisk metod' in Nääv, Maria and Zamboni, Mauro (eds), *Juridisk Metodlära* (2nd Edition, Studentlitteratur 2021) 21–46.

Koutroulis, Vaios, 'The application of international humanitarian law and international human rights law in situation of prolonged occupation: only a matter of time?' (2012) 94(885) *International Review of the Red Cross* 165–205.

Kranenborg, Herke, 'Art 8 – Protection of Personal Data' in Peers, Steve; Herve, Tamara; Kenner, Jeff and Ward, Angela (eds), *EU Charter of Fundamental Rights: A Commentary* (2nd Edition, Bloomsbury Publishing 2021) 231–290.

Lubell, Noam, 'Human rights obligations in military occupation' (2012) 94 (885) *International Review of the Red Cross* 317–337.

Lubin, Asaf, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law' in Kolb, Robert; Gaggioli, Gloria and Kilibarda, Pavle (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (Edward Elgar Publishing 2022) 463–492.

Lubin, Asaf and Shehabi, Omar Yousef, 'The New Frontlines: Digital Rights Protection in Contemporary Armed Conflicts' in Ducheine, Paul; Gill, Terry; Pijpers, Peter and Zwanenburg, Marten (eds), *A Research Agenda for Military Law* (Edward Elgar Publishing 2026) 115–125.

Mansoor, Nimra, *The Evolution of the Law of Occupation* (Conflict Law Centre, Research Society of International Law Pakistan 2023).

McCarthy, Conor, 'Legal Reasoning and the Applicability of International Human Rights Standards During Military Occupation' in Arnold, Roberta and Quénivet, Noëlle (eds), *International Humanitarian Law and Human Rights Law: Towards a New Merger in International Law* (Martinus Nijhoff Publishers 2008) 101–118.

Nabulsi, Karma: *Traditions of War: Occupation, Resistance, and the Law* (Oxford University Press 1999).

Neely, Mark E Jr, *The Fate of Liberty: Abraham Lincoln and Civil Liberties* (Oxford University Press 1991).

Nowak, Manfred, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd Revised Edition, N.P. Engel Verlag 2005).

Ovey, Clare and White, Robin C.A., *The European Convention on Human Rights* (5th Edition, Oxford University Press 2010).

Sassòli, Marco, 'Legislation and Maintenance of Public Order and Civil Life by Occupying Powers' (2005) 16(4) *European Journal of International Law* 661–694.

Schwenk, Edmund Heinz, 'Legislative Power of the Military Occupant under Article 43, Hague Regulations' (1945) 54(2) *Yale Law Journal* 393–416.

Shehabi, Omar Yousef, 'Emerging Technologies, Digital Privacy and Data Protection in Military Occupation' in Buchan, Russell and Lubin, Asaf (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE Publications 2022) 87–112.

Talbot, Rohan, 'Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory' (2020) 102(914) *International Review of the Red Cross* 823–849.

Torpey, John, *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge University Press 2000).

Véliz, Carissa, *The Ethics of Privacy and Surveillance* (Oxford University Press 2024).

Zwanenburg, Marten, 'Legal Issues Arising from the Military Use of AI-Supported Biometrics' (2026) 107 *International Law Studies* 152–183.

Zwanenburg, Marten and van de Put, Steven, 'The Use of Biometrics in Military Operations Abroad and the Right to Private Life' in Pijpers, Peter; Voskuil, Mark and Beeres, Robert (eds), *Towards a Data-Driven Military: A Multidisciplinary Perspective* (Leiden University Press 2022) 283–302.

ii. Legal instruments

International instruments

Hague Convention (II) with Respect to the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900) 187 CTS 429. (1899 Hague Regulations)

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 (adopted 18 October 1907, entered into force 26 January 1910) 205 CTS 277. (1907 Hague Regulations)

Convention relative to the Treatment of Prisoners of War (adopted 27 July 1929, entered into force 19 June 1931) 118 LNTS 343.

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 33 UNTS 993.

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)).

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287. (GCIV)

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171. (ICCPR)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3. (AP I)

Regional instruments

European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953) ETS No 5. (ECHR)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) ETS No 108. (Convention 108)

Charter of Fundamental Rights of the European Union [2000] OJ C364/1. (CFR)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC [2016] OJ L119/1. (GDPR)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89. (Law Enforcement Directive)

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 10 October 2018) CETS No 223. (Convention 108+)

Other

Instructions for the Government of Armies of the United States in the Field, General Orders No 100 (24 April 1863). (Lieber Code)

iii. Judicial decisions, advisory opinions and communications

International Court of Justice

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226, 240. (*Nuclear Weapons AO*)

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136. (*The Wall AO*)

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment) [2005] ICJ Rep 168. (*Armed Activities*)

Written Statement of the State of Israel, *Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem* (Written Proceedings, 27 July 2023) <<https://www.icj-cij.org/index.php/case/186/written-proceedings>> accessed 11 May 2026.

Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem (Advisory Opinion) [2024] ICJ Rep 753. (*Policies and Practices AO*)

United Nations Human Rights Committee

Canepa v Canada Communication No 558/1993, UN Doc CCPR/C/59/D/558/1993 (HRC, 3 April 1997).

European Court of Human Rights

The Sunday Times v. the United Kingdom App no 6538/74 (ECtHR 26 April 1979).

Niemietz v. Germany App no 13710/88 (ECtHR 16 December 1992).

Loizidou v. Turkey (Judgment) App no 15318/89 (ECtHR 18 December 1996).

Peck v. the United Kingdom App no 44647/98 (ECtHR 28 January 2003).

Perry v. the United Kingdom App no 63737/00 (ECtHR 17 July 2003).

Ilașcu and Others v. Moldova and Russia App no 48787/99 (ECtHR [GC] 8 July 2004).

Issa and Others v. Turkey App no 31821/96 (ECtHR 16 November 2004).

S. and Marper v. the United Kingdom Apps nos. 30562/04 and 30566/04 (ECtHR 4 December 2008).

Bărbulescu v. Romania App no 61496/08 (ECtHR [GC] 5 September 2017).

Gaughran v. the United Kingdom App no 45245/15 (ECtHR 13 February 2020).

Centrum för Rättvisa v. Sweden App no 35252/08 (ECtHR [GC] 25 May 2021).

Big Brother Watch and Others v. the United Kingdom Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR [GC] 25 May 2021).

Glukhin v. Russia App no 11519/20 (ECtHR, 4 July 2023).

Ukraine and the Netherlands v. Russia Apps nos 8019/16, 43800/14, 28525/20 and 11055/22 (ECtHR [GC] 9 July 2024).

International Criminal Tribunal for the former Yugoslavia

Prosecutor v Kunarac, Kovač and Vuković (Trial Judgment) IT-96-23-T & IT-96-23/1-T (ICTY, Trial Chamber, 22 February 2001).

Supreme Court of Israel

HCI 393/82 *Jam'iat Iskan Al-Ma'almoun Al-Ta'awuniya Al-Mahdouda Al-Masouliya Cooperative Society v Commander of IDF Forces in the Judea and Samaria Region* [1983] IsrSC 37(4) 785.

iv. Reports, commentary and documents from international organisations

United Nations

UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* UN Doc HRI/GEN/1/Rev.1 (8 April 1988). (Human Rights Committee *General Comment No. 16*)

UN Human Rights Committee, *CCPR General Comment No. 27: Article 12 (Freedom of Movement)* (2 November 1999) CCPR/C/21/Rev.1/Add.9. (Human Rights Committee *General Comment No. 27*)

UN Human Rights Committee, *General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant* (29 March 2004) UN Doc CCPR/C/21/Rev.1/Add.13.

UN Human Rights Committee, *Concluding Observations of the Human Rights Committee: Israel* (29 July 2010) UN Doc CCPR/C/ISR/CO/3.

UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue* UN Doc A/HRC/23/40 (17 April 2013).

UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* UN Doc

A/HRC/39/29 (3 August 2018). (HRC *Right to Privacy in the Digital Age* Report (2018)).

UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* UN Doc A/HRC/48/31 (13 September 2021). (HRC *Right to Privacy in the Digital Age* Report (2021))

UN Office of the High Commissioner for Human Rights, *The Situation of Human Rights in Ukraine in the Context of the Armed Attack by the Russian Federation, 24 February to 15 May 2022* (29 June 2022) (OHCHR *The Situation of Human Rights in Ukraine* Report).

International Committee of the Red Cross

International Committee of the Red Cross, *Documentation préliminaire pour la révision et l'établissement de Conventions ayant trait à la Croix-Rouge* (Circular No 368, Geneva, 15 February 1945).

Pictet, Jean (ed), *Commentary on the Geneva Conventions of 12 August 1949, Volume IV: Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (International Committee of the Red Cross 1958). (1958 ICRC Commentary).

International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (Report to the 33rd International Conference of the Red Cross and Red Crescent, Geneva, 12 December 2019).

Commentary on the Fourth Geneva Convention: Convention Relative to the Protection of Civilian Persons in Time of War (International Committee of the Red Cross 2025) (2025 ICRC Commentary).

Council of Europe

Council of Europe Committee of Ministers, *Explanatory Memorandum to Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector* (17 September 1987). (Council of Europe *Explanatory Memorandum*)

Council of Europe Committee of Ministers, *Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector* (adopted 17 September 1987 at the 410th meeting of the Ministers' Deputies). (Council of Europe *Recommendation No R (87) 15*)

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition* (Council of Europe 2021) <<https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>> accessed 10 April 2026. (Council of Europe *Guidelines on Facial Recognition*)

Council of Europe, *Draft Explanatory Report – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108)* <<https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2>> accessed 20 May 2026.

Council of Europe, ‘Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data’ 15-33. <<https://www.coe.int/en/web/data-protection/convention108-and-protocol>> accessed 10 April 2026. (Council of Europe *Explanatory Report on Convention 108+*)

European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights: Data Protection* (28 February 2026).

European Union

European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement* (26 April 2023).

v. Reports, commentary and documents from NGOs

Amnesty International, *Starved of Justice: Palestinians Detained Without Trial by Israel* (5 June 2012) <<https://www.amnestyusa.org/reports/starved-of-justice-palestinians-detained-without-trial-by-israel/>> accessed 20 May 2026.

B’Tselem, *Playing the Security Card: Israeli Policy in Hebron as Means to Effect Forcible Transfer of Local Palestinians* (2019) <https://www.btselem.org/sites/default/files/publications/201909_playing_the_security_card_eng.pdf> accessed 11 May 2026.

Human Rights Watch, *Born Without Civil Rights: Israel’s Use of Draconian Military Orders to Repress Palestinians in the West Bank* (2019) <<https://www.hrw.org/report/2019/12/17/born-without-civil-rights/israels-use-draconian-military-orders-repress>> accessed 15 April 2026. (HRW *Born Without Civil Rights* Report)

Human Rights Watch, *'We Had No Choice': 'Filtration' and the Crime of Forcibly Transferring Ukrainian Civilians to Russia* (2022) <https://www.hrw.org/report/2022/09/01/we-had-no-choice/filtration-and-crime-forcibly-transferring-ukrainian-civilians#_ftn116> accessed 20 May 2026 (HRW *We Had No Choice* Report).

Amnesty International, *Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT* (2 May 2023) <<https://www.amnesty.org/en/documents/mde15/6701/2023/en/>> accessed 20 May 2026. (Amnesty *Automated Apartheid* Report)

vi. Other materials

Tsvetkova, Maria and Gutterman, Steve, 'Russia's lower house votes to bring Crimea into Russia' *Reuters* (20 March 2014) <<https://www.reuters.com/article/world/russia-s-lower-house-votes-to-bring-crimea-into-russia-idUSDEEA2J04U>> accessed 20 April 2026.

Anischchuk, Alexei, 'Putin Admits Russian Forces Were Deployed to Crimea' *Reuters* (17 April 2014) <<https://www.reuters.com/article/markets/us/putin-admits-russian-forces-were-deployed-to-crimea-idUSL6N0N921H/>> accessed 20 April 2026.

Estrin, Daniel, 'Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, but Raises Concerns' *NPR* (22 August 2019) <<https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>> accessed 20 May 2026.

Amnesty International, 'Russia: Intrusive facial recognition technology must not be used to crackdown on protests' (31 January 2020) <<https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/>> accessed 10 April 2026.

Human Rights Watch, 'Russia Expands Facial Recognition Despite Privacy Concerns: Lack of Accountability, Oversight, Data Protection' (2 October 2020) <<https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns>> accessed 10 April 2026.

Human Rights Watch, 'Russia: Broad Facial Recognition Use Undermines Rights' (15 September 2021) <<https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights>> accessed 10 April 2026.

Dwoskin, Elizabeth, 'Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank' *The Washington Post* (5 November 2021) <<https://www.washingtonpost.com/world/2021/11/05/israel-palestinians-surveillance-facial-recognition/>> accessed 4 May 2026.

Asher-Schapiro, Avi and Nazih Osseiran, 'Why Does the US Still Retain the Biometrics of Millions of Iraqis?' *Reuters* (16 March 2023) <<https://www.reuters.com/article/technology/feature-why-does-the-us-still-retain-the-biometrics-of-millions-of-iraqis-idUSL8N35F028/>> accessed 16 May 2026.

Gunter, Joel, 'How Israel Jails Hundreds of Palestinians without Charge' *BBC News* (15 December 2023) <<https://bbc.com/news/world-middle-east-67600015>> accessed 16 May 2026.

Robins-Early, Nick, 'How Israel Uses Facial-Recognition Systems in Gaza and Beyond' *The Guardian* (19 April 2024) <<https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians>> accessed 16 May 2026.

Kingsley, Patrick and Bilal Shbair, 'Inside the Base Where Israel Has Detained Thousands of Gazans' *The New York Times* (6 June 2024) <<https://www.nytimes.com/2024/06/06/world/middleeast/israel-gaza-detention-base.html>> accessed 23 May 2026.

BBC Visual Journalism Team, 'Ukraine in Maps: Tracking the War with Russia' *BBC News* (24 February 2026) <<https://www.bbc.com/news/articles/c0l0k4389g2o>> accessed 1 April 2026.