The Rights to Privacy and Data Protection in Times of Armed Conflict

Edited by
Russell Buchan
Asaf Lubin

CCDCOE

The Rights to Privacy and Data Protection in Times of Armed Conflict

Russell Buchan and Asaf Lubin (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The Rights to Privacy and Data Protection in Times of Armed Conflict

ISBN (print): 978-9916-9565-6-4
ISBN (pdf): 978-9916-9565-7-1

2022 © NATO CCDCOE Publications
NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Cover design & content layout: Stuudio Stuudio

FOREWORD

For more than a decade, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has been analyzing cyberwar while wishing for cyber peace. That wish has been granted: what we have may be tumultuous, tense, and fragile, but it is peaceful. At least peaceful in the sense of existing below the threshold of conflict and violence. Consequently, non-war realities form the context for a vast share of our legal research. While, for instance, the first Tallinn Manual was a book about war, *Peacetime Regime for State Activities in Cyberspace* and Tallinn Manual 2.0, two later publications, sought to explore the uneasy kind of peace we are currently experiencing. This edited volume examines the rights to digital privacy and data protection in times of armed conflict while also offering a broader perspective on the fundamental differences between war- and peacetime thinking about cyber security and privacy. In doing so, it critically dissects how the rules of war and peace shape the ways our digital data is collected and utilized.

Legal writing on the relationship between international human rights law (IHRL) and international humanitarian law (IHL) has focused mainly on the rights that are closer to the kinetic theatre of war and thus also to the core of IHL. Even though the majority of States and experts take the view that both IHRL and IHL apply to cyber activities in relation to an armed conflict, the unsettled interplay between the two has rarely been elucidated further. Despite the militaries' increasing dependency on data, digital human rights are still, often reflexively, considered a peacetime legal concern. It is tacitly assumed that, should war break out, there would be more specific norms to rely on. Yet in fact, when it comes to the right to privacy, IHL is surprisingly silent. This silence cannot be deliberate, unless, of course, the laws of war were drafted by technological visionaries who foresaw the risks and opportunities that personal data could one day entail in terms of intelligence, weaponry, or human dignity. Therefore, building on the assumption that IHRL plays a key role in protecting our informational privacy before, during, and after an armed conflict, the essays in this anthology delve a great deal deeper into the realistic remits of privacy and data protection in a military context.

The editors and authors have elegantly united two clashing discourses—that of the critical necessities of conflict and that of the peace and freedom people seek in their daily lives. Naturally, implementing the ideas expressed here might create short-term practical and procedural

obstacles in planning or executing military (cyber) operations. That would call for a sobering reassessment of how much personal data is actually needed for any given military activity, be it the biometric identification of prisoners of war or protected persons, the development of AI-based cyber weapons, the preservation of evidence for postwar investigations, or the storage of records held by international criminal tribunals. Furthermore, hard questions must be asked, such as where the data comes from and whether it actually provides any national security or military advantages. But these contemplations are essential for a just and efficient military decision-making that can keep pace with its technological environment.

The discussions in the book are as relevant to the complex balancing act between civilian normality and military necessity as they are to data-processing practices within the military community. At their heart is a concern that people should be able to lead dignified lives that are not reducible to mere behavioral statistics and involve a few secrets. A study into the means to protect such lives from arbitrary violations can only advance our ability to understand both conflict and peace against their current technological backdrop and therefore makes for a truly valuable addition to CCDCOE's work.

Ann Väljataga
International law researcher
Lead of the Privacy in Conflict research project
CCDCOE

Table of Contents

DIGITAL RIGHTS IN THE *JUS POST BELLUM*

AUTHORS AND EDITORS

Laurie Blank is clinical professor of law, director of the Center for International and Comparative Law, and director of the International Humanitarian Law Clinic at Emory University School of Law. She is the co-author of *International Law and Armed Conflict: Fundamental Principles and Contemporary Challenges in the Law of War*, a casebook on the law of war, and is a core expert on the Woomera Manual on International Law of Military Space Operations, a senior fellow at the Lieber Institute for Law and Land Warfare, and chair of the American Society of International Law Lieber Prize Committee.

Russell Buchan is senior lecturer in international law at the University of Sheffield, UK. He has published widely in the field of public international law, including three monographs: *International Law and the Construction of the Liberal Peace* (Hart, 2013), *Cyber Espionage and International Law* (Hart, 2018), and *Regulating the Use of Force in International Law: Stability and Change* (Edward Elgar Publishing, 2021). He is also co-editor of the *Journal of International Humanitarian Legal Studies*.

Amir Cahane is a researcher at the Israel Democracy Institute and a research fellow at the Federmann Cyber Security Research Center in the Law Faculty of the Hebrew University. His current research interests are artificial intelligence and the law, as well as the oversight and regulation of online surveillance.

Tim Cochrane is a PhD candidate at the University of Cambridge Faculty of Law and Fitzwilliam College, supported by the Stan Gold PhD Studentship. His PhD research focuses on law enforcement cross-border data sharing and privacy. Tim obtained an MPhil Law (Dist) from the University of Oxford, an LLM (Dist) from the University of Pennsylvania Law School, and an LLB/BA (Hons) from the University of Otago. Tim is admitted to practice in New York, England and Wales, and New Zealand. Before returning to study, he worked as an international disputes attorney in each of these jurisdictions

Emily Crawford is an associate professor at the University of Sydney Law School, where she teaches and researches in international law, international humanitarian law and international criminal law. She has

published widely in the field, including *The Treatment of Combatants and Insurgents under the Law of Armed Conflict* (Oxford University Press, 2010) and *Identifying the Enemy: Civilian Participation in Hostilities* (Oxford University Press, 2015) and a textbook (*International Humanitarian Law* (with Alison Pert, 2nd edition, Cambridge University Press, 2020). She has just published her third monograph, on the impact of non-binding instruments in international humanitarian law. She is co-editor of the *Journal of International Humanitarian Legal Studies*.

Tara Davenport is an assistant professor at the National University of Singapore, where she teaches law of the sea and international regulation of shipping. She is a senior research fellow at the Centre for International Law (CIL) at NUS and deputy director of the Asia-Pacific Centre for Environmental Law (APCEL). She is co-rapporteur for the International Law Association's Committee on Submarine Cables and Pipelines. Her research interests are in public international law, law of the sea, marine environmental law and international dispute settlement.

Kristina Hellwig is a researcher and lecturer at the Department of Law at the School of Socio-Economics of the Faculty of Business, Economics and Social Sciences at the University of Hamburg, Germany. Her primary research interests are public international law, international criminal law and human rights law. Her current research focuses on digital evidence in international criminal law.

Deborah A. Housen-Couriel is chief legal officer and VP Regulation of the Israeli cybersecurity firm Konfidas. She teaches international and Israeli cyber law at Hebrew University, where she serves on the advisory board of the Federmann Cyber Security Research Center. Deborah was a member of the Tallinn 2.0 Manual group of experts and co-chaired the Law and Regulation Committee of Israel's National Cyber Initiative. Her current research interests include regulatory regimes mandating cyber information-sharing, and the intersection of cyber law and outer-space law.

Eric Talbot Jensen is the Robert W. Barker Professor of Law at Brigham Young University, where he teaches and writes in the areas of public international law, national security law, the law of armed conflict and criminal law. Prior to becoming a professor, he worked as a legal advisor to United States military commanders while deployed to Bosnia, Kosovo, Macedonia and Iraq.

Asaf Lubin is an associate professor of law at the Indiana University Maurer School of Law and a fellow at IU's Center for Applied Cybersecurity Research (CACR). He is also an affiliated fellow at Yale Law School's Information Society Project, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a visiting scholar at the Hebrew University of Jerusalem Federmann Cyber Security Research Center. Dr Lubin's research draws on his experiences as a former intelligence analyst, sergeant major (res.) with the Israeli Military Intelligence Branch, as well as his vast practical training and expertise in national security law and foreign policy. Dr Lubin's work also reflects his time spent serving as a Robert L. Bernstein International Human Rights Fellow with Privacy International.

Tal Mimran is the academic coordinator of the International Law Forum of the Hebrew University and the research director of the Federmann Cyber Security Research Center in the Law Faculty of the Hebrew University. Tal has worked in the past as a researcher at the Israel Democracy Institute and edited an online human rights journal. Aside from his academic work, Tal used to work as a legal adviser in the Israeli Ministry of Justice, and he serves, in reserve duty, as a legal adviser in the Israel Defense Forces (international law department).

Mary Ellen O'Connell is the Robert and Marion Short Professor of Law and Research Professor of International Dispute Resolution—Kroc Institute for International Peace Studies, University of Notre Dame. She is the author or editor of many publications, including, notably, *The Art of Law in the International Community* (Cambridge University Press, 2019), *Self-Defence Against Non-State Actors* (with C. Tams and D. Tladi; Cambridge University Press, 2019), and *The Power and Purpose of International Law* (Oxford University Press, 2008). Mary Ellen has chaired the Use of Force Committee of the International Law Association and served as a vice president of the American Society of International Law.

Yaël Ronen is professor of international law at the Academic Center for Science and Law and a research fellow at the Minerva Center for Human Rights at the Hebrew University in Jerusalem. She obtained her PhD at the University of Cambridge, England. Her scholarship focuses on the intersection between human rights, issues of territorial status, and non-state actors. Prior to her academic career, Professor Ronen served in the Israeli Foreign Ministry and was a member of the Israeli negotiating team in the Oslo Process.

Yuval Shany is the Hersch Lauterpacht Chair in International Law and former dean of the Law Faculty of the Hebrew University of Jerusalem. He also currently serves as vice president for research at the Israel Democracy Institute and was a member of the UN Human Rights Committee in 2013–2020. Professor Shany chairs the Hebrew University's Minerva Center for Human Rights academic committee, serves as the co-director of the Faculty's International Law Forum and Transitional Justice Program, and heads the CyberLaw program of the Hebrew University CyberSecurity Research Center.

Omar Yousef Shehabi is a JSD candidate at Yale Law School, where he received his LLM degree in 2020. He is also a legal officer with the United Nations Office of Administration of Justice. He is a generalist public international lawyer with particular interest in international dispute settlement, the law of international responsibility, the law of international organisations, international labour law, human rights and international humanitarian law. His recent scholarship has focused on notions of permanence and reversibility in the discourse of international law, the peaceful settlement of territorial disputes, the interplay of collective labour law and international investment law, federalism and decentralisation in the Arab world, and the evolution of the 'international law of nationalism' since the dissolution of the former Yugoslavia.

Jacqueline Van De Velde is an associate at King & Spalding LLP. She earned her JD from Yale Law School. Her work has been featured in the *University of Chicago Law Review* and the *Cardozo Law Review*, as well as published by Oxford University Press. She is interested in cyber interference and international law in the digital age.

Eliza Watt is a lecturer in law at Middlesex University, London; guest speaker at the College of Information and Cyberspace, National Defense University, Washington, DC; and a visiting lecturer at the British Law Centre, University of Warsaw. Dr Watt's research focuses on cyber law and human rights. She is the author of a monograph titled *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*, published by Edward Elgar Publishing in 2021. She has contributed, *inter alia*, to the UN Office of Disarmament Affairs 2017 study titled 'Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary' and to the 2020 European Parliament Research Service Project 'Data Subjects,

Digital Surveillance, AI and the Future of Work'. Her work has been published in a number of leading academic journals in the field of cyber surveillance and privacy.

Leah West is an assistant professor of international affairs at the Norman Paterson School of International Affairs at Carleton University, where she teaches public international law, national security law and counter-terrorism. She completed her SJD at the University of Toronto Faculty of Law in 2020; her research explored the application of criminal, constitutional and international law to state conduct in cyberspace. Leah previously served as counsel with Canada's Department of Justice in the National Security Litigation and Advisory Group. Prior to attending law school, Leah served in the Canadian Armed Forces for 10 years as an armoured officer; she deployed to Afghanistan in 2010.

ABBREVIATIONS

ABIS	US Department of Defense's Automated Biometric Identification System
AI	artificial intelligence
AP I	Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts
ASEAN	Association of Southeast Asian Nations
CCPA	California Consumer Privacy Act (US)
CCTV	closed-circuit television
CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (US)
COGAT	Israeli Coordinator of Government Activities in the Territories
COMINT	communications intelligence
COVID-19	Corona Virus Disease 2019 caused by SARS-CoV-2.
DARPA	US Department of Defense's Advanced Research Projects Agency
DCO	Israeli-Palestinian district coordination and liaison office
DNA	deoxyribonucleic acid
DP	Data protection
DPI	deep packet inspection
EC	European Commission
ECHR	European Court of Human Rights
EDA	European Defence Agency
EEZ	European economic zone
ELINT	electronic intelligence
ESG	environmental, social, and governance issues
EU	European Union
FRT	facial recognition technology
GAO	US Government Accountability Office
GB	gigabyte
GC I-IV	Geneva Conventions I-IV
GCHQ	Government Communications Headquarters (UK)
GDPR	General Data Protection Regulation
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
GWOT	Global War on Terror
HIDE	handheld interagency detection equipment
HIPAA	Health Insurance Portability and Accountability Act of 1996 (US)
HRC	UN Human Rights Council
IAC	international armed conflict
IACHR	Inter-American Commission of Human Rights
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICL	international criminal law
ICP	international criminal procedure
ICRC	International Committee of the Red Cross

ICT	information and communication technologies
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for the former Yugoslavia
IED	improvised explosive devices
IHL	international humanitarian law
IHRL	international human rights law
IMT	International Military Tribunal
IP	Internet Protocol
ISAF	NATO International Security Assistance Force
ISIS	Islamic State in Iraq and Syria
IT	information technology
LDAP	Lightweight Directory Access Protocol
LOAC	law of armed conflict
LOSC	UN Convention on the Law of the Sea of 1982
MNF-I	Multi-National Force — Iraq
MNJTF	Multinational Joint Task Force
NATO	North Atlantic Treaty Organization
NGO	non-governmental organisation
NIAC	non-international armed conflict
NISP	NATO Interoperability Standards and Profiles
NSA	National Security Agency (US)
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OEWG	UN Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies
PESCO	Permanent Structured Cooperation (EU)
PIPEDA	Personal Information and Protection and Electronic Documents Act (Canada)
POW	prisoner of war
RPE	Rules of Procedure and Evidence (ICC)
RTS	Radio Television of Serbia
SEC	Securities and Exchange Commission (US)
SIGINT	signals intelligence
SOSUS	Sound Surveillance System
TB	terabyte
TEU	Treaty on European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context
UNGPBHR	UN Guiding Principles on Business and Human Rights
US	United States
WTO	World Trade Organisation

ACKNOWLEDGEMENTS

It truly takes a village. This project would not have come to fruition if it was not for the tremendous support that we received along the way from colleagues and friends in our community. First and foremost, we wish to thank Ann Väljataga, law researcher at the NATO CCDCOE, and the entire CCDCOE team. Ann was the first person to conceive the idea for this book and to solicit our involvement in this project. As the NATO CCDCOE representative, she has been there at every juncture guiding much of the behind the scenes activity. We truly owe her a debt of gratitude. We are also very grateful to the NATO CCDCOE for publishing this book and for their continued leadership role in developing and promoting pioneering new studies at the intersection of cyber security and international law.

We also wish to thank colleagues at both Indiana University Maurer School of Law and the broader Indiana University community. In particular, we wish to thank Indiana University Global Gateway, Berlin and specifically its Director Andrea Adam Moore for putting together an unbelievable in-person workshop in the Fall of 2021 and in the midst of a global pandemic. The book evolved significantly thanks to those workshop sessions. We also wish to acknowledge the Ostrom Workshop and its Director Scott Shackelford for believing in this project and for providing seed money and guidance in support for it. Finally, we wish to thank Hannah Baxumbaum, Vice President for International Affairs at Indiana University (OVPIA), Ally Batten, Director of Global Gateway Network at Indiana University, and the entire OVPIA family for their generous matching grant funds and support.

Finally, no research project that we take on is ever possible without the support of our partners and immediate family. Thank you for always being there.

Russell Buchan
Asaf Lubin

Introduction

Russell Buchan and Asaf Lubin

As we are writing this introduction war is raging in Europe. Russian aggression[1] against Ukraine has already led to the death or injury of thousands of soldiers and civilians. Whole Ukrainian cities are under siege and subject to heavy shelling as corridors of humanitarian relief are formed to support millions of Ukrainians as they flee west in search of refuge. The images of devastation and destruction coming out of Ukraine are a chilling reminder of some of humanity's most savage tendencies. These images trigger historical trauma from wars in the European continent's past. But at least in some respects, the 2022 Russian invasion into Ukraine represents the future of warfare.

The formation of a global cyber militia to support the war efforts of Ukraine by conducting cyber attacks against Russian targets offers one example of that future.[2] Another one is represented by the role that citizens are playing in the real-time documentation of war crimes using

1 U.N. General Assembly, U.N. Doc. A/ES-11/L.1 (Mar. 1, 2022), https://www.documentcloud.org/documents/21314169-unga-resolution.

2 *See e.g.* Matt Burgess, *Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory*, Wired (Feb. 27, 2022), https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/. Russell Buchan and Nicholas Tsagourias, *Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?*, EJIL: TALK! (Mar. 9, 2022), https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/.

their smartphones. This type of "user-generated evidence" is dramatically changing the face of international criminal investigations and prosecutions.[3]

The conflict is also a propaganda war with both States trying to develop and disseminate a narrative by controlling the flow of information in and out of the region. As more and more social media giants pull out of Russia and as Russian authorities continue to censor speech, a new "digital barricade between the country and the West" is forming, "erasing the last remnants of independent information online."[4] Meanwhile, in Ukraine news conferences where captured Russian POWs are paraded "to counter the Kremlin's propaganda" have become a routine.[5] These conferences join other "gory videos" shared by Ukraine's Ministry of Internal Affairs on TikTok, Twitter, and YouTube "purporting to show dead bodies of Russian soldiers."[6]

So while we have not yet seen a full-fledged cyber war break out in Ukraine, as some had initially anticipated,[7] these anecdotal examples do tell an evolving story about the informationalization, digitization, and datafication of warfare. In fact, Ukraine only serves as the dress rehearsal for what is to come in this regard. Already now the U.S. Department of Defence (DoD) has a "formal objective to treat data as a strategic asset," and to consider its collection and deployment for warfighting efforts as "the currency of future warfare."[8] The DoD thus recognizes that "it is in a high stakes race to harness the power of data and is actively working on creating a culture of data-centric decision-making."[9] These tendencies are only likely to increase with the incorporation of machine learning and artificial intelligence applications into greater parts of the military apparatus.[10]

3 *See e.g.* Rebecca Hamilton and Lindsay Freeman, *The Int'l Criminal Court's Ukraine Investigation: A Test Case for User-Generated Evidence*, JUST SECURITY (Mar. 2, 2022), https://www.justsecurity.org/80404/the-intl-criminal-courts-ukraine-investigation-a-test-case-for-user-generated-evidence/.

4 Adam Satariano and Valerie Hopkins, *Russia, Blocked From the Global Internet, Plunges Into Digital Isolation*, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.

5 Isabelle Khurshudyan and Sammy Westfall, *Ukraine puts captured Russians on stage. It's a powerful propaganda tool, but is it a violation of POW rights?*, WASHINGTON POST (Mar. 9, 2022), https://www.washingtonpost.com/world/2022/03/09/ukraine-russia-prisoners-pows/.

6 *Id*.

7 Kari Paul, *'Catastrophic' cyberwar between Ukraine and Russia hasn't happened (yet), experts say*, THE GUARDIAN (Mar. 9, 2022), https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.

8 Robert Work and Tara Murphy Dougherty, *It's Time for the Pentagon to Take Data Principles More Seriously*, WAR ON THE ROCKS (Oct. 6, 2020), https://warontherocks.com/2020/10/its-time-for-the-pentagon-to-take-data-principles-more-seriously/.

9 *Id*.

10 *See e.g.* David Vergun, *Delivering AI to Warfighters Is Strategic Imperative*, US DEP'T DEF. (Sept. 10, 2020), https://dodcio.defense.gov/In-the-News/News-Display/Article/2347200/

But as Omri Ben-Shahar once said, "[t]he digital economy creates digital smog,"[11] in the sense that "[e]missions of data are like emissions of other pollutants; the costs are often external, degrading social interests."[12] In the context of military operations in war, that social interest being degraded might very well be our collective strive to protect the lives, the physical and mental health, and the human dignity of individuals. Consider again the digital iron curtain being erected in Russia or the collection of user-generated evidence across cities and towns in Ukraine. What is at stake in both instances are a set of digital rights — informational privacy and data protection, anonymity, encryption, internet access, freedom of online expression, freedom from online censorship, access to information, internet security, and cyber security. If we do not act soon, we might grow to regret our failure to appreciate the magnitude of the potential externalities that certain data-driven wartime practices have on this list of digital rights. Put differently, the trend towards treating data as a strategic asset in war might stand in direct opposition to a decades-long humanitarian campaign to minimize human suffering and protect persons affected by armed conflict.

Troublingly, the 1949 Geneva Conventions and 1977 Additional Protocols, the bedrock of contemporary treatises of international humanitarian law (IHL), offer very little guidance as to the protection of digital rights during war. We certainly have the Martens Clause, which the International Court of Justice once described as "an effective means of addressing the rapid evolution of military technology."[13] But the general commitment to "the laws of humanity and the requirements of the public conscience" is a poor substitute for tailored rules, standards, and analytical frameworks that could be responsive to the tectonic technological shifts generated by a growing military datasphere.

Looking beyond treaty law, "there is practically no international legal jurisprudence, commentaries, or academic literature" that applies digital rights like the rights to privacy and data protection in times of armed conflict.[14] Indeed, it would seem that the "pace of technological

delivering-ai-to-warfighters-is-strategic-imperative/; Kelley M. Sayler, *Artificial Intelligence and National Security*, CONG. RESEARCH SERV. (Nov. 10, 2020), https://crsreports.congress.gov/product/pdf/R/R45178/10.

11 Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 118 (2019).

12 *Id.*, at 112.

13 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion [1996] ICJ Rep 226, para. 78 (Jul. 8).

14 Asaf Lubin, T*he Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES 463, 466 (Robert Kolb, Gloria Gaggioli and Pavle Kilibarda eds., 2022).

innovation is outmatching the intellectual stamina and regulatory capacities of IHL rule-prescribers and rule-appliers."[15] When Asaf Lubin first wrote these words in a book chapter in 2019 he didn't imagine that they will turn into a full research agenda. But shortly after a draft of that chapter was released to the world, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) approached Asaf and asked him to lead this book project. He immediately suggested the involvement of Russell Buchan and together they spent the next two years as co-editors bringing this project to life.

In light of the technological advances in the fields of electronic surveillance, social engineering, predictive algorithms, big data analytics, artificial intelligence, automated processing, biometric analysis, and targeted hacking, we presented our contributing authors with a herculean task. We asked each author to doctrinally and theoretically explore the ways that these technologies, and others, are already interacting or could possibly inter- act in the future with wartime digital rights. In so doing, we invited the authors to grapple with the concurrent and extraterritorial application of these rights, with the limitations and possible derogations from these rights during war, and with their scope of application to actual case studies and scenarios taken from the field.

Our contributing authors rose to this challenge in two ways. First, their chapters provide a unique canvassing of the various actors that play a role in the multistakeholder and polycentric tapestry of governance that controls emerging military technologies. Particular focus is given to non-State actors and their obligations to protect digital rights in the context of wartime data generation, collection, and dissemination activities. The chapters thus provide a true *tour de force* of the ecosystem, examining such actors as military contractors, tech giants, internet service providers, cloud providers, third-party vendors and suppliers of software and hardware, armed groups, international organizations and fact-finding missions, courts and tribunals, journalists, and humanitarian actors.

Second, the chapters also offer a wide ranging account of specific IHL regimes, including the law of targeting, the law of occupation, the law of neutrality, weapon acquisition, coalition operations, the law of detainees and POWs, the protections of property in war, the law on weapons review, and the law governing *jus post bellum* investigations. Each chapter provides a deep dive into a different classic field of study in IHL and in

15 *Id.* at 491.

each chapter the authors chart riveting pathways for reconceptualizing traditional rules to futureproof them against this technological revolution.

This collection is split into four parts. Part I explores the extent to which various regimes of IHL protect the rights to digital privacy and data protection. Part I begins with a chapter by Mary Ellen O'Connell and its core claim is that the protection afforded by international law to personal data is the same during times of armed conflict as it is during times of peace. This chapter advances this claim by relying on four interrelated arguments: first, personal data plays no role in the kinetic action of armed conflict; second, and due to the non-kinetic nature of personal data, peacetime legal protections continue to apply during times of armed conflict; third, the protection of personal medical data under IHL extends by analogy to other personal data; and fourth, targeting personal data cannot be justified on the basis of military necessity and cannot be carried out in compliance with the duty to take precautions, thus rendering such operations unlawful under IHL.

In Chapter 2, Tal Mimran and Yuval Shany document the privacy-related risks associated with the development of new military technologies such as autonomous weapons, cyber operations, and the enhancement of human soldiers. This chapter argues that the weapons review obligation contained in Article 36 of Additional Protocol I to the Geneva Conventions requires State parties to integrate privacy concerns into their evaluation of new military technologies and assesses whether these technologies can be used compliantly with the right to privacy as it is protected under international human rights law. This chapter maintains that the weapons review obligation requires States to develop a unique privacy impact assessment methodology, which demands consideration of a host of difficult issues such as the likely long-term harms and indirect harms caused by autonomous and cyber weapons and when soldiers can be said to have consented to human enhancement.

In Chapter 3, Laurie Blank and Eric Talbot Jensen examine the extent to which IHL governs the seizure, destruction, and requisition of data during times of armed conflict. Critical to this assessment is whether data can be regarded as 'property' because, as they reveal, the relevant rules of IHL only apply to 'property'. Assuming that data can be regarded as property, this chapter explores when the appropriation of data can be regarded as an act of 'pillage', which is prohibited by IHL. This chapter also assesses which types of data fall within the meaning of 'war booty', which is important because IHL permits parties to armed conflicts to seize such property where it is necessary to assist the war effort.

In Chapter 4, Jacqueline Van De Velde focuses on the situation in which private companies located in neutral States transfer data to parties to armed conflicts. This chapter examines the extent to which the law of neutrality requires neutral States to monitor and prevent companies located within their jurisdictions from transferring data to parties to armed conflicts in breach of the data subject's rights to privacy and data protection. This chapter also assesses whether the law of neutrality imposes direct obligations on corporate entities, given that, in the digital age, they have come to possess quasi-sovereign status.

In Chapter 5, Omar Yousef Shehabi explains that contemporary occupying powers use a range of technologies to collect intelligence on the residents of occupied territories, including biometric IDs, facial recognition checkpoints, 'smart' video surveillance, spyware, and offensive cyber tools. Using the occupied Palestinian territory as a case study, this chapter considers how the conventional law of occupation may be progressively reinterpreted to protect digital privacy and queries whether the procedural approach to data protection duties and data subject rights emerging in human rights law interfaces with the nature of occupation regimes. It questions whether the source and scope of data rights and obligations can be defined as a matter of the general law of occupation, without resolving epistemological questions regarding particular occupation regimes.

In Chapter 6, Emily Crawford explores the privacy-related rights of prisoners of war (POWs) in the digital age. In particular, this chapter identifies the types of data that detaining powers can collect from POWs and examines how this data must be managed. It finds that there is a lack of IHL protecting the data of POWs and encourages stakeholders to develop more effective rules in this area, averring that international human rights law has much to offer in this regard and that its rules on the right to privacy can provide a model or blueprint to help guide the practice of detaining powers in the future.

Part II of this collection considers the impact of surveillance technologies on the protection of digital rights. In Chapter 7, Leah West highlights the tension between the obligation imposed on commanders by IHL to gather and use intelligence to inform their targeting decisions and the obligation imposed on parties to armed conflicts under international human rights law to respect the privacy rights of civilians who are affected by those intelligence operations. By using facial recognition technology as a case study, this chapter reveals the legal obligations that arise during an armed conflict that both necessitate and limit the use

of modern surveillance technology. It also identifies the core policy and procedural questions that commanders must consider before deploying facial recognition technology to meet those legal obligations.

In Chapter 8, Eliza Watt examines the impact of sustained drone surveillance on non-combatants in war zones and argues that legal constraints should be placed on this practice. This chapter identifies a lacuna in the IHL framework with respect to privacy and data protection rights. It demonstrates that IHL and international human rights law apply concurrently in armed conflict and contends that the international human rights law rules on mass surveillance of communications apply to this method of intelligence collection. This chapter argues that the rationale for their application is the constant care principle set out in Article 57(1) of Additional Protocol I to the Geneva Conventions, which places State parties under a continuous duty of care over civilian populations.

In Chapter 9, Tara Davenport demonstrates that attempts to intercept and collect data resident on or transiting through cable infrastructure are an increasingly common practice in armed conflict. This chapter identifies and explores the international law that applies where parties to armed conflicts seek to intercept and collect data located on cable infrastructure. Its analysis spans a range of international legal rules and regimes including the law of the sea, international human rights law, and IHL.

Part III of this collection examines the obligations of militaries and humanitarian organizations when it comes to the protection of digital rights. In Chapter 10, Tim Cochrane explores the potential for subject access rights — core data protection rights enabling a person to obtain their own personal data from others — to be used to obtain personal data from military agencies during armed conflicts, and labels these 'military subject access rights' (MSARs). This chapter explains the extent to which MSARs are available in four common law jurisdictions: Australia, Canada, New Zealand, and the United Kingdom. It then applies these MSARs to three hypothetical extraterritorial armed conflict case studies, taking into account overarching international human rights law and IHL. Overall, this chapter provides a practical roadmap for the exercise of MSARs by individuals and makes recommendations for comparator States and others to better provide and protect MSARs.

In Chapter 11, Deborah Housen-Couriel focuses on data sharing within multilateral military operations and especially the sharing of data relating to the members of their armed forces. While this chapter argues that IHL provides members of the armed forces with little data privacy protection, it maintains that coalition partners remain bound by their domestic law

regimes, which often include considerable data privacy protections. Using the European Union's General Data Protection Regulation as a sample regulatory regime for the protection of data privacy, this chapter explores the extent to which partners must respect the data privacy of members of their armed forces when sharing information. This chapter considers how personal data privacy might be supported as part of overall legal interoperability and argues that the requirement of legal interoperability exemplifies the need to coordinate civilian data protection regimes at the global level.

In Chapter 12, Asaf Lubin examines the International Committee of the Red Cross's (ICRC) obligations to protect data in the context of their humanitarian action. This chapter turns to the recent revelations of a sophisticated cyber attack that targeted ICRC servers storing the personal data of over 500,000 people worldwide. Building on that experience, this chapter explores the extent to which data custodians like the ICRC are legally bound, as a matter of international or transnational law, to protect the data of their constituencies, and the scope of such an obligation. While recognizing some of the ICRC's pioneering work in developing data protection norms and best practices for the humanitarian sector, this chapter also identifies challenges imposed by new and evolving technological, political, and market-based realities. These developments generate complex ethical and legal challenges on the ability of an organization like the ICRC to uniformly and consistently apply its data protection rules.

Part IV of this collection analyses the protection of digital rights in the *jus post bellum*. In Chapter 13, Kristina Hellwig examines the role of the right to privacy in the investigation and prosecution of international crimes. Focusing on the rules and procedures of the International Criminal Court (ICC), this chapter explores possible interferences with the right to privacy during criminal proceedings. In particular, it assesses whether the ICC's rules and procedures relating to the collection, handling, and use of digital evidence are compatible with the right to privacy as guaranteed by international human rights law. Looking forward, this chapter concludes by making some broader suggestions as to how the right to privacy should inform the work of international criminal tribunals in the future.

In Chapter 14, Yaël Ronen focuses on the 'right to be forgotten', that is, the right of individuals to remove personal information from the public sphere and especially when that personal information is linked to criminal activities. This chapter examines the human rights rationales for the removal of information relating to criminal activity from online resources,

platforms, and repositories. Moreover, it considers the factors that emerge when the criminal activity constitutes an international crime, such as the right to truth, the peremptory character of international crimes, the gravity of the international crimes in question, and public safety.

In Chapter 15, Amir Cahane proposes a 'right not to be forgotten' and does so in order to protect the identities of individuals caught up in humanitarian disasters. At the heart of this chapter is the concern that, particularly during humanitarian crises, private tech companies may deny individuals access to their online accounts. After explaining the adverse impact this can have on individual identities, this chapter explores the legal protections available to individuals affected by humanitarian disasters to maintain access to their online accounts. Finding that international law fails to adequately protect the 'right not to be forgotten', this chapter suggests that private tech companies should be subject to a moratorium that prevents them from blocking access to online accounts belonging to individuals caught up in humanitarian disasters.

Digital Rights in IHL Regimes

Chapter 1

Data Privacy Rights: The Same in War and Peace

Mary Ellen O'Connell[1]

INTRODUCTION

This chapter responds to the thesis that parties to an armed conflict may violate an individual's peacetime right to the privacy of their personal digitized data. Substantial evidence exists supporting the opposite position: people do not lose data privacy rights in armed conflict. Four supporting rationales are provided for this conclusion under the following headings: (1) the nature of personal digitized data; (2) the continuation of peacetime legal protections in armed conflict; (3) the protection of medical data in armed conflict; and (4) the restrictions imposed by military necessity.

Analysis of these four rationales proceeds in two parts. Part I briefly reviews international legal protections for personal digitized data. In the

1 Robert and Marion Short Professor of Law and Research Professor of International Dispute Resolution–Kroc Institute, University of Notre Dame. With great thanks for expert research and editing assistance to Kristen Burns, J.D. expected 2022.

course of that review, the nature of personal data is assessed—both its normative aspects and the fact it has no role in the kinetic exchange of fighting that constitutes armed conflict. The law tolerates the alteration of some rights owing to the realities of armed conflict. People may be killed, for example, and physical property may be destroyed. Personal data is not part of the kinetic exchange, meaning there is no need to alter personal data protections to gain an advantage in fighting. Part II then considers the alternative case: if personal digitized data did have some connection to armed conflict, it would nevertheless be exempt from interference under human rights protections that apply concurrently with international humanitarian law (IHL). It is well established that certain human rights protections apply at all times, even during armed conflict. While no tribunal has yet ruled on personal data protection rights in armed conflict, the same reasoning used by courts in deciding on the application of human rights during armed conflict applies to personal data. This choice of law supports the protection of personal data. Moreover, under the IHL principle of military necessity that guides the lawful targeting of persons and property in hostilities, killing and destruction are permitted only to obtain a definite military advantage. No definite military advantage accrues in a kinetic fight from malicious cyber conduct that interferes with personal data.

I
THE NATURE AND PROTECTION OF PERSONAL DIGITIZED DATA

The topic of this chapter is narrow. It is concerned not with all data that might be affected in armed conflict but with an individual's personal data in digitized form. This section describes personal data, emphasizing that it has no connection with the kinetic fighting of armed conflict. The international law relevant to personal data is international human rights law (IHRL), as well as regional and national data privacy protection laws and national criminal law.[2] The law on resort to force (*jus ad bellum*) and the law regulating the conduct of conflict (*jus in bello*) are not directly relevant.

2 *See, e.g.*, Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

While this chapter views the law from an international perspective, certain national and regional developments are influencing universal law. The definition of "personal data" in the European Union's General Data Protection Regulation (GDPR) provides a solid starting place. Personal data is:

> any information relating to an identified or identifiable natural person… one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[3]

Common examples of personal data include medical, legal, and financial records. Individuals and their communities have a clear interest in keeping personal data confidential except as they might authorize. With the advent of digitization for computer access and storage, protecting the confidentiality, integrity, and availability of personal data has become the goal of considerable lawmaking as well as technical efforts.[4]

International law on data privacy protection is developing through various national, regional, and international initiatives. The European Union's GDPR and the Council of Europe's Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data[5] both draw on human rights treaty provisions protecting privacy that predate digitization. The 1950 European Convention on Human Rights, for example, provides for protection of private life in Article 8. Two United Nations working groups have devoted considerable attention to the international legal protection of digitized data privacy: the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace (GGE) and the Open-Ended Working Group on Developments

3 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 (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 33 [hereinafter GDPR].

4 Robin Geiss and Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INT'L L. STUD. 556, 561–62 (2021). This paper is focused primarily on digitized content data, as opposed to the computer code upon which it depends. For an explanation of the distinction, see *id.* at 562.

5 Peter Hustinx, *Data Protection and International Organizations: A Dialogue Between EU Law and International Law*, 11 J. INT'L DATA PRIV. L. 77, 79 (2021). "There is no doubt that the EU—with the 1995 Directive and now the GDPR—has been very influential globally, but the substance and still growing scope of Convention 108+ has made it an obvious candidate for a global standard that is both interesting and attractive, also given the fact it is mentioned in the GDPR as [a] building block for an adequate—or essentially equivalent—level of protection for the purpose of its provisions on transborder data flows."

in the Field of Information Telecommunications in the Context of International Security (OEWG). In March 2021, the OEWG's final report became the first UN report on cybersecurity to be "adopted with direct governmental participation."[6] The report concludes that States "should respect human rights and fundamental freedoms… [and that] confidentiality of sensitive information should be ensured."[7]

The Secretariat of Legal Affairs for the Organization of American States' (OAS) Inter-American Juridical Committee confirms the existence of an international human right to personal data privacy today that flows from earlier human rights norms.[8] The OAS Secretariat cites the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), both of which include a right to privacy. The ICCPR provides in Article 17:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.[9]

The OAS Secretariat concludes that the scope of Article 17 and other forms of the right to privacy mean that "the right to privacy covers all aspects of life of the individual and also the processing of personal data by government and private organizations…."[10] The rationale for the right is closely tied to both human dignity and "respect for family life, religious, political, and sexual preferences," as well as the importance of being free from "the interception of communications, the use of hidden cameras, genetic testing, etc. The protection of privacy is necessary for the legal order to guarantee respect for personal dignity."[11]

The scope of the human right to privacy is limited by legitimate needs of law enforcement and other public purposes. In many States, a warrant

6 Adina Ponta, *Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes*, 25 ASIL INSIGHTS at 2, July 30, 2021, https://www.asil.org/sites/default/files/ASIL_Insights_2021_V25_I14_0.pdf.

7 Open-ended Working Grp. on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Sec., Final Substantive Rep., at 8, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021). *See also* Ponta, *supra* note 6, at 5.

8 Org. of Am. States Inter-Am. Jurid. Comm., Secretariat for Legal Aff., *Relation between Privacy Protection, Data Protection and Habeas Data*, http://www.oas.org/dil/data_protection_privacy_habeas_data.htm [hereinafter OAS Inter-Am. Jurid. Comm.].

9 G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights (Dec. 16, 1966).

10 OAS Inter-Am. Jurid. Comm., *supra* note 8.

11 *Id.*

or other form of legal process is required to access personal data.[12] The central question of this chapter is whether these protections end during armed conflict. The UN GGE was unable to resolve certain issues related to armed conflict. The GGE should have produced a report in 2017[13] but failed to do so because experts disagreed on "the concrete application of international law, particularly IHL, countermeasures, and the right to self-defense in cyberspace."[14] The GDPR has multiple scope provisions and exceptions that limit the law's application during national emergencies, including, apparently, armed conflict. GDPR Article 2 limits its application to the processing of personal data that form (or are intended to form) part of a filing system.[15] Thus it does not apply to "issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security" nor to "the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union."[16]

Other exceptions involve "important reasons of public interest"; the establishment, exercise, or defense of legal claims; and protection of the "vital interests of the data subject" or other people in instances where the data subject lacks the capacity to give consent.[17] Additionally, exceptions may be made where information is being provided to the public on the basis of demonstratable "legitimate interest."[18] Recital 112 explains "public interest," which figures into several of the exceptions explained above. Public interest justifications include situations where it is necessary to protect a data subject's or another person's vital interests (physical integrity or life), or data transfers to international humanitarian organizations for data subjects who are legally incapable of giving consent ("with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts").[19]

Geiss and Lahmann conclude that the GDPR seems to be precluded from applying to "any State activities in relation to conduct during situations of armed conflict."[20] In support, they cite the express limits in

12 *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-505, 100 Stat. 1848 (1986) (US).
13 Ponta, *supra* note 6, at 1.
14 *Id.*
15 GDPR, *supra* note 3, art. 2(1).
16 *Id.*
17 GDPR, *supra* note 3, art. 49(1).
18 *Id.*
19 GDPR Recital 112, https://gdpr-info.eu/recitals/no-112/.
20 Geiss & Lahmann, *supra* note 4, at 568.

the GDPR for "activities concerning national security" or "activities in relation to the common foreign and security policy of the Union" from its scope provisions.[21] Presumably, they take the view that data privacy rights do not apply in armed conflict even without express exceptions in national, regional, or international law. As discussed above, however, international law now includes human rights protections for personal data, so individuals are not dependent upon national or regional law for protection. Whether data privacy protections apply in armed conflict depends on international choice of law principles, not national or regional law scope provisions.

Even with respect to national or regional laws like the GDPR, however, national security exceptions cannot permit as much as Geiss and Lahmann seem to assume. First, States may only invoke national security exceptions in genuine national security situations. In *Russia — Measures Concerning Traffic in Transit*, the World Trade Organization (WTO) explained that an objective national security test requires the State to invoke the national security exception in good faith and meet a "minimum requirement of plausibility in relation to the proffered essential security interests."[22] Second, national and regional legislation that sets standards for the protection of human rights applies to States for the benefit of people under the State's jurisdiction. The GDPR, for example, is aimed at restricting EU States from infringing on the data privacy rights of EU nationals and others under EU prescriptive jurisdiction.[23] The GDPR and its exceptions do not apply beyond the limits of EU jurisdiction. There is no national security exception for the international human rights principles of data privacy. In an armed conflict, therefore, even if an EU member State invokes the national security exception, it would apply only to those under its prescriptive jurisdiction. The nationals of an adversary State are not under the invoking State's jurisdiction. They do not lose protections because of a national security exception. This critical point appears to be mostly overlooked in discussions of national security exceptions to the GDPR. Third, national security exceptions are usually subject to a

21 *Id.* at 566.

22 *See* Report of the Panel, *Russia — Measures Concerning Traffic in Transit*, ¶ 7.138, WTO Doc. WT/DS512/R (Apr. 5, 2019), https://www.wto.org/english/tratop_e/dispu_e/512r_e.pdf.

23 GDPR, *supra* note 3, art. 3. Article 3 states that the GDPR applies to controllers or processors in the EU, regardless of whether the processing of data actually occurs within the EU, and controllers or processors outside of the EU that process information on data subjects in the EU. *Id.* "Customary international law permits exercises of prescriptive jurisdiction if there is a genuine connection between the subject of the regulation and the state seeking to regulate." Restatement (Fourth) of the Foreign Relations Law of the United States § 407 (Am. Law Inst. 2018). *See id.* §§ 408–13 (explaining the most common bases for establishing a genuine connection as territory, effects, active personality, passive personality, protection, and universal jurisdiction).

restrictive derogation process. A decision by the Court of Justice of the European Union explained that "derogations and limitations in relation to the protection of personal data… must apply only insofar as is *strictly necessary*."[24] As a matter of general human rights law, a "right to derogate is subjected to strict formal and substantive requirements."[25]

Geiss and Lahmann also suggest that when the GDPR does not apply, due to a national security exception or some other reason, IHL is the proper law to govern privacy rights in situations linked to armed conflict. This position appears to overlook more appropriate alternatives to IHL. In the now-considerable jurisprudence on the dual application of human rights and humanitarian law in armed conflict, the disconnect between kinetic impact and personal data requires the application of privacy rights in armed conflict.

Geiss and Lahmann provide several scenarios in which digitized data is controlled or destroyed in situations that are linked to armed conflict. The scenario bearing most closely on the physical force that constitutes hostilities while also involving personal digitized data is the following:

> During an armed conflict between State A and State B, the military of State A carries out a ransomware operation against the servers of a hospital in State B that store patients' case files, encrypting them until State B is willing to withdraw its troops from a contested island located on the continental shelf of State A.[26]

The core conduct is the same as the ransomware attack aimed at the Republic of Ireland's health care sector in mid-May 2021. After an international cybercrime gang known as Conti encrypted medical files,[27] the Irish health service shut down IT systems, Reuters reported, "to protect them from a 'significant' ransomware attack, crippling diagnostic services, disrupting COVID-19 testing and forcing hospitals to cancel many appointments."[28] The difference between the real case from

24 European Data Protection Board, Guidelines 10/2020 on Restrictions under Article 23 GDPR, at 10 (Dec. 15, 2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf (quoting Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, ¶ 56 (Dec. 16, 2008) (emphasis added)).

25 *International Human Rights Law and the Role of the Legal Professions: A General Introduction*, *in* U.N. Office of the High Commissioner for Human Rights, Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers 16 (2003).

26 Geiss & Lahmann, *supra* note 4, at 557.

27 *Irish Cyber-Attack: Hackers Bail out Irish Health Service for Free*, BBC, May 21, 2021, https://www.bbc.com/news/world-europe-57197688.

28 Padraic Halpin & Connor Humphries, *Irish Health Service Hit by "Very Sophisticated" Ransomware*

Ireland and the hypothetical one is the form of the ransom. The demand in the hypothetical is related to the armed conflict, as it is for a troop withdrawal; by contrast, the demand in the Irish case was for money. For purposes of applying the proper law, it is the conduct that matters most, not the form of the ransom. In May 2021, for example, computer hackers based in Eastern Europe carried out a ransomware operation against a U.S. company operating the largest petroleum pipeline in the United States. For several days, until a U.S. $5 million payment was made, petroleum stopped flowing.[29] The hackers could just as easily have been working for the Taliban, seeking funds to purchase weapons for their armed conflict against Afghanistan's government and its ally, the United States.

In all of these cases, the law governing the ransomware operation is the national criminal law of the place of the injury or the place of the criminal conduct. The cases did not involve any direct connection to the kinetic action of an armed conflict, so IHL does not apply. State A could, for example, hack the computers of the weapons systems used by State B's troops on the contested island so that State A would have a military advantage in battling State B's troops for control of the island. State A might also hack the controls of a dam and release water to drown State B's troops. This second hypothetical use of computers in armed conflict might violate the IHL principle respecting critical civilian infrastructure.[30] It would, nevertheless, constitute a computer-enabled kinetic attack. These two hypotheticals pair computer operations with the kinetic action of weapons and a weaponized dam.

This analysis relies on two threshold definitions involving kinetic impact for the right to resort to force in self-defense and for the existence of armed conflict during which IHL applies. First, the right to resort to force under United Nations Charter Article 51 is triggered by a significant armed attack.[31] An attack of little gravity, such as a mere frontier incident, does not trigger the right of self-defense. Likewise, an attack of no kinetic impact, such as a ransomware incident, does not fit Article 51 any more than the imposition of heavy economic sanctions that might indirectly result in the deaths of people. Economic impacts have not been judged to be "armed attacks."

Attack, REUTERS, May 14, 2021, 3:39 AM, https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/.

29 *How a Major Oil Pipeline Got Held for Ransom*, VOX, June 8, 2021, 12:50 PM, https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

30 Geiss & Lahmann, *supra* note 4, at 564.

31 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 103 ¶ 195 (June 27).

Second, IHL applies only in armed conflict and occupation. Armed conflict, like armed attack, depends on the existence of certain factual prerequisites. It depends on kinetic impact—the actual exchange of armed fighting. In 2010, the International Law Association's Committee on the Use of Force reported on the definition of armed conflict in international law in light of the United States declaring a "global war on terror" in which it claimed the right to apply the combatant's privilege to kill and the right of indefinite detention worldwide regardless of the existence of hostilities within any reasonable territorial distance. Following five years of research into the practice and *opinio juris* of States from the adoption of the UN Charter in 1945 to 2010, the report said:

> The Committee confirmed that at least two characteristics are found with respect to all armed conflict:
>
> 1) The existence of organized armed groups
>
> 2) Engaged in fighting of some intensity
>
> In addition to these minimum criteria respecting all armed conflict, IHL includes additional criteria so as to classify conflicts as either international or non-international in nature.[32]

The international legal definition of armed conflict requires the exchange of armed fighting with the potential to inflict death or destruction. Some scholars take the alternative view that war or armed conflict are possible as a legal matter without kinetic impact. They argue that the use of malware against an opponent that creates injurious cyber effects alone is "cyberwar," "hybrid warfare," or just plain war. The argument fails to meet the definition of armed conflict under international law. Even those who argue for the recognition of "cyberwar" acknowledge that conflicts with minimal or no kinetic component do not easily fit the *jus ad bellum* or *jus in bello* regimes.[33] The attempt to expand what qualifies as armed conflict seems motivated by an interest in deploying new technologies

32 Int'l L. Ass'n, Committee on the Use of Force: Final Report on the Meaning of Armed Conflict in International Law 2 (2010), https://www.ila-hq.org/index.php/committees.

33 Harriet Moynihan, *The Vital Role of International Law in the Framework for Responsible State Behavior in Cyberspace*, J. Cyber Pol'y (2020), tandfonline.com/doi/pdf/10.1080/23738871.2020.1832550?needAccess=true. *See also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999); Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 Int'l L. Stud. 99 (2002).

in ways that are unlawful under existing law.[34] The discussion above on self-defense under Article 51 demonstrates that cyber attacks fail to meet the "armed attack" requirement. Malicious cyber conduct, including unauthorized use of personal data, cannot meet the requirements of IHL, in part because such conduct does not constitute armed conflict. IHL applies only in armed conflict or occupation.

II
PROTECTION OF PERSONAL DATA IN ARMED CONFLICT HOSTILITIES

In addition to the disconnect between armed conflict and personal data, further grounds exist for treating data privacy rights uniformly in peace and armed conflict. Courts have held that to the extent that normal peacetime human rights are capable of application in armed conflict, they must be honored. Given that personal data plays no role in kinetic conflict, compliance with peacetime protections is fully possible. Even if personal data played a role in conflict, two rules of IHL prohibit unauthorized use and thus preserve peacetime protection of personal data. IHL prohibits interference with medical data, which can be extended to other sensitive personal data.[35] In addition, the IHL targeting principle of military necessity leaves personal data immune from attack. Armed conflict is an abnormal occurrence that alters application and operation of rules and procedures but only to the extent necessary. Unauthorized use of personal data has little connection to overcoming the military power of an adversary.[36] Without this connection, no alteration of peacetime rights is warranted under the principle of military necessity.

34 Waxman echoes some scholars' advocacy during the Cold War for expanded rights to use military force by resorting to novel interpretations of the plain terms of the UN Charter and rules of customary international law in Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 425–26 (2011).

35 *See* Rules 25, 26, 28, and 29, Customary IHL Database, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/; Geiss & Lahmann, *supra* note 4, at 564 (citing TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 515 (Michael N. Schmitt ed., 2d ed. 2017)). *See, e.g.*, Helen McDermott, *Application of the International Human Rights Law Framework in Cyber Space*, *in* HUMAN RIGHTS AND 21ST CENTURY CHALLENGES: POVERTY, CONFLICT, AND THE ENVIRONMENT 190 (Dapo Akande, Jaakko Kuosmanen, Helen McDermott & Dominic Roser eds., 2020).

36 *See, e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I) art. 52, June 8, 1977, 1125 U.N.T.S. 3 (1979).

A THE CONCURRENT REGIMES OF IHRL AND IHL

The International Court of Justice (ICJ) held in its *Advisory Opinion on the Threat or Use of Nuclear Weapons* that certain human rights must be respected during armed conflict.[37] The ICJ cited non-derogable rights such as the right to life. Later decisions of international tribunals indicate that where conditions permit respect for normal peacetime human rights, including derogable rights, they must be respected even during armed conflict. Derogation is premised on need. Suspending the international human right to the privacy of one's personal digitized data, as discussed in Part I, is simply not critical to winning a war.

The *locus classicus* of the concurrent application of human rights and humanitarian law in armed conflict is the ICJ advisory opinion on *Nuclear Weapons*. The court famously explained "that the protection of the International Covenant of Civil and Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency."[38] Article 4 of the ICCPR does not expressly cite the right to privacy provided for in Article 17 as a non-derogable right, but it does provide strict procedural restrictions on derogation from any article, including Article 17. In particular, "States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation." As discussed above, derogation from the personal data privacy rights of non-nationals has little or no connection with the conduct permitted to defeat an adversary in an armed conflict.[39]

Moreover, meeting the further procedural requirements for derogation set out in Article 4(3) would eliminate any possible use of malware against personal data:

> Any State Party to the present Covenant availing itself of the right of derogation shall immediately inform the other States Parties to the present Covenant… of the provisions from which it has derogated and of the reasons by which it was actuated. A further communication shall be made, through the same intermediary, on the date on which it terminates such derogation.

37 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 240, ¶ 25 (July 8).
38 *Id.*
39 *See supra* notes 30 and 33 and accompanying text.

Informing other parties of derogation of digitized privacy protections should put the target of the derogation on notice to harden cyber protections.

In the ICJ's *Advisory Opinion on the Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory*, the court clarified additional aspects of the convergent regimes of IHRL and IHL. Human rights obligations under the ICCPR extend to a State exercising "jurisdiction" over individuals.[40] The best conception of cyberspace is as international space in which all customary international human rights apply, including the right to privacy, to be respected by States and non-State actors.[41] This view is consistent with the ICJ's decision in the *Wall* advisory opinion that while jurisdiction in the ICCPR is understood to be largely territorial, where a State lawfully exercises jurisdiction extraterritorially, the State must respect the ICCPR.[42]

The *Wall* advisory opinion concerned occupation, where, because of the occupier's effective control of territory, most, if not all, peacetime human rights can be applied and, therefore, must be applied. The European Court of Human Rights (ECHR) reached a similar decision respecting the British occupation zone in Iraq in *Al-Skeini v. United Kingdom*.[43] Application of human rights to situations of active armed conflict hostilities is more complex, but for rights such as the right to privacy, the outcome is the same as in occupation. In *Russia v. Georgia* (II), the ECHR extended the extraterritorial application of human rights obligations to "acts of its authorities which produce effects outside its own territory."[44] The one exception the court made to its own exercise of jurisdiction was to decline to adjudicate the kinetic uses of force in the active phase of hostilities.[45] Other, non-kinetic conduct, such as the detention and abuse of persons during active hostilities, does fall under the court's jurisdiction. The court found that Russia had violated human rights in its detention practices.[46] Interference with digitized, personal data is non-kinetic, as has been emphasized throughout this chapter, and thus, normal human rights continue to apply.

40 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 178–79 (July 9) [hereinafter Wall Advisory Opinion].
41 Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 J. CONFLICT & SECURITY L. 187, 189 (2012).
42 Wall Advisory Opinion, *supra* note 40, at 179, ¶ 109.
43 Al-Skeini v. United Kingdom, App. No. 55721/07, 53 Eur. Ct. H.R. 589 (2011).
44 Georgia v. Russia (II), App. No. 38263/08, ¶ 133 (Jan. 21, 2021), http://hudoc.echr.coe.int/fre?i=001-207757. *See also* Marko Milanovic, *Georgia v. Russia No. 2: The European Court's Resurrection of Bankovic in the Contexts of Chaos*, EJIL: TALK! (Jan. 25, 2021), https://www.ejiltalk.org/georgia-v-russia-no-2-the-european-courts-resurrection-of-bankovic-in-the-contexts-of-chaos/.
45 *Id.*
46 *Id.*

The International Committee of the Red Cross (ICRC) helpfully summarizes the dual application of IHRL and IHL in a report on detention:

> [T]he interplay between IHL and human rights law is the subject of on-going debate. The issue is particularly relevant in situations of NIAC [non-international armed conflict] where the relative absence of treaty-based IHL repeatedly raises the question of whether human rights law should step in as the default regime. It is generally agreed that IHL and human rights law are complementary legal frameworks, albeit with different scopes of application. While most rules of IHL apply only during armed conflicts, human rights law applies at all times. Therefore, in times of armed conflict, certain norms of the two regimes overlap, sometimes leading to identical outcomes, sometimes revealing a gap in humanitarian law, and sometimes resulting in conflicting standards.[47]

B IHL ALONE

As already mentioned, even without the dual application of human rights law, IHL protects personal digitized data. IHL protections for data privacy may be found in at least two principles: the protection of medical data and similar personal data, and the restrictions on targeting derived from military necessity.

IHL expressly protects various aspects of medical services. The weight of international legal scholarly opinion holds that this protection extends to personal medical data.[48] Two approaches to other personal data follow from this position. If interpretation can lead to extending protections to aspects of medical care that are not expressly mentioned in IHL treaties, it is equally possible to use the same interpretative methods to extend protections from medical records to other personal records. Such an extension is an example of the legal canon of construction *nocitur a sociis*, "it is known by its associates."[49] The extension is also supported by the rationale for privacy protection. The same need for privacy respecting

47 ICRC, *Strengthening Legal Protection for Persons Deprived of their Liberty in Relation to Non-International Armed Conflict: Regional Consultations 2012–13*, Background Paper, at 5 (2013), https://www.icrc.org/en/doc/assets/files/2013/strengthening-legal-protection-detention-consultations-2012-2013-icrc.pdf.

48 Geiss & Lahmann, *supra* note 4, at 565.

49 *See generally* Canon, BLACK'S LAW DICTIONARY (Brian A. Garner ed., 11th ed. 2019); *Noscitur a sociis*, BLACK'S LAW DICTIONARY (Brian A. Garner ed., 11th ed. 2019).

medical records to protect human dignity exists to protect personal legal and financial records.[50]

On the other hand, some will point to the specific mention of "medical" in treaties and argue that non-medical data is excluded from protection. This might be an example of another canon of construction *ejusdem generis*, "of the same kind or class," whereby the mention of a specific thing or attribute excludes examples lacking that specific thing or attribute.[51] In this case, it would be the descriptor "medical." With respect to human rights, when two interpretations are possible, there is support for giving the presumption to the more generous interpretation — the interpretation supporting more extensive rights protection.[52] The presumption for personal digitized data is that all such data is protected in the same way that medical records are.

With respect to targeting, scholars are again divided into two groups, and again, the view that supports the wider protection of privacy must receive the presumption. There is, however, some uncertainty as to what interpretation of military necessity would achieve greater protection. The uncertainty flows from a debate over the nature of digital data for purposes of applying IHL. In the long tradition of IHL, objects must have a physical dimension, so that a kinetic impact will have physical consequences.[53] Most IHL scholars take the position that data is not an object.[54] A few scholars conclude that if data is not an object, it is subject to unregulated targeting. Kubo Mačák takes this position and argues on instrumental grounds that the world should view data as an object to prevent leaving it "fair game" for attack during armed conflict.[55]

50 *See supra* notes 10 and 11 accompanying text.

51 *Ejusdem generis*, BLACK'S LAW DICTIONARY (Brian A. Garner ed., 11th ed. 2019).

52 The Inter-American Court of Human Rights provides direct support for the presumption in favor of the more generous rights standard. It frequently applies the *pro persone* or *pro homine* principle of interpretation, which holds that the court should give a human rights standard at issue in a case its "widest expression." Alejandro Rodiles, *The Law and Politics of the* Pro Persona *Principle in Latin America*, *in* THE INTERPRETATION OF INTERNATIONAL LAW BY DOMESTIC COURTS (Helmut Philipp Aust and Georg Nolte eds 2016) 153–74, 162–63. Other support is found in the UN Charter references to member States having a duty to "promote" human rights and the growing influence of human rights law on IHL that results in interpretations of IHL that are increasingly protective. On the UN Charter, see HERSCH LAUTERPACHT, INTERNATIONAL LAW AND HUMAN RIGHTS (1950, reprinted 1968), 147–54. On IHL, see Theodor Meron, *Humanizing Humanitarian Law*, 94 AM. J. INT'L L. 239–78 (2000). Within IHL there are well-known presumptions in favor of the more protective civilian and prisoner-of-war statuses, as well as the presumption of innocence in criminal trials. *See* "Presumptions" *in* MARCO SASSÒLI ET AL., HOW DOES LAW PROTECT IN WAR? https://casebook.icrc.org/glossary/presumptions.

53 Geiss & Lahmann, *supra* note 4, at 565.

54 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 437 (Michael N. Schmitt ed., 2d ed. 2017).

55 Geiss & Lahmann, *supra* note 4, at 565 (citing Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISR. L. REV. 55, 73 (2015)). Dinniss considers content-level data generally outside the scope of the law of armed conflict. Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISR. L. REV. 39, 41 (2015).

Mačák's position is unpersuasive. As a legal matter, classification is based on a thing or concept's physical, social, or legal characteristics, not external issues such as the better legal regime to regulate or protect it. In addition, data does not lose protection because it is not an object. All of the human rights protections discussed above apply. Indeed, it is argued here that they apply regardless of whether some provisions of the *lex specialis* of armed conflict are applicable to some aspects of a situation.[56] Even then, some rules of IHL protect personal data from targeting irrespective of whether it is an object, such as the medical records rule.

Nevertheless, even taking Mačák's position, the outcome regarding targeting personal data is the same as that presented in peacetime and under the IHL analogy to medical records. Article 52 of the 1977 Additional Protocol I to the Geneva Conventions restates the legal test for lawful attacks on objects during armed conflict hostilities:

> *Article 52 — General protection of civilian objects*
>
> 1. Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph
>
> 2. Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[57]

Civilian objects are "all objects which are not military objectives," as defined in paragraph 2 of Article 52.[58] Any object which falls outside the definition in Article 52(2) is a civilian object. There are no lists or categories of legitimate military targets. The legality of attacking an object on the basis that it is a military objective depends on the specific facts. A weapons depot, for example, will likely satisfy the definition, but a

56 Nuclear Weapons Advisory Opinion, *supra* note 37.

57 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I) art. 52, June 8, 1977, 1125 U.N.T.S. 3 (1979). Dinniss refers to Article 52 as "customary international law"; it may more properly belong to the category of general principles of law. Regardless of the source of the principle and regardless of the treaty, it will be binding on States. Dinniss, *supra* note 55, at 40.

58 Dinniss, *supra* note 55, at 50.

bridge will require more careful assessment. The determination depends on the use being made of the bridge at the time it is targeted and the definite military advantage to be anticipated from its destruction. Even if some bridges are legitimate targets, others will not be.

In the *Banković* case, the petitioners argued that a building housing a television station in Belgrade was unlawfully destroyed by NATO bombing during the 1999 Kosovo crisis. The petitioners claimed the station was not being used for a military purpose, per Article 51:

> Most civilian objects can become useful objects to the armed forces. Thus, for example, a school or a hotel is a civilian object, but if they are used to accommodate troops or headquarters staff, they become military objectives.... In other words, the status of the object depends on the use being made of it at the time. The use to which the object is being put must make an "effective contribution to military action." That does not require a direct connection with combat operations but does require that the object: "provides an effective contribution to the *military* phase of a Party's overall war effort."
>
> The promotion of general political support for the war effort by means of propaganda does not represent an effective contribution to *military* action.... The second reason why the RTS [Radio Television of Serbia] building did not come within the definition of a military objective is that its destruction or neutralization did not offer a "definite military advantage."... The only potential military advantage in attacking the television station was to put an end to the broadcasts. An attack on the RTS building... could only interrupt transmission for a very brief period of time. Furthermore, putting an end to the broadcasts would not offer a *military* advantage, far less a "definite military advantage."[59]

Similarly, personal medical, financial, and legal data do not contribute in any way to the conduct of armed fighting, let alone contributing a definite military advantage. Even if they did, the targeting of civilian

59 Application, Banković v. Belgium, App. No. 52207/99 (Dec. 12, 2001) (citing COMMENTARY OF THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 1448 (Yves Sandoz et al. eds. 1987); Michael Bothe, Karl Josef Partsch & Waldemar A. Solf, NEW RULES FOR VICTIMS OF ARMED CONFLICTS (2d ed. 2013)).

objects requires taking precautions to protect the civilian population.[60] When civilians face a possible missile attack, for example, leaflets and other means of communication in advance provide warnings. Warning of a planned attack on digitized personal data will lead to defensive measures that would likely render the attempt to interfere unsuccessful. Cyber attacks tend only to inflict damage when carried out without warning. IHL, however, requires that precautions be taken. Complying with this IHL principle will prevent interference with personal data.[61]

CONCLUSION

This chapter has considered two competing theses with respect to an individual's privacy rights regarding personal digitized data. One thesis holds that the peacetime protection of personal privacy rights changes or disappears during armed conflict. The other thesis holds that they do not change. The same protections apply in peace and armed conflict. No interference is justified for the purpose of winning an armed conflict. The evidence and analysis presented in this chapter appear far stronger for uniform protection, judging by the four points reviewed in the chapter. First, the nature of digitized personal data is such that it plays no role in the kinetic action of armed conflict. This data does not operate weapons, weaponize objects, or communicate with troops. Second, as a result of the non-kinetic nature of personal data, the jurisprudence on the application of human rights protections during armed conflict applies to privacy rights. A State may derogate from privacy rights owed to its own nationals during times of emergency by following the proper derogation procedures of IHRL. Derogation does not apply to the rights owed during armed conflict to foreign nationals. Third, the protection of personal medical data under IHL extends by analogy to other personal data. Finally, interference with personal data is unlawful under the IHL targeting regime. Targeting personal data cannot meet the standard of military necessity or be carried out in compliance with the duty to take precautions. The protection of personal data is the same in war and peace.

60 Protocol I, *supra* note 57, art. 57.
61 Mary Ellen O'Connell, *Attribution and Other Conditions of Lawful Countermeasures to Cyber Misconduct*, 10 Notre Dame J. Int'l & Comp. L. 1, 10 (2020).

Chapter 2

Integrating Privacy Concerns in the Development and Introduction of New Military or Dual-Use Technologies

Tal Mimran and Yuval Shany[1]

INTRODUCTION

The rapidly evolving technologies of the digital age have dramatically changed the everyday life of billions of human beings and, consequently, the "human condition."[2] New and emerging technologies also impact significantly the ways in which military operations are conducted.[3] While

1 Dr. Tal Mimran is an adjunct lecturer at the Hebrew University of Jerusalem and a research fellow at the Academic College of Zefat; Prof. Yuval Shany is the Hersch Lauterpacht Chair in Public International Law at the Hebrew University of Jerusalem. The authors wish to thank Asaf Lubin and Russell Buchan for their invitation to join the project and for their helpful comments throughout the writing process. The authors also wish to thank the other contributors in the project for the useful suggestions and advice and to thank Ms. Tamar Hacohen for her invaluable assistance to the editing process.

2 *See generally* BRADEN R. ALLENBY AND DANIEL SAREWITZ, THE TECHNO-HUMAN CONDITION (2011). *See also* François Delerue, *Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace*, 13 INTERNATIONAL CONFERENCE ON CYBER CONFLICT 9, 12 (2021).

3 Laurent Gisel, Tilman Rodenhäuser & Knut Dörmann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts*, 102 INTERNATIONAL REVIEW OF THE RED CROSS 287, 293 (2020).

digital technology has permeated many parts of the militaries of information societies,[4] notable quantum leaps have been, or are being, achieved in three particular fields: the development of autonomous weapon systems,[5] the military use of cyberspace,[6] and the human enhancement of soldiers.[7]

All three fields involve a significant change in military capabilities and in the potential to harm civilians and civilian objects. Furthermore, they all engage dual-use digital technologies that have important civilian uses, but can also be adapted to serve military needs:[8] Artificial intelligence (AI)-based autonomous systems are already employed in a wide range of civilian settings, including medicine and transportation;[9] cyber operations affect conditions in cyberspace, a domain extensively utilized by civilian users for communication and access to information, comprising a linchpin of the contemporary global economic system;[10] and human enhancement technologies have an important role to play in treating, aiding, and rehabilitating injured persons and persons with disabilities in non-military contexts.[11] Still, their application in military contexts raises difficult legal issues relating to human control over military operations and accountability for violations of the laws of war and, as discussed below, serious privacy concerns. Granted, while various other human rights, including digital human rights,[12] might be implicated by new technologies, we chose to focus on the right of privacy, since privacy interests are especially affected by new military capabilities and because,

4 *See, e.g.*, Hans-Jörg Kreowski & Dietrich Meyer-Ebrecht, *Revolution in Military Affairs: Not without Information and Communication Technology*, The Future Information Society 439 (Wolfgang Hofkirchner & Mark Borgin eds., 2017).

5 UN Human Rights Council, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns*, *Lethal Autonomous Robotics*, UN Doc. A/HRC/23/47 (Apr. 9, 2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf.

6 *See, e.g.*, Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 Yale J.L. & Tech. 376, 382 (2018).

7 Yahli Shereshevsky, *Are All Soldiers Created Equal? On the Equal Application of the Law to Enhanced Soldiers*, 61 Va. J. Int'l L. 271, 274 (2021). *See also* NATO Sci. & Tech. Org., Science & Technology Trends 2020–2040 (2020).

8 Vincent Boulanin & Maaike Verbruggen, Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies 3 (2017), https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf.

9 *See, e.g.*, Yoav Mintz & Ronit Brodie, *Introduction to Artificial Intelligence in Medicine*, 28(2) Minimally Invasive Therapy & Allied Technologies 73 (2019).

10 Kenneth Geers, *The Cyber Threat to National Critical Infrastructures: Beyond Theory*, 18 Information Security Journal: A Global Perspective 1, 2 (2009). *See also* Tal Mimran & Yuval Shany, *Israel, Cyberattacks and International Law*, Lawfare (Dec. 30, 2020), https://www.lawfareblog.com/israel-cyberattacks-and-international-law.

11 Peter Emanuel et al., Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DoD 4 (2019); U.S. Dep't of Defense, Fiscal Year (FY) 2007 Budget Estimates (2006), at 11, https://www.darpa.mil/attachments/(2G10)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2007%20(Approved).pdf.

12 For a discussion of three generations of digital human rights, see Dafna Dror-Shpoliansky and Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights — A Proposed Typology*, European Journal of International Law (Forthcoming in 2021).

unlike other rights, the interests underlying the right to privacy are not adequately protected by international humanitarian law (IHL).

According to IHL—the international law branch regulating the conduct of hostilities—the legal implications of introducing new technologies into the military should be assessed in accordance to Article 36 of the First Additional Protocol to the Geneva Conventions (API), which obligates States parties to determine "in the study, development, acquisition or adoption of a new weapon or new means or methods of warfare," whether their employment would be prohibited under international law.[13] Not only the importance, but also the challenges, of conducting proper legality reviews under Article 36 increase in cases involving new technologies with unclear impact on civilians and civilian objects.[14] The picture is even more complicated when considering long-term impacts, including those on soldiers,[15] such as privacy violations that could continue to affect them long after they finish their military service.

In this chapter, we will examine one aspect of the reliance on Article 36 in legality reviews of military development and the use of new digital technology—whether it can serve as a vehicle for integrating privacy concerns in the evaluation of new military technologies, including dual-use technologies. After this introduction, we will present Article 36 and consider how international human rights law (IHRL) forms part of the review process (Part I). Then we will present in brief the privacy risks associated with new military technologies, in particular in the three aforementioned developments — the use of autonomous weapon systems, military operations in cyberspace, and enhancing human soldiers (Part II). Subsequently, we will discuss the role of privacy concerns in the review process prescribed by Article 36 in relation to new digital technologies (Part III). The final part of this chapter provides conclusions. We believe that privacy concerns can and should constitute an important part of the process of legality assessment for new technologies, particularly in relation to human enhancement technology, which threatens personal autonomy, physical and mental integrity, and the ability to pursue private life outside of military settings.

13 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, Article 36 (hereinafter API).

14 Boulanin & Verbruggen, *supra* note 8.

15 Thibault Moulin, No More Humans? *Enhanced Soldiers as a Weapon, Means or Method of Warfare*, Federmann Cyber Security Research Center (2021), https://csrcl.huji.ac.il/book/no-more-humans-enhanced-soldiers-weapon-means-or-method-warfare

I
THE ARTICLE 36 REVIEW MECHANISM

A basic tenet in IHL is that States are limited in their choice of weapons, and means or methods of warfare, by norms of international law.[16] Such norms sometimes ban specific weapons, such as explosive projectiles weighing less than 400 grams[17] or chemical weapons,[18] or means and methods of warfare, such as perfidy[19] or the starvation of a besieged population.[20] Such bans sometimes reflect broad acceptance among States that the humanitarian harm that the weapons, means, or methods cause likely exceeds any military advantage they afford.[21] At other times, the relevant norms of IHL identify a general principle, such as the prohibition on weapons that cause superfluous injury or unnecessary suffering[22] or the principle of distinction,[23] and expect States to implement it on a case-by-case basis. In all cases, however, some *ex ante* cost-benefit assessment is undertaken by States in order to determine whether to support the regulation outlawing specific weapons, means, or methods or embrace a general principle limiting their tactical choices. Once the regulation has been adopted, those bound by it must assess its compatibility with any new weapon and means or method of warfare they contemplate developing or using.[24]

16 Broadly speaking, bringing about suffering without a military purpose infringes IHL. *See* 1 Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law, rule 70 (2006). Interestingly, API refers alternately to "methods or means of warfare" (e.g., Articles 35(1) and 55(1)), "methods and means of warfare" (e.g., in Section I of Part III), "means and methods of attack" (in Article 57(2)(a)(ii)), and "weapon, means or method of warfare" (in Article 36). For an earlier version of the rule, see Article 22 of the 1907 Hague Regulations Respecting the Laws and Customs of War on Land. For discussion, see International Committee of the Red Cross, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977, 3 (2006), https://shop.icrc.org/a-guide-to-the-legal-review-of-new-weapons-means-and-methods-of-warfare-pdf-en.

17 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St. Petersburg, 1868; International Committee of the Red Cross, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, 4 (2006), https://shop.icrc.org/a-guide-to-the-legal-review-of-new-weapons-means-and-methods-of-warfare-pdf-en.

18 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45. 115 Protocol on Blinding Laser Weapons, Geneva, Oct. 13, 1995, 1380 U.N.T.S. 370.

19 API, art. 37.

20 API, art. 54(1).

21 For discussion, see Helen Durham & Timothy LH McCormack (eds), The Changing Face of Conflict and the Efficacy of International Humanitarian Law 66–73 (1999).

22 API, art. 35(2).

23 *Id.*, art. 48 and 54; Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law, rules 7 and 54 (2006).

24 *Cf.* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 55.

Article 36 of API gives effect to IHL limits on weapons, means, or methods of warfare by introducing a procedural obligation requiring States parties to the Protocol to conduct legality reviews:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[25]

The obligation under Article 36 applies regardless of whether the State develops and manufactures weapons itself or purchases them from another State or from a private company.[26] Furthermore, although many provisions of IHL apply only during times of armed conflict, legality reviews pursuant to Article 36 can, and often do, take place in peacetime, without connection to any specific armed conflict or military operation.[27]

Legality reviews are particularly important and challenging when dealing with weapons or means or methods of warfare based on new technologies (such as computing, nanotechnology, and synthetic biotechnology),[28] given the lack of scientific certainty as to their long-term impact on humanitarian interests.[29] In such cases, questions relating to the application of the precautionary principle, or some version thereof, might present themselves.[30] Confronting questions as to the precise point in time in which a legality review for new technology should be carried out, the International Committee of the Red Cross (ICRC) has persuasively maintained that the term "study" found in Article 36 alongside "development, acquisition or adoption" indicates a broad temporal scope.[31] The technologies discussed in this article are all at either the development or implementation stage.[32] As a result, Article 36 appears to be

25 API, art. 36.
26 Isabelle Daoust, Robin Coupland & Rikke Ishoey, *New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare*, 84 International Review of the Red Cross 345, 348 (2002).
27 *Cf.* Anne Dienelt, *"After the War is Before the War": The Environment, Preventive Measures under International Humanitarian Law, and their Post-Conflict Impact*, Environmental Protection and Transitions from Conflict to Peace: Clarifying Norms, Principles, and Practices 420, 421 (Carsten Stahn, Jens Iverson & Jennifer S. Easterday eds., 2017).
28 ICRC, Legal Review of Methods of Warfare, *supra* note 17, 5.
29 Boulanin & Verbruggen, *supra* note 8, at 6.
30 *See, e.g.*, Brian Rappert and Richard Moyes, *Enhancing the Protection of Civilians from Armed Conflict: Precautionary Lessons*, 26 Medicine, Conflict and Survival 24 (2010).
31 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 23.
32 *See, e.g.*, Moulin, *supra* note 15.

sufficiently broad to require review of all of them. It should also be noted that if new evidence or knowledge comes to light after the review was held, providing new information about the operational performance or effects of the weapon, means, or method of warfare, a new evaluation under Article 36 would be required.[33]

There are three categories that fall within the ambit of Article 36: weapons, means of warfare, and methods of warfare. The term "weapons" has been understood to include a range of offensive capabilities used in combat that are capable of causing damage to objects or injury or death to persons.[34] In the view of the ICRC, the term should be read broadly so as to encompass weapons and weapon systems of all kinds, including defensive weapons.[35] "Means of warfare" is an even broader term, extending to military equipment, systems, platforms, and other associated appliances used to facilitate military operations.[36] For example, a surveillance system would fall under this category, if it can collect information about potential military targets.[37] "Methods of warfare," by comparison, extends to a variety of military strategies and practices, as well as specific tactics used in military operations.[38] The ICRC explains that a method of warfare includes the manner in which weapons and means of warfare are expected to be used in warfare.[39] When dual-use equipment is introduced in connection with the conduct of hostilities, it should be subject to review, either as a weapon or as a means of warfare.[40]

Article 36 creates a binding procedural obligation for State parties to API. However, it may be claimed that other States who have not joined API but are nonetheless bound by substantive limits on weapons, means, or methods of warfare should resort to a comparable *ex ante* review of weapons and means, so as to avoid taking measures that would lead to

33 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 24.
34 Program on Humanitarian Policy and Conflict Research, Commentary on the Manual on International Law Applicable to Air and Missile Warfare 55 (2010).
35 ICRC, LEGAL REVIEW OF METHODS OF WARFARE, *supra* note 17, 9. For discussion of the Iron Dome system used in Israel, which raises interesting questions in this regard, see Daphné Richemond-Barak & Ayal Feinberg, *The Irony of the Iron Dome: Intelligent Defense Systems, Law, and Security*, 7 Harvard National Security Journal 469 (2016).
36 Heather A. Harrison Dinniss & Jann K. Kleffner, *Soldier 2.0: Military Human Enhancement and International Law*, 92 Int'l L. Stud. 432, 437 (2016). *See also* William H. Boothby, Weapons and the Law of Armed Conflict 4 (2009).
37 Boulanin &Verbruggen, *supra* note 8, at 3.
38 Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ¶ 1402 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987); Daoust et al., *supra* note 26, at 352.
39 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 10.
40 Boulanin & Verbruggen, *supra* note 8, at 3. For a discussion of the challenges of dealing with dual-use objects and infrastructure in the cyber context, see Gisel, Rodenhäuser & Dörmann, *supra* note 3, at 320.

a violation of their substantive obligations.[41] This is especially so, since Article 36 does not dictate any particular manner in which the review should be conducted, and its actual mechanisms of application differ from one State to the other in review aspects such as format, methodology, and mandate of the reviewing body.[42] Indeed, General Comment 36 of the Human Rights Committee (HRC) takes the approach that ensuring the protection of the right to life under the International Covenant on Civil and Political Rights (ICCPR) invites prophylactic impact assessment measures, including a legality review for new weapons,[43] and in practice, some States have resorted to review procedures without being members of API.[44] In any event, it is important to note that determinations of legality or illegality by one State do not create obligations for other States, nor do they affect their obligation to conduct their own legality review.[45]

According to the ICRC, the review should follow, whenever possible, a multidisciplinary approach, with particular scrutiny given to weapons, means, or methods of warfare that generate novel health effects.[46] States should consider during the review all the IHL rules that prohibit or limit the use of specific weapons and means or methods of warfare, regardless of whether they derive from a treaty, a custom, or a general principle of law.[47] In addition, States should consider whether the weapon infringes on the principles of humanity and the dictates of public conscience (based

41 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 4.

42 Several States implement weapons review mechanisms, including Australia, Belgium, and the United States. *See* Australia: Legal review of new weapons, Australian Department of Defence Instruction (General) OPS 44-1, June 2, 2005; Belgium: Défense, Etat-Major de la Défense, Ordre Général - J/836 (July 18, 2002), establishing La Commission d'Evaluation Juridique des nouvelles armes, des nouveaux moyens et des nouvelles méthodes de guerre; the Netherlands: Beschikking van de Minister van Defensie nr. 458.614/A, May 5, 1978, establishing the Adviescommissie Internationaal Recht en Conventioneel Wapengebruik; Norway: Direktiv om folkerettslig vurdering av vapen, krigforingsmetoder og krigforingsvirkemidler, Ministry of Defence, June 18, 2003; the United States: Review of Legality of Weapons under International Law, US Department of Defense Instruction 5500.15, Oct. 16, 1974; Weapons Review, US Department of Air Force Instruction 51-402, May 13, 1994. In Sweden the committee is composed of legal, military, medical, and arms technology experts, and in Norway it includes representatives from the Defence Research Establishment, the Army Material Command, the Logistic Resources Management Division, and the Defence Staff College. *See* Daoust et al., *supra* note 26, at 355–58.

43 Human Rights Committee, *General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life*, para. 65, UN Doc. CCPR/C/GC/36 (Oct. 30, 2018).

44 Daoust et al., *supra* note 26, at 348. The US is an example of a State not party to API that adopted weapons review procedures.

45 Howard S. Levie, Protection of War Victims: Protocol I to the 1949 Geneva Conventions 287 (1980).

46 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 6.

47 Daoust et al., *supra* note 26, at 350. Examples of customary prohibitions include poison or poisoned weapons, biological weapons, chemical weapons, and herbicides. *See* Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law (2006); Patrick Lin, *Could Human Enhancement Turn Soldiers into Weapons That Violate International Law? Yes*, Atlantic (Jan. 4, 2013), https://www.theatlantic.com/technology/archive/2013/01/could-human-enhancement-turn-soldiers-into-weapons-that-violate-international-law-yes/266732/.

on the well-known Martens clause).[48] Given its broad nature, the Martens clause is in itself a source for addressing unforeseen impacts of new military technology,[49] including new health factors.[50] This is of particular relevance to the violations of the right to privacy discussed below, which may entail physical and mental health repercussions.[51]

Furthermore, Article 36 invites States to consider new weapons, means, or methods of warfare in light of IHL, IHRL, and *any other rule of international law applicable to the High Contracting Party*.[52] Given the increased acceptance of the co-application of IHL and IHRL in armed conflict situations,[53] legality reviews should, in principle, include assessment of compatibility with both bodies of law. As we explain below, this is especially the case with regard to human rights that protect aspects of personal well-being that have no close parallel in IHL, such as the right to privacy, and which are nonetheless threatened by new technology.[54] The next section discusses such new technological developments that are incorporated in new weapons and means of warfare and considers their potential impact on the enjoyment of the right to privacy. Part III then considers the role of Article 36 reviews in that regard.

II
NEW TECHNOLOGIES AND THE ASSOCIATED LEGALITY CHALLENGES

Recent decades saw a significant technological leap in a number of fields amenable to military application either as new weapons or means of warfare, deployed through new methods of warfare. We will focus below on three fields where particularly dramatic developments have taken place,

48 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 17. As stated in Article 1(2) of API: "In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."

49 Legality of the Threat or Use of Nuclear Weapons, *supra* note 24, at ¶ 87; Daoust et al., *supra* note 26, at 351.

50 ICRC, Legal Review of Methods of Warfare, *supra* note 17, at 19.

51 Bensaid v. United Kingdom, 44599/98 Eur. Ct. H.R. at ¶ 47 (2001).

52 Daoust et al., *supra* note 26, at 349.

53 Legality of the Threat or Use of Nuclear Weapons, *supra* note 24, at ¶ 25; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J Rep. 168, ¶ 168 (Dec. 19). See, in the context of the Islamic State, Comm. on Econ., Soc. and Cultural Rts, *Concluding Observations on the Fourth Periodic Report of Iraq*, U.N. Doc. E/C.12/IRQ/CO/4, ¶ 5 (Oct. 27, 2015).

54 Harrison Dinniss & Kleffner, *supra* note 36, at 433.

entailing significant implications for the ability to enjoy the right to privacy — autonomous weapons, cyberspace, and human enhancement. These developments invite the question of how to integrate their privacy implications in relevant Article 36 review processes.

A AUTONOMOUS WEAPONS

At first glance, it may seem that autonomous weapons systems raise fewer privacy concerns than the other technologies discussed in this chapter, since they "merely" involve the substitution of human decision-makers with machines without necessarily changing the *modus operandi* of the controlled weapon systems.[55] Yet, a closer look at the new technology employed is likely to raise significant privacy concerns.

The development of military technology in the field of autonomous weapon systems has progressed remarkably in recent decades. True, only a few autonomous weapon systems — that is, systems that can take and execute decisions without human beings in the decision-making loop or exercising meaningful control over such decisions[56] — have actually been put into operation.[57] Still, advanced militaries have already acquired the capacity to deploy such weapon systems. The autonomous features of these new weapon systems obviously warrant a weapon review under Article 36 assessing, for example, the actual capacity of the autonomous weapon to distinguish between military and civilian targets, the manner in which they are programmed to apply the principle of proportionality and their propensity to generate "false positives", especially in light of interaction with unforeseen or unforeseeable circumstances.[58] In addition, the review must examine the meaningful controls and safeguards that are put in place to intervene in the event of system failure.[59]

Although the link between autonomous weapons systems and the right to privacy is indirect, it is nonetheless a meaningful connection. Like other AI weapon systems, the operation of autonomous weapon

55 For discussion, see Micah Clark, Claire Finkelstein & Oren Gross, *Autonomous Systems and the Ethics of Conflict*, 7 PENN. ST. J.L. & INT'L AFF. 74 (2020).

56 *See, e.g., id.*; UN Human Rights Council, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns, Lethal Autonomous Robotics*, UN Doc. A/HRC/23/47 (Apr. 9, 2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf; Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, UN Doc. CCW/GGE.1/2018/3 (Oct. 23, 2018), https://undocs.org/pdf?symbol=en/CCW/GGE.1/2018/3.

57 BOULANIN & VERBRUGGEN, *supra* note 8, at 17.

58 BOOTHBY, *supra* note 36, 341.

59 Michael W. Meier, *Lethal Autonomous Weapons Systems (Laws): Conducting a Comprehensive Weapons Review*, 30 TEMP. INT'L & COMP. L.J. 119 (2016).

systems presumes a constant flow of data and metadata about the conduct of adversary forces that underlies AI threat predictions, target identification, and machine learning.[60] This, in turn, requires a constant supply of intelligence by means of biometric surveillance, including facial and gait recognition, digital surveillance of cellular and online activity, and big data analysis.[61] The controversial United States drone program in Pakistan, which involved *inter alia* constant monitoring from the sky of large swaths of territory with a view to identifying "patterns of life" compatible with membership in terror organizations, feeding into specific targeting decisions, is illustrative of the means or methods of warfare that could support the operation of the aforementioned autonomous weapon systems.[62] Such means or methods do, however, have serious privacy implications, as they place broad populations under constant or almost constant surveillance.[63] In particular, human rights groups have chronicled the mental harm caused to civilians living under constant drone surveillance.[64]

An Article 36 legality review of autonomous weapon systems would arguably have to consider their dependency on constant surveillance, and the right to privacy and other implications of such practices. Such a review may result, among other things, in privacy protocols for data and metadata collection, retention and use.

B CYBERSPACE

In recent years, cyberspace has become an important domain for military operations, with cyber attacks becoming part of the reality of armed conflicts.[65] New cyber weapons and cyber capacities that constitute new

60 Alan Backstrom & Ian Henderson, *New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews*, 94 International Review of the Red Cross 483, 492 (2012).

61 Maziar Homayounnejad, *The Lawful Use of Autonomous Weapon Systems for Targeted Strikes (Part 2): Targeting Law & Practice*, TLI Think! Paper 13/2018 (2018), at 54, https://ssrn.com/abstract=3200416.

62 Michael N. Schmitt & Jeffrey S. Thurnher, *Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict*, 4(2) Harv. Nat'l Sec. J. 231, 268 (2013).

63 For a discussion, see, e.g., Katharine H. Kindervater, *The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology*, 47(3) Security Dialogue 223, 224 (2016); Tyler Wall & Torin Monahan, *Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes*, 15(3) Theoretical Criminology 239 (2011).

64 International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School of Law, Living Under Drones: Death, Injury, and Trauma to Civilians From US Drone Practices in Pakistan 80 (2012). *See also* Ranjana Ferrao, *Drones and the Future of Armed Conflict*, 16 ISIL Y.B. Int'l Human. & Refugee L. 270, 273 (2016–2017); The Humanitarian Impact of Drones 37 (Ray Acheson, Matthew Bolton, Elizabeth Minor & Allison Pytlak eds., 2017).

65 Gisel, Rodenhäuser & Dörmann, *supra* note 3, at 288–89.

means of warfare or invite the application of new methods of warfare unquestionably warrant a legality review under Article 36. Such a review should explore, for example, whether cyber tools aimed at disruption, degradation, or the destruction of information in military systems and networks,[66] or rendering those systems inaccessible,[67] are indiscriminate in nature or cause disproportionate harm to civilians and civilian objects. The case that there is a duty to conduct a legality review for cyber weapons and tools is particularly strong after it has been amply demonstrated that cyber attacks can cause significant and widespread damage to real-life objects and infrastructure[68] and that cyber attacks can also precede the deployment of conventional military force, or comprise part of a broader attack.[69]

Where cyber attacks facilitate conventional attacks—for example, when a cyber attack neutralizes air-defense systems[70]—there is little question that the use of cyber attack constitutes a means of warfare supporting the use of kinetic weapons, which would merit an Article 36 legality review. It is more difficult to categorize cyber capabilities intended to produce stand-alone attacks that do not cause physical harm as requiring an Article 36 review, since they may not qualify as a weapon or means of warfare under narrow understandings of these terms.[71] Still, according to broader interpretations, cyber tools applied by the military that can infiltrate without authorization into computer systems, manipulate, erase, or disrupt data, and result in impairment of the functionality of the targeted systems and the infrastructure dependent thereon, should be considered weapons or means of warfare for the purposes of Article 36.[72] Note that even cyber tools that do not fall under

66 Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17(2) JOURNAL OF CONFLICT & SECURITY LAW 229, 229 (2012).

67 Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J NAT. SEC. LAW AND POLICY 63, 64 (2010); Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 821 (2012).

68 Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J.L. & TECH. 376, 380 (2018).

69 Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 830 (2012). *See generally* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010).

70 For example, some claim that in September 2007, Israel infiltrated and disabled the radar systems of Syria in order to enable Israeli air force planes to enter Syria undetected and conduct an air strike against a nuclear facility. *See* Kenneth Geers, T*he Cyber Threat to National Critical Infrastructures: Beyond Theory*, 18 INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE 1, 4 (2009). Additional examples are the cyber attacks in Georgia before Russia's 2008 military invasion, and the cyber attacks in Ukraine in 2015–2017, during that country's military conflict with Russia. *See* Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare*, 1(1) JOURNAL OF LAW & CYBER WARFARE 99, 114 (2012); Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17(2) JOURNAL OF CONFLICT & SECURITY LAW 187, 188 (2012).

71 *See, e.g.*, William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INT'L L. STUD. 389 (2013); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017), rule 30.

72 BOULANIN & VERBRUGGEN, *supra* note 8, at 10; Cordula Droege, *Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INTERNATIONAL REVIEW OF THE

the scope of Article 36 might still need to be subject to *ex ante* review under IHRL, if they are likely to pose a real risk to basic human rights of affected individuals.

There are three principal ways in which cyber tools or weapons can infringe on the right to privacy—mass surveillance, data theft, and the engendering of cyber security vulnerabilities.[73] The first two types of activities may occur outside an armed conflict, but they may also be undertaken as a means of warfare intended to facilitate targeting decisions or generate actionable military intelligence.[74] Where mass surveillance or data theft is undertaken by military personnel or by other security agencies whose activities are embedded in military operations, there is little question that Article 36 should be resorted to and the associated privacy concerns considered in the review process. Still, the covert and dual-use nature of espionage activity by security agencies outside the military, which is capable of producing military actionable intelligence, could raise difficult practical problems in determining the timing and scope of the review, its legal basis (e.g., whether its mandated by Article 36 or international human rights law) and how to enforce the obligation to conduct it.

The third type of cyber operation is more characteristic of armed conflict situations or preparations for them. Degrading cyber defenses, identifying existing vulnerabilities, or installing malware that could disrupt computer functionality or facilitate cyber attacks might have collateral spillover effects in the sense that they would make it easier to conduct cyber attacks against affected civilian computers and to access personal civilian data

RED CROSS 533, 559 (June 2012). For an opposing view, see Roy Schondorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, EJIL TALK!, Dec. 9, 2020, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

73 The issue of data collection and its impact on privacy have been widely discussed. *See, e.g.*, Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the US*, 28 HARV. HUM. RTS. J. 65 (2015); Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663 (2006). In the Liberty case, surveillance by the United Kingdom was deemed to be in breach of the right to privacy, as it did not set out an accessible procedure to be followed for selecting for examination, sharing, storing, and destroying intercepted material. *See* Liberty and Others v. United Kingdom, E.C.H.R., 58243/00 (2008), ¶ 59. *See also* Stefan Kirchner, *Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 369 (2014); Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson*, ¶ 30 U.N. Doc. A/69/397 (2014) [43]; Report of the Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, ¶ 22 U.N. Doc. A/HRC/27/37 (June 30, 2014).

74 Another concern for privacy in the context of cyber operations can arise when they form part of espionage activities. While espionage has a long history, the technological tools used for it today raise renewed questions about its legality. Concerns arise relating to illegal intervention, infringement of diplomatic inviolability, and privacy. Espionage also occurs in peacetime, and as such, it is also questionable whether such actions fall under one of the three categories of Article 36 (weapon, means, or method of warfare). For discussion, see Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VIRG. J. INT'L L. 291, 302 (2015); Stefan Kirchner, *Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 369 (2014).

and metadata stored in them.[75] The cyber attack against the US Office of Personal Management (OPM) database, which compromised security data and personal data of a sensitive nature, exemplifies the potential linkage between cyber attacks in a military context (in the case of the OPM, most probably for military intelligence purposes) and right-to-privacy concerns of large numbers of affected individuals.[76] It would therefore seem that an Article 36 legality review is required to evaluate the long-term privacy implications of cyber operations that weaken cyber defenses.

C ENHANCEMENT OF HUMANS

The third field of new and emerging military technologies, which is perhaps most relevant to a discussion of the right to privacy, is the human enhancement of soldiers. The idea of human enhancement has long been a source of inspiration for popular-culture depictions, but it is also the subject of contemporary scientific research aimed at restoring full functionalities to ill or disabled persons or at conferring super-human capabilities on "enhanced humans."[77] In the military context, enhanced combatants might obtain heightened capabilities by wearing, and in some cases embedding in their bodies, integrated technology that improves their organic and natural functions (e.g., additional strength, reduced need for sleep, improved vision and better decision-taking capacity, etc.).[78] Arguably, human enhancement programs do not necessarily run contrary to IHL, as they can reduce operational mistakes during hostilities and thus reduce harm to civilians and civilian objects.[79]

The US Defense Advanced Research Projects Agency (DARPA) is a principal engine for the development of human enhancement projects directed at improving the capabilities of soldiers[80] and has invested signif-

75 Examples of spillover effects include the CrashOverride, WannaCry, and NotPetya incidents. For discussion, see Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations: Starting the Conversation*, Humanitarian Law and Policy Blog, Nov. 14, 2018, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

76 For discussion of the attack, see Stephanie Gootman, *OPM Hack: The Most Dangerous Threat to the Federal Government Today*, 11(4) Journal of Applied Security Research 517 (2016); Alan Wehbe, *OPM Data Breach Case Study: Mitigating Personnel Cybersecurity Risk*, 26(1) Boston University Public Interest Law Journal 75 (2017).

77 Harrison Dinniss & Kleffner, *supra* note 36, at 433; Patrick Lin et al., *Super Soldiers (Part 2): The Ethical, Legal and Operational Implications*, Human Performance Technology: Concepts, Methodologies, Tools and Applications 82 (2019).

78 Harrison Dinniss & Kleffner, *supra* note 36, at 434. For more discussion, see Patrick Lin, *Ethical Blowback from Emerging Technologies*, 9 Journal of Military Ethics 313 (2010).

79 Oren Gross, *The New Way of War: Is There a Duty to Use Drones?* 67 Fla. L. Rev. 1 (2016); Harrison Dinniss & Kleffner, *supra* note 36, at 444.

80 Yahli Shereshevsky, *Are All Soldiers Created Equal? On the Equal Application of the Law to Enhanced Soldiers*, 61 Va. J. Int'l L. 271, 274 (2021). *See also* Michael Joseph Gross, *The Pentagon's Push*

icant resources into promoting relevant research projects.[81] Such research often involves dual-use technology, since enhancement measures, like pain blocking or machine-brain interfaces, can also be used in civilian therapeutic contexts[82] and often rely on dual-use infrastructures like the internet[83] or global navigation satellite systems.[84]

Human enhancement is commonly divided into three main categories: biochemical, cybernetic, and prosthetic.[85] *Biochemical enhancement* entails the use of pharmaceutical agents to enhance physical and mental functions.[86] *Cybernetic enhancement*, or brain-machine interface, involves technologies that aim to connect electric signals produced by the human brain directly to a machine without the need for manual input.[87] Examples include the Avatar project in the United States, which develops interfaces and algorithms that will allow a soldier to partner up with a semi-autonomous bipedal machine, and the N3 program, aimed at broadening the applicability of neural interfaces to warfighters.[88] *Prosthetic enhancement* involves physical improvements for humans,[89] including prosthetics capable of providing sensory feedback and thought-controlled movement, visual prosthetics that allow for augmented or restored vision, and auditory enhancement.[90]

to Program Soldiers' Brains, ATLANTIC, Nov. 2018, https://www.theatlantic.com/magazine/archive/2018/11/the-pentagonwants-to-weaponize-the-brain-what-could-go-wrong/570841/.

81 Research, Development, Test and Evaluation: Hearing before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the H. Comm. on House Armed Services, 108th Cong. (2003) (statement of Tony Tether, Director, Defense Advances Research Projects Agency), at 12, https://www.darpa.mil/attachments/TestimonyArchived(March%2027%202003).pdf.

82 Harrison Dinniss & Kleffner, *supra* note 36, at 449. *See also* JOEL GARREAU, RADICAL EVOLUTION: THE PROMISE AND PERIL OF ENHANCING OUR MINDS, OUR BODIES—AND WHAT IT MEANS TO BE HUMAN 27–29 (2005).

83 Michael Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, JUST SECURITY, June 10, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

84 Gisel, Rodenhäuser & Dörmann, *supra* note 3, at 320.

85 Shereshevsky, *supra* note 80, 278.. *See also* Heather A. Harrison Dinniss, *Legal Aspects of Human Enhancement Technologies*, in NEW TECHNOLOGIES AND THE LAW IN WAR AND PEACE 230, 240 (William H. Boothby ed., 2018).

86 For discussion, see LUKASZ KAMIENSKI, SHOOTING UP: A SHORT HISTORY OF DRUGS OF WAR (2016). *See also* Helen Thomson, *Narcolepsy Medication Modafinil is World's First Safe "Smart Drug,"* GUARDIAN, Aug. 20, 2015, https://www.theguardian.com/science/2015/aug/20/narcolepsy-medication-modafinil-worlds-first-safe-smart-drug.

87 Harrison Dinniss & Kleffner, *supra* note 36, at 435. *See, e.g.*, Pierre Bienaimé, *Mind-Controlled Drones Are Already a Reality*, BUSINESS INSIDER, Oct. 24, 2014, https://www.businessinsider.com.au/drones-you-can-control-with-your-mind-2014-10; Emanuel et. al., *supra* note 11, 7.

88 This includes projects intended to use neural implants to control three aircrafts at once (including an F-35 fighter). *See* Zayan Guedim, *DARPA's BCI Chip Allows Pilots to Control Drones Telepathically*, EDGI, Sept. 11, 2018, 05:30 AM, https://edgy.app/is-this-real-darpas-hivemind-is-operational; MOULIN, *supra* note 15, at 11.

89 Emanuel et al, *supra* note 11, 4.

90 Harrison Dinniss & Kleffner, *supra* note 36, at 436. *See also* David Talbot, *An Artificial Hand with Real Feelings*, MIT TECHNOLOGY REVIEW, Dec. 5, 2013, https://www.technologyreview.com/2013/12/05/14493/an-artificial-hand-with-real-feelings/; Yahli Shereshevsky, *Are All Soldiers Created Equal? On the Equal Application of the Law to Enhanced Soldiers*, 61 VA. J. INT'L L. 271, 274 (2021); EMANUEL ET AL., *supra* note 11.

It is debatable which human enhancement technologies fall within the ambit of Article 36 of API. The enhanced human combatant is generally not considered a weapon (or a military object).[91] However, when brain-computer interface facilitates remote control of weapons like drones, it arguably constitutes means of warfare.[92] It has even been argued by Boulanin and Verbruggen that the deployment of enhanced soldiers can constitute a method of warfare, when the use of the enhanced capabilities is an integral part of the deploying military's offensive activities.[93]

The more the human enhancement technology is computerized and embedded in the human body and mind, the greater is the associated privacy risk.[94] Other than the direct risks emanating from the physical bodily intrusion which most enhancements entail, other indirect risks can also arise. For example, offensive tools might be developed in order to hack brain-computer interfaces[95] with a view to manipulating brain-connected weapon systems or assisted decision-making facilities, or to access the personal data generated by prosthetic digital devices.

III
PRIVACY CONCERNS AND LEGALITY REVIEWS

A THE CO-APPLICATION OF IHL AND IHRL

As noted before, we are of the view that legality reviews under Article 36 should consider both IHL and IHRL standards. This conclusion is inescapable from the language of Article 36, which alludes to *any* other rule of international law applicable and the broad consensus among international law experts surrounding the co-application of IHL and IHRL.[96] Hence, to

91 Harrison Dinniss & Kleffner, *supra* note 36, at 438. *But see* BOULANIN &VERBRUGGEN, *supra* note *8*, at 28–29.
92 MOULIN, *supra* note 15, at 4.
93 BOULANIN & VERBRUGGEN, *supra* note 8, at 28–29.
94 Harrison Dinniss & Kleffner, *supra* note 36, at 441.
95 MOULIN, *supra* note 15, at 21.
96 Legality of the Threat or Use of Nuclear Weapons, *supra* note 24, ¶ 226 ("…In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities"). *See also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J Rep. 168, ¶ 168 (Dec. 19). *See*, in the context of the Islamic State, Comm. on Econ., Soc. and Cultural Rts, *Concluding Observations on the Fourth Periodic Report of Iraq*, U.N. Doc. E/C.12/IRQ/CO/4, ¶ 5 (Oct. 27, 2015).

the extent that new military technologies such as autonomous weapons systems, cyber capabilities, and human enhancement can potentially harm the human rights of civilians or soldiers that are protected under international law, their compatibility with these international law norms should be part of an Article 36 legality review.

While the International Court of Justice (ICJ) considered IHL to be the *lex specialis* which enjoys interpretive precedence over IHRL,[97] this is not necessarily the case with respect to legal areas where IHRL contains more detailed norms or where IHL contains lacunae.[98] For example, the prohibition against torture, which constitutes a grave breach of the Geneva Conventions,[99] should be interpreted during an armed conflict in light of the Convention against Torture,[100] and the right to privacy, which is missing from IHL treaties,[101] can be applied as part of IHRL, as long as it does not contradict applicable IHL norms. In the latter context, it has also been claimed in the literature, although State practice does not appear to support this, that international law should adopt a *pro humanitate* presumption, favoring the international standard most protective of human well-being.[102] Accepting such a presumption might have led

97 Legality of the Threat or Use of Nuclear Weapons, *supra* note 24, ¶ 226 ("In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities"). Other international institutions have supported the view that both regimes apply simultaneously and have enriched the discussion on this issue. The Human Rights Committee grants priority to the norm which benefits the individual most in the relevant context, unlike the *lex specialis* suggested by the ICJ. The European Court of Human Rights (ECHR) and the Inter-American Commission of Human Rights (IACHR) also take a similar view to that prescribed by the Human Rights Committee. *See* Human Rights Committee, *General Comment No. 29: Article 4: Derogations during a State of Emergency*, U.N. Doc. CCPR/C/21/Rev.1/Add.11 (Aug. 31, 2001); Human Rights Committee, *General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life*, UN Doc. CCPR/C/GC/36 (Oct. 30, 2018), ¶ 64 ("both spheres of law are complementary, not mutually exclusive… practices inconsistent with international humanitarian law, entailing a risk to the lives of civilians and other persons protected by international humanitarian law… would also violate article 6 of the Covenant."); Hassan v. United Kingdom [GC], no. 29750/09 (Sept. 16, 2014); Isayeva v. Russia, App. No. 57950/00 (Feb. 24, 2005), ¶ 176; IACmHR, Juan Carlos Abella (Tablada case), Case No. 11.137, Nov. 18, 1997, Annual Report of the IACmHR 1997 (OEA/Ser.L/V/II.95 Doc. 7 rev) 271. For a discussion by the African Commission of Human Rights, see *Sudan Human Rights Organisation & Centre on Housing Rights and Evictions (COHRE) v. Sudan*, May 27, 2009 (45th Ordinary Session).

98 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 106 (July 9); Martti Koskenniemi (Chairman of Int'l L. Comm.), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, U.N. Doc. A/CN.4/L.682 (Apr. 13, 2006).

99 Convention (III) relative to the Treatment of Prisoners of War, Geneva, Aug. 12, 1949, 75 UNTS 135, art. 130; Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, Aug. 12, 1949, 75 U.N.T.S. 287, art. 147 [hereinafter GC IV].

100 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 1984, UN Doc. A/39/51; Nigel S. Rodley, *The Prohibition of Torture: Absolute Means Absolute*, 34 Denv. J. Int'l L. & Pol'y 145 (2006).

101 For a discussion, see Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., 2022).

102 William Schabas, *Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum*, 40 Israel Law Review 592, 593 (2007).

to the application of the right to privacy even with respect to matters directly regulated by IHL.

B CONSIDERATIONS OF PRIVACY IN THE EVALUATION OF NEW TECHNOLOGIES

Article 17 of the ICCPR, which lays out the global IHRL right to privacy norm, provides for the right of every person to be protected against arbitrary or unlawful interference with his or her privacy, as well as against unlawful attacks on his or her honor and reputation, whether emanating from State authorities or from other legal persons.[103] This right has been understood as protective of core aspects of human dignity[104] and autonomy[105] and as an important condition for physical and mental well-being and the enjoyment of other human rights.[106] Unlike many other human rights which are mirrored to a considerable extent by provisions of IHL, the right to privacy and associated international law norms (such as data protection obligations) enjoy only a very limited level of protection under IHL.[107]

Article 17 deals with protection against interference which is unlawful, namely not authorized in law, and with interference that is arbitrary, a notion that the HRC, which is the expert body responsible for monitoring the implementation of the ICCPR, has construed as including elements of inappropriateness, injustice, lack of predictability, reasonableness, necessity, proportionality, and due process of law.[108] From the States'

103 International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (1966); UN Human Rights Committee (HRC), *CCPR 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*, Apr. 8, 1988, ¶ 1, https://www.refworld.org/docid/453883f922.html. *See also* European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, 5 E.T.S. (1950).

104 Beizaras and Levickas v. Lithuania, App. No. 41288/15 Eur. Ct. H.R. ¶ 117 (2020).

105 Reklos and Davourlis v. Greece, App. No. 1234/05 Eur. Ct. H.R. ¶ 38 (2009).

106 For a discussion, see UN Human Rights Committee (HRC), *CCPR 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*, Apr. 8, 1988, ¶ 11, https://www.refworld.org/docid/453883f922.html.

107 See e.g., GC IV, art. 27 ("Protected persons 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*") (emphasis added).

108 UN Human Rights Committee, Views adopted by the Committee under Article 5(4) of the Optional Protocol, concerning communication No. 2081/2011, CCPR/C/117/D/2081/2011, Sept. 29, 2016, ¶ 7.6, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/217/46/PDF/G1621746.pdf?OpenElement. The ECHR also seeks to examine compatibility with the rule of law. *See* European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights—Right to Respect for Private and Family Life*, Aug. 31, 2020, ¶ 14, https://www.refworld.org/docid/5a016ebe4.html. In addition, part of the evaluation of a possible infringement of the right to privacy entails looking into the decision-making process leading to it (particularly if it was fair, and if due respect was afforded to the rights of the individual). *See* Buckley v. United

perspective, legitimate grounds for interference with the right to privacy may include national security, public safety, public health, or the protection of the rights and freedoms of others.[109]

As indicated above, all three military technologies discussed in the chapter have direct or indirect privacy implications, which may be relevant for Article 36 legality reviews: autonomous weapons depend on extensive data collection, military use of cyberspace is likely to result in a less secure online environment for personal data and metadata, and human enhancement might imply a direct intervention in the human body or mind or create conditions for digital surveillance and "brain hacking." Note that privacy harms potentially caused by the first two technologies implicate methods of warfare employed to use such weapons or means of warfare, whereas for the third technology, it is the weapon or means themselves that might violate the right to privacy. Indeed, human enhancement is the most challenging of the three new military technologies, not only because of its more direct privacy implications but also because of the magnitude of the challenge: the embedding of digital technology in human bodies may entail a dramatic invasion of the private sphere (even if consented to by the soldier in question), a change in personal identity, and a dire threat to personal autonomy,[110] given the possibility for manipulating bodily functions, including brain activities.[111]

An Article 36 legality review process, which evaluates the legal implications of possible harm to privacy caused by new military technology, should comprise a mapping of possible interferences with privacy, assessment of operational safeguards that can prevent or minimize any harm caused, and analysis of possible circumstances that might nonetheless justify the deployment of the reviewed technology. As indicated above, significant changes in the technology—for example, following a technical version update—would arguably require a new review either at the development stage or—especially when relying on private technology, at the introduction to use stage.

With regard to autonomous weapons and cyber operations, the conceptual issues (heightened surveillance, lower cyber security) are rather

Kingdom, App. No. 20348/92 Eur. Ct. H.R. (1996).

109 European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights—Right to Respect for Private and Family Life*, Aug. 31, 2020, ¶ 1, https://www.refworld.org/docid/5a016ebe4.html.

110 For a discussion, see Harrison Dinniss & Kleffner, *supra* note 36, at 453. There, Dinniss and Kleffner discuss somewhat analogous cases of genetic and chromosomal abnormalities: *X v. United Kingdom*, App. No. 8416/79, 19 Eur. Comm'n H.R. Dec. & Rep. 244 (1980); *H.L. v. United Kingdom*, 2004-IX Eur. Ct. H.R. 197; *Zarzycki v. Poland*, App. No. 15351/03 (2013) (ECtHR).

111 BOULANIN & VERBRUGGEN, *supra* note 8, at 30.

straightforward, and the review should focus on issues such as harm probabilities, safeguard or mitigation measures, and national security thresholds for the application of such technology. With regard to human enhancement, a more complex analysis will be required, bearing in mind also the diverse scope of enhancement techniques. For example, one aspect that might need consideration is the long-term personality modification and mental-well-being consequences for soldiers who have undergone human enhancement[112] and the possible harm to "personal honour and reputation" that might accrue from social stigma or negative public opinion against enhanced humans.[113]

In addition, as far as safeguards are concerned, it would be important to examine in the legality review process whether the enhancement system is embedded in the body or removable, what maintenance and version update operations are required, and whether it is possible to stop recording data generated by the system when the soldier is off-duty[114] or in private or intimate settings.[115] Another set of safeguards—also relevant to extensive data collection operations intended to facilitate the use of autonomous weapon systems—is the taking of effective measures to ensure that data collected from human enhancement devices will not reach the hands of persons who are not authorized by law to receive, process, or use it.[116] Finally, the legality review would have to consider the question of consent to human enhancement—the manner in which it is given; whether free, prior, and informed consent can be given in military settings; and whether all foreseeable and unforeseeable harms caused to the enhanced person can be cured or mitigated by any level of consent.[117] Cases where there is no free, prior, and informed consent by the enhanced human will most probably lead to a violation of the right to privacy, regardless of the actual impact of the technology at hand.

112 MOULIN, *supra* note 15, at 25.

113 UN Human Rights Committee (HRC), *CCPR 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*, ¶ 11, Apr. 8, 1988, https://www.refworld.org/docid/453883f922.html.

114 Harrison Dinniss & Kleffner, *supra* note 36, at 464; MOULIN, *supra* note 15, at 30.

115 MOULIN, *supra* note 15, at 31. By a way of an analogy, the ECHR recognized in the past that the lack of a divide between the sanitary facilities and the rest of the cell, in the context of detention, constitutes inhuman and degrading treatment (a prohibition sharing several values with right to privacy—physical and mental well-being, dignity, and the protection of autonomy). *See* Szafrański v. Poland, App. No. 17249/12, Eur, Ct. H.R. ¶ 24, and ¶ 38 (2015).

116 UN Human Rights Committee (HRC), *CCPR 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*, Apr. 8, 1988, ¶ 10, https://www.refworld.org/docid/453883f922.html.

117 Efthimios Parasidis, *Human Enhancement and Experimental Research in the Military*, *in* BEYOND BIOETHICS: TOWARD A NEW BIOPOLITICS 301 (Osagie K. Obasogie & Marcy Darnovsky eds., 2018). *See also* Thibault Moulin, *Doctors Playing Gods? The Legal Challenges in Regulating the Experimental Stage of Cybernetic Human Enhancement*, 54 ISR. L. REV. 236–62 (2021); Sahar Latheef & Adam Henschke, *Can a Soldier Say No to an Enhancing Intervention?* 5(3) PHILOSOPHIES 13 (2020).

As a result, the legality review may rule out any possible justification for application in a military context of certain military enhancement technologies and provide contexts and conditions under which some other enhancement technologies might be resorted to.

One consequence of accepting a duty to conduct a legality review for monitoring privacy harm is the need to develop a suitable impact assessment methodology. This is not a new insight: the ICRC's SIrUS Project, which brought together experts in the fields of weapons, medicine, law, and communications,[118] demonstrated the challenge of developing measurable indicators for the health effects of different weapon systems.[119] The concluding report of that project asserted that the effects of weapons on health should be the leading consideration when making legal, ethical, technical, and political decisions with respect to them.[120] Arguably, a similar need to develop indicators exists with regard to effects on different dimensions of privacy needs and interests, especially given the proven links between enjoyment of the right to privacy and physical and mental health.[121]

CONCLUSION

Developments in the fields of autonomous weapons, cyber operations, and human enhancement present new challenges for upholding IHRL in general, and the right to privacy in particular, in military contexts. An important mechanism for integrating privacy concerns in the development and introduction of new technologies into military use is the legality review afforded Article 36 of API.

Given the privacy implications of all three technologies discussed in the chapter—the reliance of autonomous weapons on extensive surveillance and data collection, the corrosive effects of cyber operations on cyber security and data protection, and the potentially dramatic intervention

118 For an overview, see Douglas Holdstock, Jack Piachaud & Robin M. Coupland, *The SIrUS Project towards a Determination of Which Weapons Cause "Superfluous Injury or Unnecessary Suffering,"* 14 Medicine, Conflict & Survival 243 (1998). For a critical view on this project, see Donna Marie Verchio, *Just Say No—The SIrUS Project: Well-Intentioned, but Unnecessary and Superfluous*, 51 A.F. L. Rev. 183 (2001).

119 Daoust et al., *supra* note 26, at 353; Holdstock et al., *supra* note 118.

120 Robin Coupland (ed.), The SIrUS Project: Towards a Determination of Which Weapons Cause "Superfluous Injury or Unnecessary Suffering" 13 (1997).

121 *See* Bensaid v. United Kingdom, App. No. 44599/98, Eur. Ct. H.R. ¶ 47 (2001); Vasileva v. Bulgaria, App No. 23796/10, Eur. Ct. H.R. ¶¶ 63–69 (2016).

in the bodies and minds of enhanced persons—Article 36 reviews are arguably warranted for all three types of technologies, albeit under different Article 36 categories (weapons, means, methods). Such reviews would need to delineate possible harms and consider safeguard measures and the circumstances that would justify use. Ultimately, a new privacy impact assessment methodology would need to be developed, covering difficult issues such as consent, long-term harm, and indirect harms so as to usefully utilize Article 36 legality reviews to effectively protect the right to privacy.

Chapter 3

LOAC and the Protection and Use of Digital Property in Armed Conflict

Laurie R. Blank[1] and Eric Talbot Jensen[2]

INTRODUCTION

Data protection is one of the catchphrases of contemporary society and an essential component of individual privacy and the smooth and secure functioning of societies and economies. Digital property refers to any information in digital form, whether online or housed in an electronic storage device, and can include images, text, sounds, and video. As commonly understood, data protection refers to the process of and efforts to secure and safeguard such digital property from loss, corruption, or compromise, whether inadvertent or due to the nefarious actions of other actors. The need to preserve and protect such digital property does not disappear during armed conflict; in fact, it may well be stronger in the face

1 Clinical Professor of Law; Director, Center for International and Comparative Law; Director, International Humanitarian Law Clinic, Emory University School of Law.
2 Robert W. Barker Professor of Law, J. Reuben Clark Law School, Brigham Young University.

of efforts by the adversary, criminals, or other opportunistic actors to take advantage of the chaos of conflict and gain access to such information.

Data is also critical to strategic, operational, and tactical decision-making and action during armed conflict. Militaries rely on data for targeting analysis and decisions; for assessing proportionality and other precautionary obligations; for evaluating the strength, weaknesses, and capabilities of the adversary; for humanitarian purposes; and for many other considerations. Any cyber operations inherently use, manipulate, or, at a minimum, encounter digital property or the storage or transit mechanisms for such property. The increasing reliance on new and emerging technologies, including machine learning, during military operations and conflict only reinforces the importance of analyzing and understanding the appropriate parameters for the protection and use or exploitation of data during armed conflict.

Although the Tallinn Manual and other recent literature have briefly examined the treatment of data and digital property in the context of cyber operations and issues during armed conflict, a more focused analysis of how the law of armed conflict's (LOAC) rules on the protection of property—including seizure and destruction, requisition and other uses of property—apply to data and digital property can provide needed clarity. Treaty law setting forth the protections for property and the limits on seizure or destruction of property during military operations first appeared in the Hague Conventions of 1899 and 1907, which sought to prevent total war and minimize war's destructive impact on civilian property and infrastructure. Applying the law in the context of digital property may not, however, be as simple as translating the rules from buildings to bytes. It introduces questions about the meaning of terms such as property, seizure, destruction, war booty, and others in the digital context. In addition, as with physical property, effective implementation of the law requires analysis not only from the perspective of the needs and rights of individuals to protect and continue to have use of and access to their data but also in light of the military and operational needs of warring parties to use, seize, and restrict access to data for military purposes.

Part I of this chapter identifies and frames the key issues, including the type of operations in question and the relevant actors and users of digital property in such situations. In addition, this part briefly provides background on the relevant law of armed conflict rules governing the seizure, destruction, and requisition of property during conflict and the core preliminary question of whether data constitutes property for purposes of the legal rules. Part II of this chapter then examines how

each of the main legal rules applies in the digital space. A first question, for example, concerns the types of actions with respect to data that constitute pillage and the types of data or digital property that fall within the meaning of war booty as understood in customary international law. Second, Part II analyzes the meaning and application to digital property of Article 23(g) of the 1907 Hague Convention on the seizure and destruction of property, including, for example, whether copying or a loss of functionality or access constitutes seizure and whether manipulation of data could constitute destruction as traditionally understood. Finally, given the extensive and increasing demand for data for many core functionalities in military operations, the parameters for requisition of and access to data are equally critical.

I
FRAMING THE ISSUE

A WHO AND WHAT

With the onset of the digital age, the transition of information to digital sources has become an ever-increasing fact of modern life. One recent study found that at the beginning of 2020, there were 44 zettabytes—that is, 44,000,000,000,000,000,000,000 bytes—of data in the world. This means that the number of bytes in the world is "40 times bigger than the number of stars in the observable universe."[3] This number is estimated to more than triple by 2025. This vast transition of information to electronic data significantly impacts society in general, dramatically increasing the ease of access to virtually all sources of information. In addition, data is not only the substantive content that can be transformed into information readily accessible to humans but also includes the "'raw material' needed by computer systems to function."[4] Heather Harrison Dinniss has helpfully described these two categories of data as content-level data—the type of data that transforms into readily useable information—and operational-level data—the data that provides

3 Jeff Desjardins, *How Much Data Is Generated Each Day?* WORLD ECONOMIC FORUM, Apr. 17, 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

4 Robin Geiss & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INT'L. L. STUD. 556, 560 (2021).

functionality and the ability to perform specific tasks.[5] The internet, the primary tool to access this information, was built on the foundational premise of access superseding security.

Against this backdrop, the potential use of data in armed conflict has also taken on increased significance, and the value of data to warring parties is unquestioned. Examining the legal protections for such data and the parameters for any action to use, destroy, or capture such information is therefore essential. The enormous growth of and interest in cyber capabilities over the past two decades has led to a robust academic and practitioner literature analyzing the application of international law to attacks and other uses of force in the cyber arena.[6] Such analysis includes examination of what constitutes a lawful target of attack in cyberspace or by cyber means and how to assess and minimize incidental harm to civilians and civilian property in the course of such attacks (otherwise commonly known as collateral damage). However, the literature has paid little, if any, attention to protections for and use or exploitation of digital property beyond the conduct of hostilities and attacks, the subject of this chapter. Analyzing how the law of armed conflict applies to the seizure and destruction of digital property does not address attacks, the deliberate and incidental consequences of such actions, or the precautions required to mitigate the risk to civilians. Rather—and importantly for the proper application of the law—the rules on seizure and destruction of property discussed below apply outside the context of attacks, such as the clearing of property to enable passage of military vehicles or other actions to provide support for military operations. Countless actions taken with respect to data and other digital information fall within this broader category of actions outside of attacks, such as the seizure or erasure of military or government data, the manipulation of images for propaganda purposes, or the exploitation or destruction of civilian medical records, tax records, or other information integral to everyday life.[7]

In addition to the type of data and how it might be used or destroyed, another important question in exploring the legal framework is who

5 Heather Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 Isr. L. Rev. 39, 41 (2015).

6 *See generally* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2017); Ashley Deeks, Noam Lubell & Daragh Murray, *Machine Learning, Artificial Intelligence, and the Use of Force by States*, 10 J. Nat'l Sec. L. & Pol'y 1, 5 (2019); Geiss & Lahmann, *supra* note 4, at 560.

7 *See, e.g.*, Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 Int'l L. Stud. 395, 400 (2021) ("For this reason, practices such as certain types of electronic warfare, psychological warfare, economic sanctions, seizure of property, and detention have never been considered to be attacks as such, and, accordingly, were not considered as subject to LOAC targeting rules.").

might interact with such data during armed conflict. A range of actors is likely to have an interest in various types of data in times of armed conflict. For example, consider the data containing details on the sewer and other underground utilities. An attacker, whether state or non-state, would be interested in securing this data for many reasons, including identifying the location of specific utility lines for both targeting and non-targeting, as well as sewer lines and other transit-capable lines to be able to interdict potential underground warfare.[8] In addition to the

attacker, others would also be interested in access to and the protection of that data, including: (1) defending forces for similar reasons as the attacker; and (2) the creators of the data, such as: (a) the administrator of the system upon which the data exists; and (b) the individuals or entity responsible for securing that data, in order to preserve this data from destruction or exploitation by one or both sides of the conflict. Many other individuals, groups, or entities would be anxious to either have access to or prevent access to various forms of data. In terms of pertinent legal categories, interested parties involve a broad spectrum that includes combatants or fighters, civilians who are directly participating in hostilities on either a one-time or recurring basis, members of organized armed groups, criminal enterprises, civilians assisting one side of a conflict, and non-participating civilians whose data may be at risk. In addition, humanitarian relief organizations and other external actors will have relevant goals and interests with respect to their own data and that of others.

B THE LAW

The law of armed conflict regulates the treatment and disposal of property during armed conflict. In particular, both treaty and customary international law prohibit the destruction or seizure of enemy property unless imperatively demanded by the necessities of war, prohibit pillage, set rules for the requisition of property by military forces, and provide for the capture of war booty.[9] Part II of this chapter below examines each of these rules regarding the use or abuse of property in the specific context of digital property, highlighting key issues and challenges in how these long-standing rules apply in this contemporary and quickly evolving domain.

8 *See generally* Daphné Richemond-Barak, Underground Warfare (2019).
9 *See generally* William Gerald Downey, Jr., *Captured Enemy Property: Booty of War and Seized Enemy Property*, 44 AM. J. Int'l L. 488 (1950).

First, the law forbids pillage in all types of conflict, whether international or non-international. Pillage is the act of taking, for private or personal use, any public or private property belonging to the enemy State; to wounded, sick, or shipwrecked persons; or to prisoners of war by a party to an armed conflict.[10] Pillage is generally synonymous with looting and plunder, and most military manuals treat all three acts in an identical manner.[11] In addition, international courts adjudicating charges of pillage post-World War II have not limited the crime to members of armed forces but have included non-state actors and entities.[12]

A soldier who takes a camera from a civilian or prisoner of war and keeps it for her own use therefore commits the war crime of pillage. In contrast, seizure of enemy property for use by the armed forces is permissible when that property falls within the meaning of war booty. Customary international law has long permitted a party to an international armed conflict to seize as war booty all enemy public movable property and any enemy private movable property that is "susceptible to direct military use."[13] Public property is property that belongs to the State or an agency of the State, such as any military or government property. Although private property is protected from seizure as a general rule, any such property that is susceptible to direct military use, such as "arms, ammunition, military papers or property that can be used as military equipment (e.g., as a means of transportation or communication),"[14] can be captured as war booty. During non-international armed conflict, however, the law includes no provision for the capture of property as war booty.

With regard to the seizure and destruction of property, the primary rule appears in Article 23(g) of the Hague Regulations of 1907, which states that it is forbidden to "destroy or seize the enemy's property, unless

10 *See* Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land arts. 28, 47, Oct. 18, 1907, 36 Stat. 2277, T.S. 539 [hereinafter Hague IV]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 33(2), 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]; Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 4(2)(g), June 8, 1977, 1125 U.N.T.S. 609; Rome Statute of the International Criminal Court, art. 8(2)(b)(xvi), July 17, 1998, 2187 U.N.T.S. 90; Australian Defence Force, Law of Armed Conflicts—Commander's Guide ¶¶ 743, 1224; Office of the Judge Advocate, Canadian Armed Forces, The Law of Armed Conflict at the Operational and Tactical Level, at 12–18; OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 5.17.4.1 (2015, rev'd Dec. 2016) [hereinafter DOD LAW OF WAR MANUAL].

11 Christopher D. Greulich & Eric Talbot Jensen, *Cyber Pillage*, 26 SOUTHWESTERN J. INT'L L. 264, 267 (2020).

12 *Id*. at 278.

13 DOD LAW OF WAR MANUAL, *supra* note 10, § 5.17.3. *See also* LAUTERPACHT, II OPPENHEIM'S INTERNATIONAL LAW 406 (§144) ("Private enemy property on the battlefield is no longer in every case an object of booty. Arms, horses, and military papers may indeed be appropriated, even if they are private property, as may also private means of transport, such as cars and other vehicles which an enemy may make use of.").

14 DOD LAW OF WAR MANUAL, *supra* note 10, § 5.17.3.

such destruction or seizure be imperatively demanded by the necessities of war."[15] Commonly accepted justifications for seizure or destruction of property imperatively demanded by the necessities of war include actions that provide support for military operations or diminish the enemy's ability to conduct or sustain military operations. In contrast, wanton or extensive destruction of property not justified by military necessity is a grave breach of the Geneva Conventions and a war crime.[16] Any destruction of property thus must have a reasonable connection to the effort to overcome the adversary—"[d]evastation as an end in itself or as a separate measure of war is not sanctioned by the law of war."[17] Destruction or seizure of property will be accepted as "imperatively demanded by the necessities of war" when it contributes to military operations or hampers or neutralizes the adversary's ability to pursue its own military objectives or campaign. Consider, for example, the seizure of trucks, railroad cars, or other means of transportation to transport supplies or troops, or destroying buildings or cutting down trees to deny the enemy cover or to clear a field of fire.[18] In essence, the rules on seizure and destruction of property balance the goal of having war "affect private citizens and their property as little as possible"[19] with the recognition that, in armed conflict, "military necessity justifies behaviour (seizure and destruction of property) which otherwise would be unlawful."[20]

Finally, during occupation, although the occupying party may not seize private enemy property, it may requisition such property to fulfill the needs of the occupying forces. Any property deemed necessary for the maintenance of the army may be requisitioned, such as "fuel, food, clothing, building materials, machinery, tools, vehicles, or furnishings for quarters."[21] The occupying power must either pay for the requisitioned property in cash at the time of the requisition or provide a receipt and subsequent payment as soon as possible.

15 Hague IV, *supra* note 10, art. 23(g). The First, Second, and Fourth Geneva Conventions also include rules to this effect. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 33, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, arts. 22–25, 27–28, 38–39, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention IV, arts. 18, 19, 53.

16 Geneva Convention 1, art. 50; Geneva Convention II, art. 51; Geneva Convention IV, art. 147; Statute of the ICTY, art. 2(d); Rome Statute of the International Criminal Court, arts. 8(2)(b)(xiii), 8(2)(e)(xii), July 17, 1998, 2187 U.N.T.S. 90.

17 Department of the Army, FM 27–10, The Law of Land Warfare ¶ 56 (1956) (Change 1976).

18 DoD Law of War Manual, *supra* note 10, § 5.17.2.2.

19 Partial Award—Civilians Claims, Eritrea's Claims 15, 16, 23 & 27–32 ¶ 125, Eri-Eth. Cl. Comm. (2005).

20 Michael N. Schmitt, Charles H.B. Garraway & Yoram Dinstein, The Manual on the Law of Non-International Armed Conflict with Commentary 55 (2006), http://www.dur.ac.uk/resources/law/NIACManualIYBHR15th.pdf.

21 FM 6-27/MCTP 11-10C, The Commander's Handbook on the Law of Land Warfare, ¶ 6–103 (2019).

II
USE AND PROTECTION OF DIGITAL PROPERTY

As the brief background on the law above highlights, these rules regarding the protection, destruction, and seizure of property center on the concept of property and, more specifically, "enemy property." Enemy property includes both public and private property, whether movable or immovable. International law does not include a specific definition of enemy property,[22] but the term is generally understood to mean the property of the adversary in the armed conflict. Such property is generally on the territory of the adversary State or "belong[s] to individuals or entities aligned with or with allegiance to a party to the conflict adverse or hostile to the perpetrator."[23]

To apply this existing treaty law to cyber data effectively, determining whether cyber data equates to "property" as contemplated in these legal documents is an essential predicate.[24] However, neither treaty commentaries nor international or domestic jurisprudence offer any guidance on this question. The Tallinn Manual does consider the nature of digital data, predominantly with respect to whether it constitutes an "object" with respect to the law of armed conflict and targeting, a critical issue for the application of the core principles of distinction, proportionality, and precautions. The majority of participating experts determined that data is not an object,[25] sparking extensive debate among scholars and practitioners supporting[26] and arguing against[27] the manual's conclusions. Unfortunately, few States have commented directly on this issue, providing little help in advancing the debate.[28] Although the question of

22 Note that the First, Second, and Fourth Geneva Conventions refer not to "property of the adversary" but to "property protected by the Convention." Geneva Convention I, art. 50; Geneva Convention II, art. 51; Geneva Convention IV, art. 147.

23 Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui, ICC-01/04-01/07, Decision on Confirmation of Charges, ¶¶ 310 (Int'l Crim. Court, Sept. 30, 2008).

24 *See* Geiss & Lahmann, *supra* note 4, where they argue that only "content level data" presents difficult issues and that operational-level data should be understood as an operation not against data but rather against the system itself.

25 TALLINN MANUAL, *supra* note 6, cmt. to r. 100, ¶ 6, at 437.

26 Geiss & Lahmann, *supra* note 4, at 566–67; Ori Pomson, *'Objects'? The Legal Status of Computer Data under International Humanitarian Law*, Mar. 1, 2021, https://ssrn.com/abstract=3795479 or http://dx.doi.org/10.2139/ssrn.3795479.

27 Dinniss, *supra* note 5; Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISR. L. REV. 55 (2015).

28 *See* Schöndorf, *supra* note 7, at 401; NORWAY, CHIEF OF DEFENCE, MANUAL OF THE LAW OF ARMED CONFLICT 210 (2013) 210; DANISH MINISTRY OF DEFENCE, MILITARY MANUAL ON INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS 292 (Jes Rynkeby

property for the instant discussion of the law of armed conflict's rules on seizure and destruction is broader, with "object" a subset of property, the Tallinn Manual's analysis regarding the status of data as an object is instructive, as are subsequent developments in the intervening decade.

The Tallinn Manual experts focused on the "intangible" nature of data and argued that, as a result, data "[n]either falls within the 'ordinary meaning' of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary."[29] In contrast, the minority of the experts argued that, "at a minimum, civilian data that is 'essential' to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such."[30] This decision carries significant import. "If data is an object, the rule on distinction applies and international humanitarian law prohibits the targeting of civilian data in the context of an armed conflict. If data does not constitute an object, the targeting of data *per se* is not unlawful and the rule on distinction does not apply."[31] Critically, for those identifying data as an object, "the limitation with the majority position is not that military code cannot be targeted. Rather, it is that civilian code can also be targeted. Because the majority does not consider code an object, the law of targeting does not apply to operations directed against it."[32]

The Tallinn Manual experts took a similar approach—and were also split in a debate—with respect to data as property. For similar reasons as those noted above with respect to data as object, a majority determined that "*sensu stricto*, data does not qualify as property."[33] This, of course, does not mean that data has no protections. Some indirect protection accrues to data at rest, because cyber infrastructure such as computers and servers receives protection as property. As with the question of whether data is an object, a minority of the experts argued that "data can qualify as property."[34]

Ten years after those initial discussions, it is unclear whether the Tallinn Manual experts would reach the same conclusion on either data as object or data as property. The International Committee of the Red

Knudsen ed., 2016); Ministère des Armées de France, *Droit international appliqué aux opérations dans le cyberespace* 16 (2019); Ori Pomson, *'Objects'? The Legal Status of Computer Data under International Humanitarian Law*, Mar. 1, 2021, https://ssrn.com/abstract=3795479 or http://dx.doi.org/10.2139/ssrn.3795479.

29 TALLINN MANUAL, *supra* note 6, cmt. to r. 100, ¶ 6, at 437.

30 *Id*. cmt. to r. 100, ¶ 7, at 437.

31 Tim McCormack, *International Humanitarian Law and the Targeting of Data*, 94 INT'L L. STUD. 222, 227 (2018).

32 *Id*. 232.

33 TALLINN MANUAL, *supra* note 6, cmt. to r. 149, ¶ 3, at 550.

34 *Id*.

Cross takes a more inclusive approach, arguing that "data belonging to certain categories of objects… enjoy specific protection under IHL," with specific mention of data belonging to medical facilities.[35] Some of the Tallinn Manual experts have expressly changed their views with regard to the nature of data as an object since the first Manual was published.[36] In addition, although the general consensus appears to be that digital information is not property as so understood for domestic law purposes,[37] courts in several countries have begun to affirm that digital information is property within the context of criminal law and other relevant legal regimes. These developments may demonstrate a shift in the understanding of how to conceptualize data and digital information in the context of longstanding legal frameworks, definitions, and categories. For example, the Supreme Court of New Zealand held in 2017 that digital information is property because "digital files can be identified, have a value and are capable of being transferred to others. They also have a physical presence, albeit one that cannot be detected by means of the unaided senses."[38]

States have not expressed any consensus on the nature of digital information as property in the context of international law generally or the law of armed conflict specifically. Given the strong minority view favoring the treatment of data and digital information as property and the apparent trend in this direction and towards greater recognition of protections for data, this chapter examines the application of the relevant law of armed conflict rules as if data is, or will soon be, considered property during times of armed conflict.

A PILLAGE AND WAR BOOTY

As stated above, pillage is "the non-consensual taking of public or private property… during armed conflict for private or personal use."[39] Members of a State's armed forces, of non-state organized armed groups,

35 Int'l Comm. Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 97 INT'L REV. RED CROSS 1427, 1478 (2016).
36 McCormack, *supra* note 31, at 240.
37 *See, e.g.*, Oxford v. Moss, (1979) 68 Cr App R 183 (QB); R v. Stewart, [1988] 1 SCR 963; TS & B Retail Systems Pty Ltd v. 3Fold Resources Pty Ltd (No 3) [2007] FCA 151. For a detailed discussion, see João Marinotti, *Tangibility as Technology*, 37 GA. S. UNIV. L. REV. 671, 723 n. 238 (2021).
38 Dixon v. R [2015] NZSC 147, [2016] 1 NZLR 678, at 25. Several efforts at proposed legislation in the United States have sought to establish property rights in data, such as the "Own Your Own Data Act of 2019" introduced by Senator John Kennedy or California governor Gavin Newsom's proposed "data dividend." Cameron F. Kerry & John B. Morris, Jr., *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, Brookings Institution, June 26, 2019, https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.
39 Greulich & Jensen, *supra* note 11, at 267.

of transnational terrorist and criminal groups, and even individuals and corporations can be guilty of pillage. Thus, not only would a uniformed member of United States Cyber Command (CyberCom) who steals private digital data for personal use during an armed conflict be prosecutable for pillage, but a civilian employee of the National Security Agency (NSA) would also be guilty of such an offense. Indeed, a government contractor working for a private cyber company that is contracted to the US government would also be potentially guilty of pillage if he or she committed the same type of act with a nexus to the armed conflict.

For example, consider that during an armed conflict between State A and State B, a defense contractor in State B is shipping defense goods and articles to its military to assist with operations, and State A's cyber team hacks into the contractor's computer systems to disrupt the shipping of goods by deleting or corrupting the tracking data for military shipments. While in the defense contractor's systems, a member of the cyber team uncovers computer data containing trade secrets for certain items that the contractor produces.

If the member of the cyber team took those trade secrets and then sold them for private gain, he or she would be guilty of pillage: the trade secrets are the private property of the defense contractor, and the cyber operator takes that property for personal gain. Questions that could arise here include the meaning of "taking" digital property: does "taking" include only the removal of such digital property such that it no longer exists in the original server, file, or other storage capacity, or does it also include copying the digital information in order to use it for personal gain while still leaving its original content in its original location? The purpose of the prohibition of pillage strongly suggests that both scenarios fall within the meaning of taking property, because both involve the undesirable and prohibited act of private gain.

In contrast, if the cyber operator instead removes or copies trade secrets or other digital information for the development of weapons or for supply chain logistics on behalf of State A (i.e., does not keep or sell such data for private gain), such digital property would constitute war booty and would—at least in this international armed conflict between State A and State B—be lawful. Any such data that belongs to State B is automatically war booty as enemy public property, and if the data belongs to the defense contractor, both weapons data and supply chain logistics are "susceptible to direct military use"[40] and become war booty. If, for

40 DoD Law of War Manual, *supra* note 10, § 5.17.3 (2015, rev'd 2016).

example, the Taliban's reported seizure of biometric data during and after the United States withdrawal had occurred during an international armed conflict, it would constitute war booty—public enemy property seized on the battlefield. Property lawfully taken as war booty becomes the property of the capturing state; it does not need to be returned and may even be destroyed.[41] As another example, if State A's operators hack into State B's government cryptocurrency wallet and transfer the cryptocurrency into State A's government account, such data-taking would be considered war booty, not theft, and would not be a violation of international law. In the context of digital information, the notion of war booty thus becomes enormously consequential—a state that acquires data belonging to its adversary state may keep it, a significant boost to its own capabilities, or may destroy it altogether, at equally significant cost to the adversary. Measures to protect such data, and to encourage or even require equivalent protection of private data that is "susceptible to direct military use," are therefore essential, indeed existential, in contemporary and future conflicts.

B SEIZURE AND DESTRUCTION

The question of whether data and other digital information constitutes property within the meaning of the law of armed conflict is of particular consequence for the law's broader proscriptions on the seizure and destruction of property. The basic rule, as stated above, is that the seizure or destruction of property outside the context of attacks is prohibited unless imperatively demanded by the necessities of war. If data is not property, the Hague and Geneva proscriptions[42] will not apply to the seizure or destruction of any data, regardless of whether it is public or private, or military or non-military in use, leaving States and other parties to armed conflict free to do so pending some other explicit prohibition. In effect, if data is not property, the law does not appear to prohibit a State or other conflict actor from taking any data from the enemy State or private persons or entities during armed conflict and using it for its own purposes. Similarly, the restraints of Hague and Geneva would not preclude the destruction of any data—the LOAC obligations mandating protection for civilian property during targeting or during

41 Int'l Comm. Red Cross, Customary International Humanitarian Law, Rule 49.
42 *See supra* note 10.

military operations more generally would not protect data from damage or destruction, since data is not property and thus does not fall within the ambit of the rules. Article 57 of Additional Protocol I's constant care obligation would offer some protection where restraint with respect to data is relevant to "spar[ing] the civilian population, civilians and civilian objects,"[43] for all Additional Protocol I treaty parties and all States to the extent that the provision reflects customary international law. However, the general restraints on the conduct of attacks found in the remainder of Article 57, as well as the obligation to take feasible precautions against the effects of attacks found in Article 58, would not strictly apply, leaving data in a precarious position, as noted above.

Assuming, however, that States may come to consider data to be property, the LOAC prohibits the seizure and destruction of data unless imperatively demanded by the necessities of war. Notably, as explained above, the rules for seizure and destruction do not apply to objects that qualify as military objectives or to incidental harm caused in the context of an attack on a lawful military objective. Thus, for example, if data is indeed an object, then data meeting the definition of a military objective, such as military troop movements or weapons development plans or schedules, falls outside the scope of this rule and can be attacked in accordance with the core principles of targeting. Similarly, incidental erasure or damage to civilian data in the course of such attack is not unlawful as long as such damage is not excessive in relation to the military advantage gained from the attack.

Many other types of digital information might be susceptible to destruction or seizure in the course of conflict but do not qualify as military objectives. For example, one party to a conflict might seek to seize data on local utilities and location of utility infrastructure for use as it advances into enemy territory, or might destroy meteorological data to hamper the adversary's planning. Applying the LOAC's rules—primarily set forth in Article 23(g) of the 1907 Hague Regulations—to the protection of such digital property thus requires an analysis of the meaning of three terms with respect to data: destruction, seizure, and "imperatively demanded by the necessities of war."

Destruction includes acts such as demolishing, destroying, or otherwise damaging property. An action that wipes away certain data should

43 Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 57(1), June 8, 1977, 1125 U.N.T.S. 3. *See also* Asaf Lubin, *The Duty of Constant Care and Data Protection in War*, *in* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD (Berg & Dickinson, eds., forthcoming, 2022).

qualify as demolishing or destroying in the context of digital information: the information existed, and then it did not. Damaging may be a more elusive concept and could include corrupting or manipulating the data but leaves open questions of temporality and repairability, issues with which the Tallinn Manual experts wrestled in considering the level of cyber action constituting an attack.[44] For example, a state planning to attack and take control of the adversary's main airfield might seek to disable the traffic lights on the surrounding streets in order to clog the roads and slow down the adversary's ability to muster forces in response. Deleting the data altogether would fall within the meaning of destruction, but other avenues for altering data, such as adjusting the timing indicators, corrupting the sensors, or other actions, require further inquiry in considering whether they would constitute damage or destruction.

More challenging, perhaps, is how to apply the notion of "seizure" to digital information. Although no formal definition of "seizure" appears in treaty or case law, the term is generally accepted to refer to the custody or use of property, such as by appropriation or control, a relatively straightforward concept for physical items. One might gain control of data in a variety of ways beyond or in a different manner than this physical concept of taking custody, however, such as using, copying, corrupting, or preventing access to it. An action that prevents the original owner from using or accessing the data, such as encryption or changing passwords, should fall squarely within the notion of seizure, including when such actions are temporary or episodic. The use, copying, manipulation, or corruption of data is a harder question, because the original owner seems to still have access to the data in some fashion. By a strict and technical interpretation of seizure, such actions might be excluded, but a more purpose-driven interpretation based on the LOAC's goal of minimizing the effect and dangers of war for the civilian population could properly encompass such acts.

The generally accepted understanding of "imperatively demanded by the necessities of war"—supporting military operations or diminishing the enemy's ability to conduct such operations—is likely to encompass large categories, types, and quantities of data, including any digital information regarding infrastructure, population movements, or personal identifying information. Consider the example above with the traffic lights en route to the airfield. The traffic-light data is not a military objective

44 TALLINN MANUAL 2.0, *supra* note 6, cmt. to r. 92, ¶ 10, at 417 (after "extensive discussion," a majority was of the view that "interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components").

and cannot be attacked, but its destruction or damage surely contributes to diminishing the adversary's ability to conduct operations. Similarly, if State A is occupying State B, the seizure of digital maintenance records of key infrastructure, or the local criminal and prison records, would be necessary for State A to fulfill its role as occupying power. Similarly, when taking the obligatory feasible precautions in launching an attack that might affect a water treatment plant, the attacker would want information regarding that infrastructure, or information regarding sewers and subway tunnels for any subterranean maneuvers or to protect individuals in underground shelters. Actions going far beyond this criterion of "imperatively demanded by the necessities of war," such as deleting or destroying all banking data throughout the country, for example, would violate the prohibition on wanton or extensive destruction of data not justified by military necessity, thus constituting a war crime and a grave breach of the Geneva Conventions.

C REQUISITION

The rules on requisition mirror those of seizure, with the exception that they apply to private property in occupation and require immediate payment or a voucher. As with seizure, the Tallinn Manual experts concluded that data was not property with respect to requisition,[45] meaning that an occupying force that took data from private entities would ordinarily not have to comply with the rules on compensation for requisition of private property.[46] However, if data is considered to be property, or becomes considered as property, the rules on compensation would apply. For example, when State A is occupying a portion of State B, if State A wanted to gather historical commercial consumption data from a retail store in order to continue to provide a steady stream of goods for the civilians in occupied territory, then State A would be required to purchase that data at market price.

Once data has been requisitioned (or seized as discussed above) lawfully under the applicable law, that data can be put to use as described previously. However, it is important to note that at some point after requisition (or seizure), obligations may arise with respect to the disposition of that data by way of human rights law, as discussed elsewhere in this volume.

45 *Id.* cmt. to r. 149, ¶ 3, at 550.
46 *Id.* ("[T]his fact [that data is not property] does not preclude the Occupying Power from making use of State data for its military operations.").

LOOKING FORWARD

The growing use of new and emerging technologies and the essential role of data in both everyday life and armed conflict only serve to emphasize the need for further research and discourse regarding the protection and use of digital information during armed conflict. As a starting point, the protections for certain categories of data—based on its use or nature, regardless of whether it falls within the definition of property—may offer lessons for the development of further granularity across all types of digital information. These existing protections for medical data, the data of POWs and civilian internees, digital cultural property, and the data of neutrals are integral to the fulfillment of the LOAC's core purposes of protecting those not involved with the conflict and those who are *hors de combat*, as well as ensuring the preservation of functions and services essential to the civilian population. Several of the other chapters in this volume highlight specific issues in this regard, laying the foundation for further research and analysis in the future.

First, medical data and "data that form an integral part of the operations or administration of medical units and transports" is protected at all times.[47] For example, if a State involved in an international armed conflict aims to undermine the confidence of the adversary State in its medical records, including its blood typing, gaining access to the medical records of individuals in that State and changing the blood type would be a violation of the LOAC. Indeed, accessing the data and not changing it but leaving the impression that the information was corrupted would also be unlawful.

Second, data collected as part of the internment of civilian internees or detention of prisoners of war must be protected from disclosure and maintained separately from other data that may be targetable as a military objective.[48] Such protections include the data containing information at initial in-processing and throughout the internment, as well as data concerning the location of the remains of deceased persons.

A third area of current protection for data in the LOAC is cultural property. Notwithstanding the continued uncertainty regarding the status of data as property for the purposes of the LOAC, a majority of the Tallinn

47 *Id.* cmt. to r. 132, ¶ 3, at 515.
48 *Id.* cmt. to r. 135, ¶ 4, at 521. *See also* Emily Crawford's chapter in this volume.

Manual experts argued that "digital manifestations of cultural property are entitled to … protection… when the original is either inaccessible or has been destroyed."[49] In this case, the data comprising the digital manifestation would be protected, not necessarily because it is data, but because it comprises cultural property.

Finally, any use or destruction of, or damage to, a neutral country's data, regardless of whether it is characterized as property, would likely amount to a violation of neutrality in accordance with the rules on neutrality during international armed conflict. As the Tallinn Manual explains, the violation of a neutral country's cyber infrastructure or a neutral country allowing use of its cyber infrastructure by a belligerent would violate the doctrine of neutrality.[50] Presumably, neutral data would also fall within this rule. Consider, for example, an armed conflict between State A and State B, during which a computer engineering company in neutral State C sells computer software to State B. If State A hacks into the computer engineering company in State C and inserts malware into the software that will be sold to State B in order to infect State B's government computer systems, State A would be violating international law.

Looking forward, further exploration and analysis of the LOAC's rules on the use, seizure, and destruction of digital property during armed conflict will be important for protecting the rights and needs of individuals with respect to their own digital information and for determining the appropriate parameters governing the rights and obligations of parties to armed conflict in terms of using, destroying, seizing, or restricting access to digital information.

49 *Id*. cmt. to r. 142, ¶ 6, at 535.
50 *Id*. cmt. to r. 150–53, at 553–61.

Chapter 4

From Telegraphs to Terabytes: The Implications of the Law of Neutrality for Data Protection by "Third" States and the Corporations Within Them

Jacqueline Van De Velde [1]

INTRODUCTION

Parties to a conflict[2] are increasingly recipients of data or internet-related services from technology companies situated in States otherwise unconnected to the conflict. Social networks must consider whether to moderate content in situations where the laws of war (international

1 Jacqueline Van De Velde is an associate at King & Spalding, LLP. The author's views are her own.
2 For the purposes of this chapter, a "conflict situation" is a situation where international humanitarian law applies and could therefore include instances of occupation. Although neutrality law is formally only triggered by international armed conflicts, recent scholarship has suggested its application to non-international armed conflicts, which we also consider.

humanitarian law) may be applicable; technology companies selling data storage/processing tools must assess the implications of their use by belligerents; and technology companies must evaluate State-issued customer data requests, ranging from subpoenas to national security requests.[3] In such scenarios, the State receiving the data or service is typically *other* than the one where the technology company is headquartered, data is stored, or from whence a response travels. In international legal parlance, the company is situated in a "third" State.

Because data transfer impacts the digital rights—including privacy and data protection — of those whose data is requested or used, it is critical to determine the international legal obligations owed by States where a corporation is headquartered or stores data. Beyond the perennial issue that some States disclaim extraterritorial human rights obligations, corporate involvement complicates or limits the application of human rights law, given attribution issues and less-defined corporate responsibility. Uncertainties are especially pronounced for positive human rights and due diligence obligations.

A longstanding, albeit "slightly musty,"[4] area of international humanitarian law — the law of neutrality — is well-configured to address such limitations, but its application remains unexplored.[5] As a doctrine, neutrality law originated to define the legal relationship between belligerents and third parties. Because it is triggered by the existence of armed conflict,[6] it provides a provenance of obligation that *must* be turned to. But in addition, neutrality law *should* be turned to, given its historic concern with private actors (including those involved with the high tech of the time, e.g., telegraph towers and submarine cables). Never mind that,

3 *See, e.g.*, Kim Lyons, *Myanmar Orders Internet Providers to Block Twitter and Instagram in the Country,* The Verge, Feb. 6, 2021, 10:10AM EST, https://www.theverge.com/2021/2/6/22269831/myanmar-orders-block-twitter-facebook-instagram-military-coup#:~:text=%E2%80%9CAll%20mobile%20operators%2C%20international%20gateways,company%20Telenor%20said%20in%20a; Ellen Nakashima, *Report: Web Monitoring Devices Made by U.S. Firm Blue Coat Detected in Iran, Sudan*, WASHINGTON POST, July 8, 2013, https://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html. *Compare* Facebook, *Government Requests for User Data*, https://transparency.facebook.com/government-data-requests (noting that between January and June 2020, Facebook received 173,592 total requests for data, including requests from India (33,374), Pakistan (1,358), Ukraine (9), and Iraq (9)), *with* Rule of Law in Armed Conflicts, *Conflicts*, GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS, https://www.rulac.org/browse/conflicts (recording international armed conflicts between India and China, between India and Pakistan, and in Ukraine, Iraq, and Syria).

4 *See* Committee for the Red Cross, *Neutrality in Cyber War*, https://www.law.berkeley.edu/files/Neutrality_in_Cyber_War_for_web.pdf.

5 Notably, neutrality law has been discussed in great detail in the context of cyber operations, and in particular the extent to which IHL applies to them. However, cyber attacks are only one example of the type of conflict issues that implicate digital rights. A broader examination of the role of neutrality and digital rights in respect to armed conflict situations is thus warranted.

6 *See* Rebecca Ingber, *Untangling Belligerency from Neutrality in the Conflict with Al-Qaeda*, 47 TEX. INT'L L. J. 75, 79 (2011).

at the time of the doctrine's conception, belligerents and neutrals were telegraph operators and kings: when technology companies transfer data or provide services from a neutral State to an entity in a belligerent State, the same legal relationship is in play. Just as importantly, neutrality law clarifies the scope and content of States' obligations and rights towards private actors. This chapter is the first to address the operation of neutrality principles in relation to data transfer affecting digital rights in conflict situations, as well as to import the doctrine concerning private actors into this context.

This chapter examines four aspects of neutrality law applied to data transfer. *First*, it analyzes two threshold issues: the extent to which: (a) digital goods can be analogized to instruments of warfare, as recognized under neutrality law (e.g., data transfer to telecommunications, data processing tools to munitions,[7] and social networking to something in between); and (b) neutrality law's utility in digital spaces, versus traditional territorial divisions.[8]

Second, this chapter identifies conditions under which neutral States are obligated to monitor or prevent data distribution/tools for use in conflict — e.g., limit data tool provision to conflicts where the capability is likely to be asymmetrically accessed and used by one side.[9]

Third, it presents scenarios where impartiality and prevention of neutrality violations, among more specific neutrality duties, are capable of regulating corporate conduct where human rights may not. For instance, recent examples suggest that technology companies sometimes comply with neutrality principles, including by modifying corporate behavior based on normative assessments of belligerents, with potentially rights-advancing outcomes.[10] It also considers whether and how

7 *See, e.g.*, Nakashima, *supra* note 3 (reporting the detection of technological devices produced by U.S.-based technology companies for internet monitoring, on government networks in Iran and Sudan during periods of armed conflict and noting uncertainty about whether their sale and delivery violated U.S. sanctions laws).

8 *See* Noam Neuman, *Neutrality and Cyberspace: Bridging the Gap Between Theory and Reality*, 97 INT'L L. STUD. 765, 766–71 (2021) (noting that neutrality law was developed with attention to the concrete attributes of the physical domains of land, sea, and air).

9 *See, e.g.*, Ryan Gallagher, *Belarusian Officials Shut Down Internet with Technology Made by U.S. Firm*, Bloomberg, Aug. 28, 2020, 7:22 AM EDT, https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm (describing alleged deployment of deep packet inspection (DPI) equipment by the Belarusian government to interrupt internet access before a contested election—equipment that had been manufactured by a U.S. corporation—and discussing the use of similar equipment in Iran, Egypt, and Turkey). Although State sanctions regimes were designed to, and generally do, capture physical goods transported for use in armed conflict, it is less clear to what extent services transferred entirely over the internet are captured by those systems.

10 *See, e.g.*, Eric Auchard, *Yahoo Settles Case over Chinese Dissident E-Mails*, Reuters, Nov. 13, 2007, 2:13 PM, https://www.reuters.com/article/us-yahoo-china/yahoo-settles-case-over-chinese-dissident-e-mails-idUSN1360603420071113. It is not difficult to imagine similar conduct occurring in the context of armed conflict, although most such examples are likely classified. Moreover,

neutrality law is capable of governing corporations' now quasi-sovereign status: while distinctions between the actors and the centrality of territory in the *lex lata* present challenges, State neutrality rules may imply a heightened duty to ensure neutrality compliance for quasi-sovereigns.

Fourth, this chapter considers how neutrality law can complicate digital rights protection, through contradictions among rules applicable to different territories or certain rules' direct operation.

While acknowledging the limitations to neutrality law's application in the data transfer context, this chapter demonstrates that neutrality law can serve a clarifying — even gap-filling — role with respect to digital rights protection in conflict.

I
THE ORIGINS OF NEUTRALITY LAW AND ITS MODERN LEGAL STATUS

Shaped over the 18th and 19th centuries and codified in the 20th century, neutrality law developed alongside—and in response to—tremendous technological advances in warfare and business. Telephone and telegraph wires made communications more efficient,[11] while the internal combustion engine accelerated transport and manufacturing alike.[12] But these inventions had military impacts, too. Now military communications could race across neutral States in telegraph cables, and steamships could quickly supply an enemy with weapons or munitions, undetected.

Thus neutrality law arose, defining the relationship between parties engaged in armed conflict (belligerents) and those not engaged in armed conflict (neutrals).[13] Neutrality limits the scope of warfare in two ways: it protects the territorial sovereignty of neutral States from warfare's spillover effects while shielding belligerents from potential State or corporate

we will point out how even narrower duties derived from the corpus of neutrality law—e.g., the duty to determine whether the particular recipient is under belligerent control—should be recognized and can contribute to this framework.

11 *See* John Bourne, *Total War I: The Great War*, *in* THE OXFORD HISTORY OF MODERN WAR 132–35 (Charles Townshend ed. 2005).

12 *See* David French, *The Nation in Arms II: The Nineteenth Century*, *in* THE OXFORD HISTORY OF MODERN WAR 87–88 (Charles Townshend ed. 2005).

13 *The Law of Neutrality*, in ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (A.R. Thomas and James C. Duncan eds.), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1558&context=ils/.

interference in a conflict.[14] The doctrine thus provides a mechanism by which belligerents and neutral States can continue to interact without interrupting international commerce.

Neutrality was codified in Hague Conventions V and XIII of 1907, which mapped the rules applicable to land and sea, respectively.[15] The conventions set forth the rights and duties owed by and to neutral States and belligerents, which were automatically triggered by the existence of an armed conflict.[16] Chief among those rights and duties was the concept of the inviolability of territorial sovereignty. As an extension of that right, belligerents were prohibited from entering, passing through (at least on land), recruiting from, or installing or using telecommunications equipment in neutral space.[17] For their part, neutral States are obligated to act impartially; to abstain from hostilities and refrain from providing belligerents "war material of any kind"; to ensure belligerent respect for neutrality, including by using force to repel violation of territorial sovereignty; and to intern belligerent forces, vehicles, vessels, aircraft, and equipment located in neutral territory.[18]

Interestingly, Hague Conventions V and XIII concerned themselves not only with the obligations of States, but also with the role of corporations. Common across both conventions was a theme that the obligations to respect neutrality were owed by the State, who in turn was obligated to enforce it upon private actors within its territorial sovereignty. The obligations within Hague V and XIII that relate either to technological developments, corporate conduct, or private actors are outlined below:

14 *See generally* Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, NATO Cooperate Cyber Defence Centre of Excellence 37 (2012), https://ccdcoe.org/uploads/2012/01/1_3_von_Heinegg_NeutralityInCyberspace.pdf/.

15 *See* Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 10, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [*hereinafter* Hague V]; Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [*hereinafter* Hague XIII]. Similar rules applicable to airspace were drafted in the 1923 Hague Rules of Air Warfare; however, these rules were never incorporated into a binding international treaty. Commission of Jurists to Consider and Report Upon the Revision of the Rules of Warfare, Rules of Air Warfare art. 12, Feb. 19, 1923, reprinted in 32 American Journal of International Law Supplement 12 (1938).

16 *See* Rebecca Ingber, *Untangling Belligerency from Neutrality in the Conflict with Al-Qaeda*, 47 Tex. Int'l L. J. 75, 79 (2011).

17 Hague V, art. 1. *See also* Hitoshi Nasu, *The Laws of Neutrality in the Interconnected World: Mapping the Future Scenarios*, Exeter Centre for Int'l L. Working Paper Series (2020), https://www.researchgate.net/publication/345978014_The_Laws_of_Neutrality_in_the_Interconnected_World_Mapping_the_Future_Scenarios.

18 These rights and duties were articulated by Jeremy K. Davis in his article *Bilateral Defense-Related Treaties and the Dilemma Posed by the Law of Neutrality*, 11 Harv. Nat'l Sec. J. 455, 464 (2020) (outlining this framework for obligations of neutrals under the law of neutrality).

HAGUE V

Art. 2; Art. 5	Moving war supplies	• Belligerents may not move munitions or war supplies across neutral territory. • A neutral power must not allow this act to occur on its territory and has an obligation to punish such a violation of neutrality if committed on its territory.
Art. 3(a); Art. 5	Communications apparatus construction	• Belligerents may not erect a wireless telegraphy station or other apparatus on neutral territory for the purpose of communicating with belligerent forces on land or sea. • A neutral power must not allow this act to occur on its territory and has an obligation to punish such a violation of neutrality if committed on its territory.
Art. 3(b); Art. 5	Communications apparatus use	• Belligerents may not use any apparatus established before war on neutral territory for purely military purposes where that apparatus has not been opened for service of public messages. • A neutral power must not allow this act to occur on its territory and has an obligation to punish such a violation of neutrality if committed on its territory.
Art. 7	Preventing supply transit	• Neutrals are not obligated to prevent export or transport on behalf of a belligerent of anything that could be of use to an army or fleet.
Art. 8	Restricting apparatus use	• Neutrals are not obligated to forbid/restrict belligerents' use of telegraph or telephone cables or wireless telegraphy apparatus belonging to it or to private companies or individuals.
Art. 9	Ensuring corporations and private actors treat belligerents impartially	• Neutrals must ensure that companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus treat belligerents impartially.
Art. 19	Requisition or railway material	• Railway material should only be requisitioned by neutrals or belligerents when absolutely necessary. • Compensation shall be paid in proportion to material used and period of usage.

HAGUE XIII

Art. 5	Communications apparatus construction	• In neutral ports and waters, belligerents may not erect wireless telegraphy stations or apparatus for the purpose of communicating with belligerent forces on land or sea.
Art. 6; Art 7	War supplies; Preventing supply transit	• Neutrals may not supply warships, ammunitions, or war material to belligerents. • However, neutrals need not prevent the export or transit of anything that could be of use to an army or fleet.

In the decades after neutrality law was codified, the rules of warfare were transformed by the advent of the Kellogg-Briand Pact, the establishment of the United Nations, and the dawn of the modern collective security regime.[19]

The centralized security structures constructed within Article 16 of the Covenant of the League of Nations,[20] followed by Articles 2(4), 25, and 40 of the UN Charter,[21] called into question member States' abilities to behave impartially towards States that violated either the Covenant or the Charter. Practically, too, neutrality law—which applies only in international armed conflicts—proved unhelpful with respect to increasingly common conflicts involving non-State actors. Thus, for the past century, neutrality law has been given cursory treatment.

Whether the law of neutrality, derived from the laws of war, is "extinct" or retains independent normative and legal force in contemporary international politics has since been subject to debate.[22] While some scholars assert that neutrality law conflicts with the post-UN collective security structure,[23] others assert that the collective security regime and neutrality can coexist.[24] Specifically, those scholars note that member

19 *See* Detlev F. Vagts, *The Traditional Legal Concept of Neutrality in a Changing Environment*, 14 AM. U. INT'L L. REV. 83, 84 (1998). Article 2, para. 5 of the UN Charter obligates members to assist the United Nations in actions taken in accordance with the UN Charter and refrain from assisting States against which the United Nations is taking preventative or enforcement action. In this way, the UN Charter contemplates that no member State will be neutral to a conflict.

20 Article 16 of the Covenant of the League of Nations obligated member States to immediately cease economic relations with any State that waged an aggressive war contrary to Covenant principles, permit transit of foreign troops carrying out military sanctions recommended by the League's Council, and blockade the aggressor.

21 Article 2(5) of the UN Charter obligates member States to assist the United Nations at all times and to refrain from assisting any State against which the UN is taking preventative or enforcement action. Article 25 obligates all member States to be bound by all Security Council decisions. Article 40 of the Charter obligates States to join in affording mutual assistance in carrying out any measures decided upon by the Security Council.

22 *See, e.g.*, Michael Bothe, *The Law of Neutrality*, in THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 571, 573-75 (Dieter Fleck ed., 2d ed. 2008) ("These [Hague] rules of 1907 have in part been rendered obsolete by later practice. The Charter of the United Nations completed the development of the international legal prohibition of the use of force and established a system of collective security, by the reaction of the international community against breaches of peace. The traditional law of neutrality with its duty of impartiality, i.e. the prohibition of discrimination between the parties to the conflict, seems to be incompatible with this development which outlaws the aggressor. However, this is not generally the case. Also under the UN Charter, neutrality during international armed conflicts is permissible and possible. States expressly rely on the law of neutrality. The International Court of Justice as well as national courts have recently upheld the continued validity of the law of neutrality. The impartiality of the neutral state retains its important functions at least as long as there is no possibility of a binding decision concerning the question of who in a given conflict is the aggressor and who is the victim.... [but] the duty of non-participation as well as that of impartiality may be restricted by decisions of the Security Council. But it must be ascertained in each particular case how far this has been the case.").

23 *See generally* Maria Gavouneli, *Neutrality: A Survivor?* 23 EUR. J. INT'L L. 267, 267 (2012) (describing Nicholas Politis's argument that neutrality law was obsolete following the establishment of the collective security system).

24 For an argument for the continued utility of neutrality law after the UN Charter's comprehensive regulation of the use of force, see James Upcher, NEUTRALITY IN CONTEMPORARY INTERNATIONAL LAW 1–5, 217–62 (2020).

States are bound by the general obligation within Article 2(5) to refrain from giving assistance to an aggressor State and are bound to conduct certain enforcement actions only when called upon by the Security Council per Articles 24 and 25.[25] However, nothing in neutrality law prevents States from creating treaty-based and commitment-based bilateral and multilateral collective security frameworks that run against the duty of non-participation, providing support for the enduring power of neutrality law.

State practice is perhaps telling with respect to neutrality law's modern legal status. My research has been unable to identify any statement, by any State, disavowing neutrality law's continued force. Rather, as others have pointed out, many States continue to interpret their obligations vis-à-vis neutrality law within international armed conflicts.[26] This chapter thus assumes that neutrality law remains operational — though the boundaries of when and how remain unsettled.

II
NEUTRALITY LAW'S MODERN APPLICATION

Modern military operations almost necessarily rely on infrastructure passing through a neutral State via infrastructure or multinational corporations. It is not difficult to imagine examples in which data transfer, storage, or moderation requests, implicating a third State, could arise in an armed conflict situation and thus implicate neutrality law.[27]

25 *See, e.g.*, Heribert Franz Koeck, *A Permanently Neutral State in the Security Council*, 6 CORNELL INT'L L. J. 137, 147 (1973) (discussing the status of neutral States, such as Switzerland, within the collective security system and their obligations vis-à-vis the UN Charter).

26 *See generally* Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE 36 and fns. 4–10 (2012), https://ccdcoe.org/uploads/2012/01/1_3_von_Heinegg_NeutralityInCyberspace.pdf/ (collecting provisions relating to neutrality in the military manuals of the United States, Canada, the United Kingdom, Germany, the San Remo Manual, the ILA Helsinki Principles, and the HPCR Manual).

27 For example, consider these scenarios: (1) U.S.-created web-monitoring devices found in Iran; (2) a request for data from a server in Ireland by a government committing human rights/LOAC violations, where the server company is headquartered in the U.S.; and (3) a request from a belligerent (e.g., Syria or the government of Myanmar) to a company in Turkey or Bangladesh (respectively), or another country with a large refugee population, for data stored/processed about the refugees in connection with military efforts against the victim/refugee group remaining in the country.

A EXAMPLES OF DATA TRANSFER, STORAGE, OR MODERATION FROM THIRD STATES

Take three recent examples of scenarios that arose outside an international armed conflict. First, in August 2020, Bloomberg reported that the government of Belarus had shut down citizens' internet access amidst a contested election.[28] To interrupt the internet, the government had allegedly deployed deep packet inspection (DPI) equipment manufactured by an American company. According to news reports, this was not the first time that American-made content interruption software had been identified on other States' computer networks. According to the Bloomberg news agency, that software had also been identified in Turkey, Syria, and Egypt. Previous news reports alleged that other, similar American-made software had been deployed in Iran, Sudan, Egypt, and China.[29]

Second: in November 2007, Yahoo allegedly provided information to the Chinese government, pursuant to a data request, about a Chinese dissident involved in advocating for democratic reform. Accorded to a lawsuit filed in the United States, the Chinese government allegedly used that Yahoo-provided information to prosecute the Chinese dissident.[30] Data requests issued directly from States to multinational companies have since exploded in scale and scope. To respond to these requests, technology companies have built robust regulatory and compliance architectures to address and organize their cross-border data transfer process.[31]

Third: in February 2021, Myanmar ordered its local mobile network and internet service providers to block Twitter and Instagram in the country.[32] Facebook responded with a formal statement that the company

28 *See, e.g.*, Ryan Gallagher, *Belarusian Officials Shut Down Internet with Technology Made by U.S. Firm*, Bloomberg, Aug. 28, 2020, 7:22 AM EDT, https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm.

29 *See* Ellen Nakashima, *Report: Web Monitoring Devices Made by U.S. Firm Blue Coat Detected in Iran, Sudan*, WASHINGTON POST, July 8, 2013, https://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html.

30 *See* Eric Auchard, *Yahoo Settles Case over Chinese Dissident E-Mails*, Reuters, Nov. 13, 2007, https://www.reuters.com/article/us-yahoo-china/yahoo-settles-case-over-chinese-dissident-e-mails-idUSN1360603420071113.

31 *Compare Microsoft Releases Report on Law Enforcement Requests*, Access Now, Mar. 25, 2013, 3:31 PM, https://www.accessnow.org/microsoft-releases-report-on-law-enforcement-requests/, *with Information Request Report*, Amazon (Dec. 2020), https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf, *and Transparency Report*, Google, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US, (exemplifying emergent State practice of corporate due diligence programs, with characteristics akin to sanctions regimes traditionally undertaken by States).

32 *See, e.g.*, Kim Lyons, *Myanmar Orders Internet Providers to Block Twitter and Instagram in the Country*, THE VERGE, Feb. 6, 2021, 10:10 AM EST, https://www.theverge.com/2021/2/6/22269831/myanmar-orders-block-twitter-facebook-instagram-military-coup (noting Facebook's response

was "extremely concerned" by the shutdown orders; urged authorities to unblock access; and noted that during the ongoing military coup, it was particularly important for citizens to be able to access information and communicate with their loved ones. Twitter promised to "continue to advocate to end destructive government-led shutdowns."[33] Those statements reflect a broader trend in which corporations are called to set policy in response to a repressive State's violation of digital rights.

If any of these examples took place in the context of an international armed conflict, the data transfer, storage, and moderation would implicate neutrality law, with the neutral State in which the corporation was headquartered at risk of having violated its impartiality obligations.

B NEUTRALITY LAW AND MODERN DIGITAL GOODS AND SPACES

The characteristics and purposes of modern goods are similar to the weapons, information, and instruments that neutrality law was created to govern. In this way, neutrality law has potential application to digital goods and spaces in modern armed conflict, including social media content moderation, data storage or processing tool provisions, or evaluation of State-issued consumer data requests.

A caveat: the domain-specific nature of neutrality law is an obvious limitation on its extension to the digital context. Although neutrality law explicitly governs physical domains—namely land and sea[34]—data and infrastructure provisions operate both within and beyond physical space.[35] Digital space lacks territorial boundaries and optical visibility (and thus easy attribution) of the physical domain. But because data transfer can also have kinetic effects, cross territorial borders, and pass through sea and air, it could involve the rules of land, air, and sea. Some scholars have

to Myanmar's orders that ISPs block Twitter and Facebook-owned Instagram: "At this critical time, the people of Myanmar need access to important information and to be able to communicate with their loved ones").

33 *See id*.

34 For an analysis of State practice and *opinio juris* relating to the applicability of the law of neutrality to digital space, see Neuman, *supra* note 8, at 779–86.

35 *See generally* Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L. J. 815, 824–30 (2012) (applying laws of neutrality to cyber incidents on sea and land to reach coherent results). *See also* TALLINN MANUAL 2.0 rules 150 through 154 (noting that the law of neutrality developed in situations in which entry or exit from a neutral State's territory constituted a physical act, but digital space's realities involve transit irrespective of geopolitical borders. Although the International Group of Experts advised caution and careful consideration in assessing a neutral State's violations under the law of neutrality or drawing conclusions about violations of a State's neutrality, they concluded that neutrality law had application to the cyber domain.)

noted that the application of neutrality laws to cyber actions may lead to inconsistent results, depending on which domain's rules are applied.[36]

1 *Corporate Acts Subject to Regulation*

Assuming the domain-specific limitations of neutrality law do not prevent its application to digital space, how (if at all) might neutrality law's obligations and prohibitions map onto modern corporate acts occurring within international armed conflicts? What obligations might neutrality impose on States, and what obligation might States be expected to, in turn, enforce upon corporations?

Data requests and compelled assistance: Neutrality law could govern data requests made by belligerent States. Modern data transfers have several potential analogues under the Hague Conventions:

- To the use of telecommunications and related equipment for the intangible transfer of information,[37] where that apparatus is also open for service of public messages, per Hague V, arts. 3(a) and 5; and
- To the movement of things of use to an army or fleet, per Hague V, art. 7 and Hague XIII, arts. 6–7.

36 *See generally* Neuman, *supra* note 8, at 787–98 (outlining conflicting outcomes from applying rules applicable to different domains to a cyber context). Neuman ultimately concludes that the various domains share overarching principles applicable to all, such as inviolability and impartiality, that can govern actions in cyberspace even in the face of a domain-specific conflict. Where the various conventions would lead to inconsistency, this chapter offers no solution to which doctrine to apply, other than to suggest that digital actions may be best gauged individually, with the *lex specialis* that most accurately describes the content, nature, and venue of the cyber act as the one that governs.

37 In "The Law of Maritime Neutrality and Submarine Cables," James Kraska disagrees with this assessment. In his view, information packets are more like "radio or sound waves" that "merely propagate energy and cannot be analogised to physically violating neutral territory." *See* James Kraska, *The Law of Maritime Neutrality and Submarine Cables*, EJIL: TALK! July 29, 2020, https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/. Kraska relies primarily on a 1923 arbitration, in which the tribunal determined that a belligerent was permitted to cut an underseas cable outside neutral territory. *See Eastern Extension, Autralasia and China Telegraph Company, Ltd. (Great Britain) v. United States*, Arbitral Award of Nov. 9, 1923, 6 Rep. J. Int'l. Arb. Awards (11) Arb. 1923. Kraska's argument can be distinguished from the majority of the data transfers we discuss in this chapter. First, Kraska lists reasons to distinguish data storage from classic "cyber" information flows that center on whether they create a physical violation. But many of the examples considered in this chapter—particularly those relating to the provision of data from a storage facility in a third State, e.g., a data request emanating from a Microsoft Ireland server—have a physical aspect to them. An information request directed to a physical facility used to store and process data is different than merely having unmonitorable information flows going through a cable that happens to pass through the building. Moreover, the transfer of software from a third State that can be offensively used by a belligerent calls up the seminal debate about whether a cyber attack must result in physical effects. *See, e.g.*, Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L. L.J. ONLINE 1, 2–7 (2012); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 841–48 (2012). In addition, most of the law on which Kraska relies is *lex specialis* to the maritime context. However, the law of neutrality has some role to play on governing data transfer in armed conflict, and *lex specialis* should not apply.

The Hague Conventions do not forbid information transfer, facilitated by corporations or private actors, to a belligerent. However, such a data transfer from a corporation to a belligerent is subject to the obligation for neutrals to ensure that companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus treat belligerents impartially, per Hague V, art. 8.

The implicit obligation behind this provision is for States to monitor corporate compliance in data transfer to belligerents—whether compelled or voluntary—to ensure that any assistance is rendered impartially.

Trade: Neutrality also might impose obligations vis-à-vis the trade of data processing tools.[38] Applicable Hague provisions include:

- The obligation of belligerents not to move munitions of war or supplies across neutral territory, and the related obligation on neutrals to prevent this act from occurring on its territory and punishing any such violation that occurs, per Hague V, arts. 2 and 5; and

- The obligation of neutrals to not supply warships, ammunitions, or war material to belligerents, per Hague XIII, art. 6.

Though belligerents are prohibited from moving supplies across neutral territory, private corporations are free to export them. Hague V, art. 7 and Hague XIII, art. 7 clarify that neutrals need not prevent the export or transit, on land or sea, of anything that could be of use to an army or a fleet.

Inherent in these articles is a responsibility of the neutral State to assess what is being provided by corporations to belligerents. The neutral State has an obligation to ensure that any data or equipment traveling across its territory is not munitions or supply for warfare; it has the obligation to prevent and to punish such transfers. To the extent that data could be used as a weapon—such as via denial of service—neutral States would also be responsible for assessing and interfacing with its transfer.

That being said, as with information transfer, neutrals are obligated to ensure that companies or private individuals owning telegraph or

38 This view is consistent with Rule 150 of the Tallinn Manual 2.0. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 48–52 (Michael N. Schmitt ed., 2017) [*hereinafter* TALLINN MANUAL 2.0]. That rule states that the "exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited." Implicit within this rule is the concept that cyber operations can be analogized to the physical transportation or munitions or supplies of war through a neutral power, as Kraska points out. *See* Kraska, *supra* at 37.

telephone cables and wireless telegraphy apparatus treat belligerents impartially, per Hague V, art. 9. In the context of the export or provision of data-processing tools, that could look like monitoring corporate exports and ensuring that they are not unfairly assisting one party to the conflict.

Platform provision: This subset of data transfers encompasses uses of platforms, as well as conducting content restrictions or moderations on those platforms. This seems most akin to Hague V, art. 3(b)'s requirement that belligerents not use any apparatus established before war on neutral territory for purely military purposes where that apparatus has not been opened to convey public messages. But that scenario seems unlikely to occur on social media platforms or messaging services, which generally hold themselves out for public use. Platform usage likely implicates Hague V, art. 7 and Hague XIII, art. 7; again, these clarify that neutrals need not prevent the export or transit, on land or sea, of anything that could be of use to an army or a fleet.

Akin to platform provision is a belligerent's request to conduct content restriction or moderation. To the extent that content restriction or moderation goes a step beyond denying access to *manipulating* access—for example, through redirection to another website—content restriction becomes like a munition. To the extent that a moderation or content restriction operates like an instrument of warfare, a belligerent would not be permitted to move content restrictions across neutral territory, and neutral powers would have an obligation to prevent this from occurring on their territory and punish any violations committed on their territory, per Hague V, arts. 2 and 5.

Infrastructure provision: Finally, the Hague provisions most easily map onto the provision of physical infrastructure that makes data services possible, like underseas cables or telecommunications equipment and structures. For these, the Hague analogues are relatively clear:

- Belligerents may not erect equipment, for the purposes of communicating with belligerent forces, on neutral territory, per Hague V, art. 3(a) and Hague XIII, art. 5;

- Neutrals need not forbid or restrict belligerent use of such equipment belonging to it or to private companies or individuals, per Hague V, art. 8; and

- Neutrals and belligerents may requisition such equipment only when absolutely necessary, and even then must pay proportionate compensation, per Hague V, art. 19.

The construction and use of infrastructure or equipment requires less State monitoring of corporate conduct. Since infrastructure has closer ties to physical space (generally, cell towers or data storage and processing centers built on land or underseas cable laid at sea), the Hague provisions map neatly onto these potential issues.

2 *State Obligations and Consequences of Non-Compliance*

The above analysis suggests that neutral States are bound to ensure that their corporations treat belligerents impartially in their exports of data and digital tools and thus violate neutrality by failing to ensure that their corporations treat belligerents neutrally.

A neutral State that has failed to fulfill the duty of impartiality may be subject to countermeasures, including forceful countermeasures, from belligerents.[39] The text of Hague V and Hague XIII make clear that the obligation to ensure impartiality is absolute.[40] However, scholars have drawn a distinction between "slight" and "substantial" violations of neutrality, arguing that belligerents can institute measures other than the use of force that deny neutrals some or all of the benefits of neutrality.[41]

However, it is unclear whether a neutral State is rendered a belligerent or a co-belligerent by failing to impose the duty of impartiality on private actors within its territory. Most scholars believe that breaching neutrality does not per se render an actor a co-belligerent;[42] rather, only

39 *See The Law of Neutrality*, in U.S. DEP'T OF DEFENSE LAW OF WAR MANUAL 957 (June 2015) (*citing* ROBERT W. TUCKER, THE LAW OF WAR AND NEUTRALITY AT SEA 203, fn. 14 (1955) ("The duties of a neutral state may also be classified—and frequently are so classified—as duties of abstention, prevention and acquiescence (or toleration). … [D]uties of acquiescence have reference to neutral obligations to permit belligerent measures of repression against neutral subjects found rendering certain acts of assistance to an enemy")).

40 *See, e.g.*, Hague V, art. 9.

41 *See* L. OPPENHEIM, INTERNATIONAL LAW § 359 (H. Lauterpacht ed., 8th ed. 1952) ("If the violation is only slight and unimportant, the offended State will often merely complain. If, on the other hand, the violation is very substantial and grave, the offended State will perhaps at once declare that it considers itself at war with the offender"); *see also* Rebecca Ingber, *Untangling Belligerency from Neutrality in the Conflict with Al-Qaeda*, 47 TEX. INT'L L. J. 75, 87–88 (2011) (noting that violations of neutrality "often do not permit the use of force in return, particularly in the post-U.N. Charter world" and that "states negotiating details of neutrality law in its heyday constructed elaborate regimes for redressing violations that fell far short of declaring war at any particular instance and included remedies such as financial compensation").

42 *See* Clyde Eagleton, *The Duty of Impartiality on the Part of a Neutral*, 34 AM. J. INT'L L. 99, 101 ("The failure to perform a specific duty… would permit a legal claim and perhaps the collection of damages; the failure to be impartial, on the other hand, would not arouse or justify a legal claim for damages, but might modify or end neutral status"). *See also* United Nations General Assembly, Extrajudicial, summary or arbitrary executions, ¶ 60, U.N. Doc. A/68/382 ("Co-belligerency is a concept that applies to international armed conflicts and entails a sovereign State becoming

systematic, serious violations of the law of neutrality do so.[43] But what constitutes "systematic" violations of the law of neutrality has yet to be explored in the data transfer context. In particular, whether a State commits systematic violations of the laws of neutrality through failure to monitor and ensure the impartiality of corporations within its territory with respect to data transfer is undetermined.

3 *What Actions Might a State Stop?*

Taking a step back, neutrality might be operationalized in a corporate context to obligate a degree of State oversight over data, data services, and data infrastructure requests made by belligerent States involved in international armed conflicts.[44]

States might assess the nature of the requests for data transfers or services made by belligerent States and serve as the umpire for whether the provision of the requested material would favor one belligerent over the other. If so, States might stop its export entirely, or else delay it until after the international armed conflict has concluded.

Relatedly, States might be called upon to assess whether data or services requested could function as munitions—something that could be used by one State against the other in a conflict. Things like denials of service, data collection tools, or other digital systems could arguably fall within that category. For those, States would be obligated not only to prevent their export but also to punish their movement across its territory.

These questions are particularly relevant in the context of State practice. The United States has created an infrastructure for extraterritorial data sharing and facilitation of government data requests via the CLOUD Act, which provides transnational access to personal data in criminal law enforcement investigations. One of the effects of the CLOUD Act is that qualifying foreign governments have now been permitted to send data

a party to a conflict, either through formal or informal processes.... [A]n informal process could involve providing assistance to or establishing a common cause with belligerent forces") (not opining on the degree of assistance required to establish co-belligerency).

43 *See* Ingber, *supra* note 41, at 87–88 (2011) ("The law of neutrality itself did not traditionally articulate when a state or individual gave up its neutral state and became a belligerent...; it simply acknowledged that, once a state or individual became a belligerent, it could no longer avail itself of its prior neutrality"); Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2112–13 (2005) ("One way that a state can become a co-belligerent is through systematic or significant violations of its duties under the law of neutrality.... [A] state is deemed to be in an armed conflict with a 'neutral' state that systematically violates its neutral duties"); Nathalie Weizmann, *Associated Forces and Co-Belligerency*, JUST SECURITY, Feb. 24, 2015, https://www.justsecurity.org/20344/isil-aumf-forces-co-belligerency/ (last accessed Nov. 12, 2021).

44 This proposal may be hampered by feasibility, consider the amount of data and the number of companies making frequent, and sometimes automated, decisions regarding data processing and transfer. The amount of data and number of requests that would need to be umpired, though, may be limited by the relatively small number of international armed conflicts.

requests directly to U.S. companies for data, rather than contacting the U.S. Department of Justice to obtain warrants for that data from U.S. judges. So the CLOUD Act has functionally decreased a neutral State's review of data provision.

III
SCENARIOS THAT NEUTRALITY DUTIES MIGHT REGULATE BUT HUMAN RIGHTS MIGHT NOT

At a high level, international human rights law provides protections for digital rights that include the right to privacy and the right to data protection.[45] States are obligated to respect and ensure those rights to all individuals within their territory and potentially to individuals within their effective control.[46] So too must States refrain from violating or restricting those rights.[47] Soft law likewise suggests corporate obligations: to respect international human rights, avoid causing adverse impacts, and seek to prevent and mitigate human rights impacts through their businesses.[48]

Concerning digital rights, the law of neutrality varies from human rights law in the following manners. First, the law of neutrality and human rights law vary as to their *scope of application*. One way of thinking about the two doctrines is their relative applications in times of peace and in times of war. International human rights apply to States during both war and peace;[49] however, States can derogate from human rights

45 *See* Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, in Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives 468–76 (Robert Kolb, Gloria Gaggioli and Pavle Kilibarda eds., Edward Elgar, 2022).

46 For an overview of the debate concerning extraterritorial human rights obligations, see generally Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011); and Oona Hathaway et al., *Human Rights Abroad: When Do Human Rights Treaty Obligations Apply Extraterritorially*? 43 Arizona State L. J. 389 (2011).

47 *See, e.g.*, The Right to Privacy in the Digital Act (Aug. 3, 2018), A/HRC/39/29.

48 *See, e.g.*, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (May 11, 2016), A/HRC/32/38 ("The private sector, however, also plays independent roles that may either advance or restrict rights, a point the Human Rights Council well understood by adopting the Guiding Principles on Business and Human Rights in 2011 as general guidance in that field"); Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (Guiding Principles), UN Doc. HR/PUB/11/04 (2011), www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

49 *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 55 (July 8) ("The Court observes that the protection of the International Covenant of Civil and

obligations under emergency situations, including in wartime.[50] The law of neutrality operates only when States are at war; however, the laws apply automatically and without derogation to all States, even those at peace.[51] Moreover, as the *lex specialis*, the law of neutrality will apply when human rights law and the law of neutrality conflict.[52] Thus the laws of neutrality could theoretically provide a backstop for human rights-like obligations during emergency periods in which States are permitted to derogate from international human rights law.

Second, the law of neutrality and human rights law differ in terms of their *triggering test*. The indicator for whether neutrality is violated (i.e., whether one side is being assisted more than the other) is fundamentally different than the human-rights-derived triggering tests (e.g., effective control). Comparing the two, it is simpler to gauge whether the laws of neutrality have been violated than to determine whether effective control is at play. Effective control has uncertain application with respect to digital rights abroad in some circumstances,[53] whereas the laws of war feature no such constraint.[54] Neutrality law can thus embolden the application of positive human rights due diligence obligations and offer value by filling a gap left by uncertain extraterritorial human rights obligations.

Third, the law of neutrality and human rights law vary with respect to the *obligations imposed upon States*. International human rights due diligence obligations are less clear-cut than the question of impartiality obligation under neutrality law.[55] But neutrality imposes three clear

Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities").

50 *See, e.g.*, International Covenant on Civil and Political Rights, art. 4(1), Dec. 19, 1966, 999 UNTS 171, 174.

51 *See supra* sources cited at fn. 39. States that are at peace have obligations under neutrality law in relation to States that are at war.

52 *See* C. Wilfred Jenks, *The Conflict of Law-Making Treaties*, 30 BRITISH YEARBOOK OF INTERNATIONAL LAW 401, 446 (1953) ("A clear illustration of [*lex specialis*'s] applicability is afforded by instruments relating to the laws of war which, in the absence of evidence of a contrary intention or other special circumstances, must clearly be regarded as a *leges speciales* in relation to instruments laying down peace-time norms concerning the same subjects").

53 *See, e.g.*, *10 Human Rights Organizations v. United Kingdom*, App. No. 24960/15 (May 2015) (holding that "a contracting state owes no obligation under Article 8 [the right to respect for privacy] to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through the state"). The case—and thus the question of the extraterritorial application of human rights under the European Convention on Human Rights—is awaiting judgment from the European Court of Human Rights.

54 *See, e.g.*, Montgomery Sapone, *Have Rifle With Scope, Will Travel: The Global Economy of Mercenary Violence*, 30 CAL. W. INT'L L.J. 1, 32 (1999) ("The United States need not recognize the belligerent status of the political entity in order for the Act to apply; actual conflict triggers application of the Act").

55 *See, e.g.*, Annual Report of the United Nations High Commissioner for Human Rights, Addendum, Report of the United Nations High Commissioner for Human Rights on the Situation of Human

obligations onto States: to refrain from acting (much like negative human rights obligations), to prevent the commission of certain acts (much like positive human rights obligations), and to acquiesce (to permit belligerents to repress neutral subjects to render assistance to an enemy).[56] Those "positive neutrality law obligations" are more clear-cut than those that international human rights law can offer. For example, neutral States have an obligation to prevent specific acts by anyone within their jurisdiction, including belligerent acts of hostility in neutral waters and the use of neutral ports as operational bases.

Fourth, the law of neutrality and human rights law vary with respect to the *obligations imposed upon private actors within a State.* For its part, human rights law generally imposes obligations on State governments with respect to citizens; corporations, being neither, are governed by human rights law only by analogy and soft law.[57] But neutrality law imposes obligations on corporations directly, while permitting States to enforce compliance.[58]

The fourth point is of particular interest. Recent examples suggest that technology companies sometimes comply with neutrality principles, including by assessing whether a State is engaging in armed conflict

Rights in Colombia, UN Doc A/HRC/22/17/Add.3 (Jan. 7, 2013) ("Everyone has rights and obligations under human rights law. The State holds primary responsibility, as not only must it respect human rights and respond when it violates them, but it also has the duty to protect against violations by third parties and to create an environment where all rights are respected. While, for example, armed actors, landlords and businesses must all respect human rights and be accountable for violations they commit, the State, through its policies, programmes and laws, must act to stop these violations and prevent their repetition"). Negative obligations on States (prohibition from action in a manner that violates or unlawfully restricts rights and freedoms guaranteed by human rights treaty) are more clear-cut than their positive law obligations (adoption of measures to protect individuals over whom the State exercises effective control from violations of rights by State organs, State agents, or private actors).

56 *See The Law of Neutrality*, in U.S. Dep't of Defense Law of War Manual 957 (June 2015) (*citing* Robert W. Tucker, The Law of War and Neutrality at Sea 203, fn. 14 (1955) ("The duties of a neutral state may also be classified—and frequently are so classified—as duties of abstention, prevention and acquiescence (or toleration). Duties of abstention refer to acts the neutral state itself must refrain from performing; duties of prevention refer to acts the commission of which within its jurisdiction the neutral is obligated to prevent; and, finally, duties of acquiescence have reference to neutral obligations to permit belligerent measures of repression against neutral subjects found rendering certain acts of assistance to an enemy")).

57 *See, e.g.*, United Nations Remarks on Signing International Covenants on Human Rights, 1 Pub. Papers 1734 (Oct. 5, 1977) ("The Covenant on Civil and Political Rights concerns what governments must not do to their people, and the Covenant on Economic, Social and Cultural Rights concerns what governments must do for their people. By ratifying the Covenant on Civil and Political Rights, a government pledges, as a matter of law, to refrain from subjecting its own people to arbitrary imprisonment or execution or to cruel or degrading treatment. It recognizes the right of every person to freedom of thought, freedom of conscience, freedom of religion, freedom of opinion, freedom of expression").

58 *See, e.g.*, Hague V, art. 9 ("Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus"). The text's suggestion is that the obligations regarding impartial transport of goods and information applies to corporations and that States have an enforcement obligation.

and determining whether their interactions with one party to a conflict would serve as asymmetric assistance. Based on those normative assessments, corporations have modified their behavior with potentially rights-advancing outcomes.[59]

This observation is particularly important given that modern technology companies—although they are not sovereigns themselves and are not subject to neutrality law directly—exercise features of sovereignty as recognized in international law within contemporary international relations. Take, for example, Microsoft's handling of a data request. For data requests to U.S.-based technology corporations, the CLOUD Act permits foreign governments, under certain circumstances, to coordinate directly with foreign governments about data requests.[60] Technology companies are asked to make normative assessments of conflict and in fact do so. Although technology companies do not exercise power over territory, their rising degree of power over both internal and external affairs reflects at least one conception of sovereignty discussed in international law.[61]

Impartiality, abstention, and the prevention of neutrality violations offer opportunities to regulate corporate conduct where human rights may not.[62] Distinctions between the actors and the centrality of territory in the *lex lata* present challenges, but neutrality already purports to impose conduct upon corporations and empower States to enforce compliance.

59 For example, Facebook released a report noting that it removed accounts and pages linked to Sluha Narodu, a Ukrainian political party that supports Ukraine's current government. *See April 2021 Coordinated Inauthentic Behavior Report*, Facebook, May 6, 2021, https://about.fb.com/news/2021/05/april-2021-coordinated-inauthentic-behavior-report/; "Facebook removes Ukrainian Pages Promoting Zelensky's Political Party," Medium, May 6, 2021, https://medium.com/dfrlab/facebook-removes-ukrainian-pages-promoting-zelenskys-political-party-d5600998cb06. Facebook has cited international organizations' assessments related to international human rights violations for making similar de-platforming determinations. *See* Jenny Domino, *Gambia v. Facebook: What the Discovery Request Reveals about Facebook's Content Moderation*, JUST SECURITY, July 6, 2020 ("International experts, most recently in a report by the UN Human Rights Council-authorized Fact-Finding Mission on Myanmar, have found evidence that many of these individuals and organizations committed or enabled serious human rights abuses in the country"), https://www.justsecurity.org/71157/gambia-v-facebook-what-the-discovery-request-reveals-about-facebooks-content-moderation/.

60 *See* Stephen P. Mulligan, *Cross-Border Data Sharing under the CLOUD Act*, Congressional Research Service, Apr. 23, 2018.

61 *See generally* Samantha Besson, *Sovereignty*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW ¶¶ 69–73 (Apr. 2011), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=MPIL.

62 This chapter does not offer a systematic articulation of the circumstances in which international human rights law applies and neutrality does not, or vice versa. Rather, this chapter focuses on the human rights that fall under the new umbrella of "digital rights," chief among them the right to privacy, and discusses how human rights principles of necessity and due process operate within and alongside the context of neutrals.

CONCLUSION

The law of neutrality has historically been excluded from international humanitarian law. Christopher Greenwood wrote:

> The term "international humanitarian law" is of relatively recent origin and does not appear in the Geneva Conventions of 1949.... International humanitarian law thus includes most of what used to be known as the laws of war, although strictly speaking some parts of those laws, such as the law of neutrality, are not included since their primary purpose is not humanitarian.[63]

This chapter posits that although the law of neutrality's primary purpose is not humanitarian, its application—particularly in the contested and evolving field of digital rights—may well be. Neutrality law offers a potential backstop to gaps in international human rights law, with particular regard to questions about the extraterritorial application of human rights and situations in which human rights obligations have been derogated. At bottom, this chapter outlines certain circumstances where neutrality works to govern conflict in situations where international human rights obligations are sufficiently uncertain. Thus neutrality is capable of doing work that international human rights law, as of yet, cannot.

Likewise, neutrality, on its face and as reflected in practice, extends its authority to govern not only States but also corporations. And State practice suggests that data companies are complying with principles of neutrality by making normative assessments of conflicts and seeking to render impartial assistance.

63 Christopher Greenwood, *Historical Development and Legal Basis*, in Dieter Fleck, The Handbook Of Humanitarian Law In Armed Conflicts 9 (¶102) (1999).

Chapter 5

Emerging Technologies, Digital Privacy, and Data Protection in Military Occupation

Omar Yousef Shehabi[1]

INTRODUCTION

In the occupied Palestinian territory, *al-munasiq*, Arabic for "the coordinator", is understood to refer to the Israeli Coordinator of Government Activities in the Territories (COGAT). COGAT is the branch of the Israeli military government in the occupied territory responsible for civilian affairs, including permits to work in Israel.[2] Palestinian labour in Israel has been an abiding feature of the occupation, peaking in 1988, at the end of the open borders era, when roughly one-third of the occupied

1 JSD candidate, Yale Law School, omar.shehabi@yale.edu. I thank Carmel Alshaibi for her research assistance, Omar Dajani, Ardi Imseis, Polina Levina Mahnad and Michael Schoiswohl for their comments, and the editors and contributors to this book project for their insights. The views expressed are my own and do not necessarily reflect the view of the United Nations. All internet sources herein were last accessed on 20 January 2022.

2 COGAT is the parent entity of the Civil Administration, the occupation bureaucracy established by Military Order No. 947 of 1981.

territory's workforce worked in "Israel proper".[3] In 2019, some 133,000 Palestinians — roughly 11 per cent of the West Bank's working-age population[4] — worked in Israel or Israeli settlements in the occupied territory.

That year, COGAT launched the al-Munasiq smartphone app, which allows Palestinians to check the status of their permits. Previously, this required a visit to Israeli-Palestinian district coordination and liaison offices (DCOs) in the West Bank. To register in the app, the user was required to accept terms of service which authorised COGAT and third parties to use the information collected "for any purpose, including for security purposes" and to store user information in COGAT's databases.[5] The app gave COGAT access to users' contacts, photos, files, chats, emails, camera and location data.

When the coronavirus pandemic forced the DCOs to close in March 2020, al-Munasiq became the only way for Palestinians to check the status of their permits. An Israeli NGO petitioned the Israeli High Court of Justice for a ruling that in the context of a health emergency which effectively rendered use of the app mandatory, its terms of service violated the right to privacy under Israeli and international law. While the petition was pending, COGAT announced amendments to the app's terms of service and that data collection would be limited to the forms specified therein, including location services and camera and file access for scanning and uploading documents.[6] In May 2020, the Israeli high court dismissed the petition, which did not name individual petitioners or plead actual harm, as premature and theoretical.[7] By then, over 50,000 Palestinians had downloaded the app. What became of the data extracted from users under the earlier terms of use is unclear,[8] and the app does not allow users to request deletion of their data.

Al-Munasiq is but a small part of an ecosystem of surveillance in the occupied territory that includes biometric checkpoints, social media data-mining, and CCTV camera networks enhanced with facial recognition technology and machine learning. Israel, of course, is not unique

3 Andrew Ross, Who Built Zion? Palestinian Labor and the Case for Political Rights, 27(3) NEW LABOR F. 44, 47 (2018).

4 The West Bank's working-age population stood at 1,173,530 at the 2017 census. *Labour Force Participation and Employment in the State of Palestine* 30, PALESTINIAN CENTRAL BUREAU OF STATISTICS (2020), https://pcbs.gov.ps/Downloads/book2507.pdf

5 Hagar Shezaf, *Israel Tells Court Would Stop Forcing Palestinian Laborers to Give Access to Phone Data*, HAARETZ (May 15, 2020), https://www.haaretz.com/middle-east-news/palestinians/.premium-over-50-000-palestinians-forced-to-give-phone-data-to-israel-1.8844580.

6 *Id.*

7 HCJ 20/2992 *HaMoked v. Ministry of Defence*, https://hamoked.org.il/files/2020/1664225.pdf.

8 Following HaMoked's demand: the military amended the invasive terms of use of the mobile app enabling Palestinians to check the status of permit requests, HAMOKED (June 2, 2020), http://www.hamoked.org/Document.aspx?dID=Updates2175.

among occupying powers in deploying mass surveillance technologies. The United States established a data mining programme in occupied Iraq and a biometric database of roughly two million Iraqis.[9] There is every reason to believe that other contemporary occupying powers deploy many of the same technologies.[10]

As these technologies grow in ubiquity, democratic societies are grappling with standards governing the collection, storage, and processing of personal data (data protection standards) and the right of data subjects to have some control over these processes (data subject rights). In the inherently coercive context of military occupation, the desire to regulate surveillance technologies, limit the use of the data they yield, and endow data subjects (*i.e.*, protected persons in the occupied territory) with some degree of agency over their personal data is compelling. However, the pursuit of a doctrinally sound way to regulate the use of these technologies raises thorny epistemological questions regarding the law of occupation and its place within international law. This short contribution merely endeavours to highlight the challenges in establishing a data privacy and protection regime for occupied territory, using the occupied Palestinian territory as a most imperfect case study.

The chapter proceeds as follows. Part I samples Israel's use of mass and targeted surveillance technologies in the occupied Palestinian territory. Part II examines the few provisions of the conventional law of occupation which relate to privacy and how these provisions might be progressively reinterpreted to reach digital privacy. Part III assesses whether and to what extent the digital privacy and data subject rights emerging in human rights law are interoperable with international humanitarian law (IHL) in the context of military occupation. Part IV considers, however inadequately, the inescapable epistemological questions conjured up by the question of digital privacy and data protection in settler-occupations and transformative occupations. The final part concludes with a sober assessment of the prospects for regulating digital privacy and data protection in the general law of occupation.

9 Henrik Moltke, *Mission Creep: How the NSA's Game-Changing Targeting System Built for Iraq and Afghanistan Ended Up on the Mexico Border*, THE INTERCEPT (May 29, 2019), https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/; Farah Stockman, *Worries About US Data on Iraqis*, BOSTON GLOBE (Aug. 31, 2010), http://archive.boston.com/news/nation/washington/articles/2010/08/31/questions_arise_about_use_of_data_gathered_in_iraq_war/.

10 Laurens Cerulus, *How Ukraine became a testbed for cyberweaponry*, POLITICO (Feb. 14, 2019), https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks (describing Russian surveillance and cyber activities in Donbas region of eastern Ukraine); KHAYRALLAH AL-HILU, AFRIN UNDER TURKISH CONTROL: POLITICAL, ECONOMIC AND SOCIAL TRANSFORMATIONS, 3–5 (2019) (describing Turkish intelligence network in occupied parts of northern Syria).

I
SURVEILLANCE, DATA COLLECTION AND DATA MINING IN OCCUPIED TERRITORY

A BIOMETRIC DATABASES

It's no secret that the occupied Palestinian territory is Israel's proving grounds for emerging technologies and the capabilities of its military intelligence units, most prominently its signals intelligence corps, Unit 8200.[11] With biometrics — the "automated recognition of individuals based on their biological and behavioural characteristics" such as fingerprints, facial structure, irises, palm veins, or DNA[12] — the process began with the Basel system of biometric work permits for Palestinian workers in Israel and biometric verification at checkpoints, first implemented in 1999 for Gaza Strip residents[13] and extended to the West Bank around 2005.[14] The biometric ID supplemented the non-biometric magnetic cards which entered into circulation in 1998 and would become a prerequisite for a permit to work in Israel.[15] Until 2007, Israeli policy was only to issue magnetic cards to Palestinians vetted and approved by Israel's internal security service, the Shabak.[16] Since 2007, COGAT has issued magnetic cards to Palestinians not approved by the Shabak to work in Israel, transforming the card from a confirmation of security-vetting to a form of identification only.[17]

The Basel system served as the technological basis for the Moaz biometric system for non-Palestinian foreign workers in Israel, which

11 *See* Amos Barshad, *Inside Israel's lucrative—and secretive—cybersurveillance industry*, REST OF WORLD (Mar. 9, 2021), https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/; Hagar Shezaf & Jonathan Jacobson, *Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays*, HAARETZ (Oct. 20, 2018), https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027; JEFF HALPER, WAR AGAINST THE PEOPLE: ISRAEL, THE PALESTINIANS AND GLOBAL PACIFICATION (2015).

12 Martin Zwanenburg, *Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law*, 97 INT'L L. STUD. 1404, 1406 (2021), citing the International Organization for Standardization (ISO) definition of biometrics.

13 Privacy International, *Biometrics and Counter-Terrorism: Case Study of Israel/Palestine*, 9 (2021), https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israelpalestine.

14 Amira Hass, *The Yearnings for a Magnetic Card*, HAARETZ (May 9, 2007), https://www.haaretz.com/1.4819750.

15 Privacy International, *supra* note 13, at 9.

16 Formally known as the General Security Service and also known by its Hebrew initials, Shin Bet.

17 Hass, *supra* note 14.

launched in 2004.[18] Subsequently, Israel's interior ministry pushed to create a national biometric identification system. That effort, which included a voluntary pilot programme launched in 2013, culminated in a 2017 law that made biometric IDs mandatory for Israeli citizens and residents.[19] As a product of the democratic process, the final law made certain compromises in favour of privacy, such as revocable consent to fingerprint storage.[20]

B FACIAL RECOGNITION CHECKPOINTS

In late 2018, Israel began to add facial recognition technology to its checkpoints.[21] To use the facial recognition scanners, which expedites the crossing process, Palestinians must be fingerprinted and photographed at a DCO. The facial recognition software was developed by Israeli firm AnyVision, which was recently rebranded Oosto.[22] By August 2019, the Israeli military said that 450,000 West Bank Palestinians were registered in the biometric database.[23]

C REAL-TIME IDENTIFICATION BY FACIAL RECOGNITION

Blue Wolf is a project of the information technologies command implementation unit of the Israeli military's central command.[24] It consists of

18 Privacy International, *supra* note 13, at 9.

19 Inclusion of Biometric Means of Identification and Biometric Identification Data in Identity Documents and in an Information Database Law (Amendment and Temporary Order), 5777-2017.

20 See generally Michelle Spektor, *Imagining the Biometric Future: Debates Over National Biometric Identification in Israel*, 29 SCIENCE AS CULTURE 100 (2020).

21 Amitai Ziv, *This Israeli Face-recognition Startup Is Secretly Tracking Palestinians*, HAARETZ (July 15, 2019), https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359. The literature often differentiates "internal checkpoints" from "border crossings", irrespective of whether the "border" being crossed is the 1949 armistice line, the Israeli separation barrier, or checkpoints separating East Jerusalem from other West Bank territory.

22 The company is called AnyVision herein because it is identified as such in all relevant materials. *See Visual AI Company AnyVision Changes its Name to Oosto*, BUSINESSWIRE (Oct. 27, 2021), https://www.businesswire.com/news/home/20211027005340/en/Visual-AI-Company-AnyVision-Changes-its-Name-to-Oosto. AnyVision sells a facial recognition access-control product, Abraxas (now called OnAccess), based on the same technology. *See* https://oosto.com/wp-content/uploads/2021/10/oosto-touchless-access-control-brochure.pdf.

23 Daniel Estrin, *Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns*, NPR (Aug. 29, 2019), https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc.

24 לוחכ באז"ל סג רתוא רופהת השדה הקלחמ ?ש"ויאב וק ספות [Stationed at a post in the West Bank? A new platoon will turn you into a 'blue wolf'], ISRAEL DEFENCE FORCES (June 15, 2021), https://www.idf.il/לוחכ-באז-ימחול-היגולונכט-תוכרדה-בושקת-זכרמ-דוקיפ-העמטה-תקלחמ/רבסב-הנגההו-בושקתה-חגא/סירתא/.

a smartphone app linked to a database of images of Palestinian residents of the occupied territory. A soldier scans either the subject's face or the magnetic strip on their identity card and the app alerts the soldier using a colour-coded system whether the subject should be allowed to pass, be detained for questioning, or be arrested. If the subject does not appear in the database, the solider may add them by photographing him or her and inputting personal details taken from the ID card.[25] The military reportedly developed the database through CCTV surveillance, social media data-mining, and assigning soldiers on patrol to photograph as many Palestinians as possible.[26]

White Wolf is a smartphone app employing the same technology and possibly linked to the same database as Blue Wolf, which allows volunteer security personnel in West Bank settlements to scan the ID cards of Palestinians before they enter the settlement.[27]

D VIDEO SURVEILLANCE WITH BEHAVIOUR-PREDICTIVE MACHINE LEARNING

The Israeli and international media have widely reported that Israel has deployed AnyVision's facial recognition technology throughout the West Bank to "spot and monitor potential Palestinian assailants", for which AnyVision won the Israel Defence Prize.[28] This program, although officially denied by AnyVision,[29] reportedly employs the same technologies as an AnyVision commercial product, Better Tomorrow (now called OnWatch), which combines facial and body recognition with machine learning to identify suspicious behaviour.[30] AnyVision claims that Better Tomorrow "can trace a person-of-interest across multiple cameras; find repeated appearances of an individual; detect suspects and suspicious objects caught on camera; rapidly perform historic video analysis for

25 Elizabeth Dwoskin, *Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank*, WASHINGTON POST (Nov. 8, 2021), https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

26 *Id*.

27 *Id*.

28 Ziv, *supra* note 21. The programme is reportedly nicknamed Google Ayosh despite no connection to Google, *Ayosh* being a Hebrew acronym for the West Bank. Olivia Solon, *Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?*, NBC NEWS (Oct. 28, 2019), https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116; *AnyVision Interactive Technologies*, WHO PROFITS (July 17, 2019), https://www.whoprofits.org/company/anyvision-interactive-technologies/.

29 *Joint statement by Microsoft & AnyVision*, M12 (Mar. 27, 2020), https://m12.vc/news/joint-statement-by-microsoft-anyvision.

30 https://oosto.com/wp-content/uploads/2021/10/oosto-onwatch-overview.pdf.

forensic purposes; and extract, analyze and store face images of all individuals who pass within a camera's view".[31] The platform also supports heat mapping which can detect crowd formations and traffic patterns. Better Tomorrow reportedly can be used with most types of CCTV cameras without elaborate retrofitting.[32]

Video surveillance in Jerusalem's Old City is long-standing, comprehensive, open and notorious. Roughly 40,000 residents, the vast majority of them Palestinian, live within the 0.9-square kilometre walled enclosure. The video surveillance system therein is known as Mabat 2000, reflecting the year of its introduction. Its 400 CCTV cameras monitor roughly 90 per cent of the Old City's public areas. As of 2011, the Israeli police operated the system without a code of practice restricting its permissible uses (e.g. forbidding inspection of private residential or commercial properties) or governing data retention;[33] whether that remains the case is unclear. In 2017, the Israeli government upgraded Mabat 2000 with facial recognition capabilities.[34] A 2014 Israeli government resolution expanded the Mabat surveillance model into the Kedem sub-district of the Jerusalem District Police, covering Palestinian neighbourhoods north of the Old City.[35] Mabat Kedem is known to include CCTV cameras with licence-plate capture capabilities.[36] The Israeli military has established a real-time video surveillance system in and around Hebron's Old City, where roughly 700 settlers live interspersed amongst 34,000 Palestinians, which reportedly operates similarly to Mabat 2000.[37]

Video surveillance extends to the West Bank road network. TSG IT Advanced Systems, a parastatal Israeli firm specialising in command-and-control systems, video analysis and behaviour-predictive artificial intelligence (AI), has developed and deployed an analytic CCTV system with facial recognition capabilities for the West Bank road network that can reportedly locate a car according to its licence plate, model and colour, identify irregular behaviour, and send automatic alerts.[38]

31 Privacy International, *supra* note 13, at 15–16.

32 *8 AI-based video analytics platforms advance security implementation,* ASMAG.COM (July 29, 2019), https://www.asmag.com/showpost/28633.aspx.

33 Usama Halabi, *Legal Analysis and Critique of Some Surveillance Methods Used by Israel, in* SURVEILLANCE AND CONTROL IN ISRAEL/PALESTINE: POPULATION, TERRITORY AND POWER, 210–11 (Elia Zureik, David Lyon, and Yasmeen Abu-Laban eds., 2010).

34 Who Profits, "Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem, 11–12 (2018).

35 Government of Israel resolution 1775 (June 29, 2014).

36 Who Profits, *supra* note 34, at 11–12.

37 The surveillance network is called "Hebron Smart City" in media reports. Dwoskin, *supra* note 25. For a map of CCTV installations in Hebron, see *Map*, MAPPING THE APARTHEID, https://www.hebronapartheid.org/mapPDF/CAMERAS.pdf.

38 Ami Rojkes Dombe, *Our Vision Is to Become a World Leader in the Field of C2 and Intelligence,* ISRAEL DEFENSE (Jan. 12, 2018), https://www.israeldefense.co.il/en/node/32613.

E SPYWARE AND OTHER CYBER TOOLS

NSO Group, maker of the now-infamous Pegasus spyware,[39] is an Israeli firm founded by former Unit 8200 members. The Israeli defence ministry's export control agency licenses NSO to sell Pegasus abroad.[40] NSO's export licence stipulates that only the Israeli security services are authorised to monitor Israeli (+972) and Palestinian (+970) phone numbers, and NSO has stated that Pegasus is not authorised for use against Israeli (or US) phone numbers.[41]

On 16 October 2021, the Palestinian NGO Al-Haq contacted forensic investigators with suspicions that an employee's smartphone had been targeted with spyware. Investigators checked the devices of 75 employees of West Bank-based civil society organisations and determined that six had been hacked using Pegasus at various times between July 2020 and April 2021.[42] On 19 October 2021, the Israeli defence ministry declared six Palestinian civil society organisations to be terrorist organisations for their alleged affiliation with the Popular Front for the Liberation of Palestine, a Palestinian political faction with a paramilitary wing which is banned by Israel.[43] Three of the six individuals whose devices were hacked agreed to be named; all three worked at one of these proscribed organisations.

In November 2021, Palestinian government officials made an uncorroborated allegation that Israel had used Pegasus to spy on three senior diplomats working on Palestine's referral to the International Criminal Court.[44]

Beyond NSO, the Israeli cyber tools industry is vast and reliable details regarding the deployment of these tools in the occupied territory

39 Dana Priest, Craig Timberg & Souad Mekhennet, *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, WASHINGTON POST (July 18, 2021), https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/.

40 In response to the Pegasus scandal, Israel updated its export control policy governing cyber systems and updated its end-user declaration. *See Israel MoD tightens control of cyber exports*, ISRAEL MINISTRY OF FOREIGN AFFAIRS (Dec. 7, 2021), https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021.

41 Patrick O'Neill, *Inside NSO, Israel's billion-dollar spyware giant*, MIT TECHNOLOGY REVIEW (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/; Amitai Ziv & Amira Hass, *NSO Spyware Used Against Palestinian Activists From NGOs Israel Outlawed, Report Says*, HAARETZ (Nov. 8, 2021), https://www.haaretz.com/israel-news/.premium.HIGHLIGHT-nso-spyware-used-against-palestinian-activists-in-black-listed-ngos-report-says-1.10363231.

42 *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware*, AMNESTY INTERNATIONAL (Nov. 8, 2021), https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.

43 *The Minister of Defense designated six organizations of the "Popular Front for the Liberation of Palestine" as terror organizations*, NATIONAL BUREAU FOR COUNTER TERROR FINANCING IN ISRAEL (Oct. 19, 2021), https://nbctf.mod.gov.il/en/Pages/211021EN.aspx.

44 Patrick Kingsley & Rawan Sheikh Ahmad, *Palestinian Diplomats Targeted by Israeli Spyware, Official Says*, N.Y. TIMES (Nov. 11, 2021), https://www.nytimes.com/2021/11/11/world/middleeast/israel-palestinian-nso-hacking.html.

are thin. It bears noting, however, that Israel's military may procure versions of these tools unencumbered by export control restrictions.

F IMPLICATIONS AND LIMITATIONS

These surveillance technologies enhance Israel's formidable human and signals intelligence apparatus in the occupied territory, including its network of informants.[45] They consolidate Israeli spatial control of the occupied territory by creating a data trail of movement across a dynamic constellation of "land cells" created by the checkpoints and permit regime,[46] with a view towards discouraging movement altogether — what Ariel Handel calls "exclusionary surveillance".[47] These surveillance technologies are now an integral part of the Israeli separation wall's "associated régime" of administrative measures, including permits and ID cards, which the International Court of Justice considered to "gravely infringe a number of rights of Palestinians".[48] Whether the isolating and self-disciplining effect of video surveillance in Jerusalem and Hebron,[49] the use of digital surveillance to augment the recruitment of collaborators, or the use of spyware in efforts to discredit civil society organisations, the surveillance technologies deployed in the occupied territory render Palestinian society more atomised, more riven with suspicion, and less capable of mobilising against Israeli rule.

Any remedial effort grounded in the law of occupation must confront "the inherent limitations of existing IHL, which at its core is concerned with the physical effects of armed conflict."[50] These limitations are highlighted by the debate over whether data has an object-quality, and thus whether cyber attacks must comply with the principles of distinction, proportionality and precautions in attack.[51] Additionally, the emerging technologies surveyed above, with the possible exception of offensive cybertools, would not seem to constitute means or methods of warfare

45 *See generally* SURVEILLANCE AND CONTROL IN ISRAEL/PALESTINE, *supra* note 33; IAN BLACK & BENNY MORRIS, ISRAEL'S SECRET WARS: A HISTORY OF ISRAEL'S INTELLIGENCE SERVICES (1992).

46 *See generally* Ariel Handel, *Where, Where to, and When in the Occupied Territories: An Introduction to Geography of Disaster*, in THE POWER OF EXCLUSIVE INCLUSION: ANATOMY OF ISRAELI RULE IN THE OCCUPIED PALESTINIAN TERRITORIES 179-226 (Michal Givoni, Sari Hanafi & Adi Ophir eds., 2009).

47 Ariel Handel, *Exclusionary Surveillance and Spatial Uncertainty in the Occupied Palestinian Territories*, in Zureik, Lyon and Abu-Laban, *supra* note 33, 259, 270.

48 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 193 (July 9).

49 Dwoskin, *supra* note 25.

50 Robin Geiß & Henning Lahmann, *Data Protection in Armed Conflict*, VERFASSUNGSBLOG (Feb. 15, 2021), https://verfassungsblog.de/data-protection-in-armed-conflict/.

51 *Id.*

subject to legal review before deployment.[52] Given these limitations, if the law of occupation is to offer protection from the coercive effect of emerging surveillance technologies, that defence will be located in the rights of the civilian population rather than restraints on the technologies directly.

II
PRIVACY AND THE LAW OF OCCUPATION

As the last major codifications of *jus in bello* occurred in the late 1940s and mid-1970s, the black-letter law of occupation says little about privacy.[53] It obviously says nothing about data collection practices by an occupying power and the data privacy rights of the occupied territory's protected persons. The *travaux préparatoires* of the Universal Declaration of Human Rights and the European Convention on Human Rights, as the human rights contemporaries to the Geneva Conventions of 1949, show that the right to privacy was incorporated "as an afterthought".[54] The same is true of the International Covenant on Civil and Political Rights (ICCPR) a generation later.[55] Privacy was scarcely mentioned in the Diplomatic Conference which studied and endorsed Additional Protocols I and II to the Geneva Conventions and in the myriad General Assembly resolutions on *respect for human rights and armed conflict* adopted before and during the Diplomatic Conference.[56]

To the extent that one can derive a right to digital privacy from conventional IHL, the starting point is Article 27 of Convention (IV), which establishes the general standard of treatment of protected persons. The provisions of Article 27 potentially relevant to privacy are the duty to show protected persons "respect for their persons, their honour, [and]

52 Zwanenburg, *supra* note 12, at 1413-1415; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 36, 1125 U.N.T.S. 3 (June 8, 1977).

53 Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, in Research Handbook on Human Rights and Humanitarian Law Further Reflections and Perspectives 463, 464 (Robert Kolb, Gloria Gaggioli and Pavle Kilibarda eds., 2022).

54 Vivek Krishnamurthy, *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy*, 114 Am. J. Int'l L. Unbound 26, 27 (2020).

55 *Id*.

56 Starting with G.A. Res. 2444 (XXIII) (Dec. 19, 1968), based on the eponymous resolution adopted at the Tehran Conference on Human Rights earlier that year.

their family rights"; the duty to afford them humane treatment; and the article's reservation clause, which recognizes the occupying power's authority to institute control and security measures.

Article 27's guarantee of respect for persons, honour and family rights has the same connotations and coverage as "family honour and rights" in Article 46 of the 1907 Hague Regulations: protection against "arbitrary interference" with the home, "marriage ties", and the "community of parents and children which constitute a family".[57] This drafting history would not seem to invite an expansive interpretation of family rights such as that which the Human Rights Committee has given to Article 17 ICCPR.[58] Nevertheless, one path towards a right to digital privacy, consistent with the principle of IHL-human rights law complementarity, would be to interpret "family rights" synonymously with the dyad "privacy [and] family" or "private and family life" as used in Article 17 ICCPR and Article 8 ECHR, respectively. The Pictet commentary to Convention (IV) hints at this normative convergence with human rights law.[59] Recalling that the high contracting parties narrowly voted down a more robust preamble with "respect [for] the principles of human rights which constitute the safeguard of civilization" as part of the Convention's object and purpose,[60] the commentary asserts that Article 27 fills that interpretative void and "reflect[s] the spirit which imbues the whole Convention in regard to the rights of the individual."[61]

Beyond the concept of family honour, "respect for honour" as used in Article 27 of Convention (IV) also means what it does in Article 14 of Convention (III): protection against libel, slander, insult, and "any violation of secrets of a personal nature."[62] The updated commentary to Convention (III) observes that new surveillance technologies implicate "the right of prisoners to respect for their persons and honour."[63] The new commentary submits that "limited, well-regulated and well-managed video surveillance" in prisoner-of-war camps "should not in principle be considered as prohibited" by Article 14 insofar as it may prevent or

57 International Committee of the Red Cross (ICRC), Commentary to Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War 202 (Oscar Uhler and Henri Coursier, eds., 1958) ('Convention (IV) Commentary'); 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, art. 46 (Oct. 18, 1907) ('Hague Regulations').

58 Human Rights Committee, General Comment No. 16, ¶ 5 (Apr. 8, 1988).

59 Convention (IV) Commentary, *supra* note 57, at 207.

60 *Id*. at 12.

61 *Id*. at 200.

62 ICRC, Commentary to Geneva Convention (III) Relative to the Treatment of Prisoners of War 145 (Jean de Preux et al eds., 1960); *compare* Convention (IV) Commentary, *supra* note 57, at 202.

63 ICRC, Updated Commentary on Geneva Convention (III) Relative to the Treatment of Prisoners of War ¶ 1674 (2021) ('Updated Convention (III) Commentary').

deter escape or suicide attempts, abuse by guards, and intra-prisoner violence.[64] In contrast, constant video surveillance of all prisoners would seem disproportionate and would thus be prohibited, as would filming family visits and bathroom use "if other ways to prevent security breaches … would be equally effective."[65] The updated commentary, which confines its analysis of new surveillance technologies to video monitoring and electronic tracking bracelets, cites no authorities for these principles and standards.[66] The forthcoming updated commentary to Convention (IV) faces the far greater task of addressing the various technologies used by occupying powers to surveil an entire civilian population.

Article 27 also requires that protected persons in occupied territory be "humanely treated" and protected from "*tout acte de violence ou d'intimidation, contre les insultes et la curiosité publique*", an identical formulation to Article 13 of Convention (III) on the humane treatment of prisoners of war.[67] While the Pictet commentaries to Conventions (III) and (IV) define humane treatment in general and largely tautological terms, the ICRC's updated commentary to Convention (III) interprets this duty of protection to prohibit all forms of physical or psychological abuse and humiliation.[68] The updated commentary also observes that "protection from public curiosity has gained particular relevance… owing to the rapid developments in communication technology", "mass media in the coverage of armed conflicts", and "the ubiquity of social media as a means of distributing both images and comment".[69] But while taking and disseminating Abu Ghraib-type images of detainee abuse to humiliate an enemy clearly violate this prohibition,[70] its application in the Convention (IV) context poses tougher, highly contextual questions — for example, whether and in

64 *Id.* ¶¶ 1675-1676. The updated commentary also states that measures of "special surveillance" imposed on a prisoner-of-war following an escape attempt pursuant to article 92 must be "necessary, proportionate to their intended aim and serve a legal purpose". *Id.* ¶ 3840.

65 *Id*. ¶ 1677.

66 The Updated Convention (III) Commentary has been criticised for underweighting State operational practice relative to military manuals and other secondary sources. In this vein, *see* Michael Meier, *The Updated GC III Commentary: A Flawed Methodology?*, ARTICLES OF WAR (Feb. 3, 2021), https://lieber.westpoint.edu/updated-gciii-commentary-flawed-methodology/.

67 This phrase originates in Article 2 of the 1929 Geneva POW Convention, the predecessor to Convention (III). The English version of Article 27 of Convention (IV) prohibits "all acts of violence or threats thereof and against insults and public curiosity", without using the term *intimidation*, which appears in the French text. The French and English versions of the Conventions are equally authentic.

68 Updated Convention (III) Commentary, *supra* note 63, ¶ 1563.

69 *Id*.

70 *See American Civil Liberties Union v. Department of Defense*, 543 F.3d 59, 90 (2nd Cir. 2008), *vacated on other grounds*, 558 U.S. 1042 (2009) (in case concerning public disclosure of photographs depicting abusive treatment by US forces in Iraq and Afghanistan, holding that "Article 13 of the Third Geneva Convention and Article 27 of the Fourth Geneva Convention do not prohibit dissemination of images of detainees being abused when the images are redacted so as to protect the identities of the detainees, at least in situations where… the purpose of the dissemination is not itself to humiliate the detainees".)

what circumstances non-consensual photographing of protected persons for facial recognition purposes (such as Blue Wolf) goes beyond a legitimate security measure and constitutes instead a form of intimidation or humiliation.

Article 27's reservation clause recognizes the occupying power's right to take "such measures of control and security in regard to protected persons as may be necessary as a result of the war." The Convention (IV) commentary suggests that "necessary" as used in this reservation is more permissive than the concept of military necessity.[71] This interpretation is bolstered by Article 78, which in contrast with Article 27's general standard for security measures requires "imperative reasons of security" for two exceptional control and security measures: internment and assigned residence. The Pictet commentary to Convention (IV) provides a non-exhaustive list of examples of permissible measures, including less intrusive restrictions such as requiring the carrying of identity cards—which can by analogised to include the use of technologies that identify those permitted access and restrict those considered a security risk.

Article 75 of Additional Protocol I expands the protections of Article 27 of Convention (IV) by prohibiting discrimination in the enjoyment of Convention rights based *inter alia* on "political or other opinion" and enshrining respect for non-religious "convictions" on top of existing protections for religious beliefs and observance. Respect for convictions "implies that a person professing any particular convictions cannot be arrested or imprisoned for this reason alone" and stands as the non-derogable counterpart to the derogable right to free expression under Article 19 ICCPR.[72]

Upon this sparse framework of conventional IHL, those who would advocate for a more robust concept of privacy in the law of occupation urge an evolved understanding of humane treatment. Eyal Benvenisti, for one, does so by appealing to the common origins of IHL and human rights law in human dignity. He suggests "the principle of human dignity arguably obliges the occupying army to treat enemy nationals under its control as ends and not merely as means" — that a warring army's

71 Convention (IV) Commentary, *supra* note 57, at 207 (stating of security measures anticipated by Article 27's reservation clause: "[a] great deal is thus left to the discretion of [the occupying power] as regards the choice of means"). *Military necessity* permits measures necessary to accomplish a legitimate military objective that are not otherwise prohibited. *Military necessity*, ICRC Online Casebook, https://casebook.icrc.org/glossary/military-necessity. Legitimate military objectives in occupation are to restore and ensure public order in the occupied territory (with law enforcement and judicial measures favoured over the use of force) and to provide for military security. *See* MARCO LONGOBARDO, THE USE OF FORCE IN OCCUPIED TERRITORY, 238–40 (2008).

72 ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 871 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

"attenuated duties" to *respect* certain rights of the enemy's civilian population are transformed by exclusive control of the territory into a duty to *ensure* a wider array of rights.[73]

A variant of this move is to extrapolate an evolving right to privacy from the local law predating the occupation, rather than human rights law or notions of human dignity. In this vein is a recent article which considered the data gathering and storage practices alleged by Unit 8200 "refuseniks" and concluded that these practices ran afoul of Article 43 of the Hague Regulations because they violated the right to privacy enshrined in the Jordanian and Egyptian constitutions applicable in the West Bank and Gaza, respectively, when the occupation commenced, and were not justified by military necessity.[74] But adequately regulated uses of surveillance technologies might equally be viewed as legitimate measures to restore public order and civil life in a manner consistent with this evolving right to privacy, with its focus on data subject rights rather than the outright prohibition of mass surveillance.

The absence of express rights to privacy and data protection in conventional IHL is unlikely to change anytime soon. As Amanda Alexander has illustrated, however, the ascendancy of the humanitarian dimension of *ius in bello* is recent, historically contingent, fitful in its development, and less attributable to States and the ICRC than the conventional narrative of continuity suggests.[75] Alexander has documented how human rights organisations played an outsized role in building consensus regarding the customary status of large swathes of Additional Protocol I, persistent objectors notwithstanding.[76] So, too, might non-State actors take the lead on digital privacy and data protection in times of occupation, whether through interpretations of IHL of the types just described or by appeal to human rights law, to which we now turn.

73 Eyal Benvenisti, The International Law of Occupation, 90 (1st ed. 2006).
74 Benjamin Waters, *An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories*, 50 Geo. J. Int'l L. 573, 590–94 (2019). Peter Beaumont, *Israeli intelligence veterans refuse to serve in Palestinian territories*, Guardian (Sept. 12, 2014), https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories.
75 Amanda Alexander, *A Short History of International Humanitarian Law*, 26 Eur. J. Int'l L. 109 (2015).
76 *Id.* at 126–35.

III
DOES THE HUMAN RIGHTS FRAMEWORK FOR DIGITAL PRIVACY AND DATA PROTECTION RIGHTS TRANSLATE TO THE OCCUPATION CONTEXT?

As Asaf Lubin notes, while "IHL will more often than not be silent" as to emerging surveillance technologies, human rights law "has been developing at a far faster rate" to address the challenges such technologies pose.[77] This raises the question of the interoperability of IHL and human rights law, the subject of a vast literature which has yielded two prevailing views.[78] The first, complementarity, posits their concurrent application and mutually informed interpretation. The second, conflict resolution, posits that true conflicts between the regimes, while perhaps rare, do exist and cannot be resolved by appeal to a normative hierarchy but only by policy choices.[79] The questions are thus to what extent digital privacy and data protection as they are developing in human rights law can apply concurrently and without conflict to the law of occupation; and where there are conflicts, which policy interests should be prioritised in mediating their resolution. This section focuses on the former question and leaves the latter for another day.

Other contributions in this volume closely examine these developments in human rights law, which we need only summarise here. Lubin, while acknowledging that "at the international level, data protection remains fragmented and weak",[80] identifies six "emerging norms" of a right to digital privacy and data protection: data collection and processing that is (1) "lawful, fair and transparent", i.e. legally-grounded and restricted, and (2) accurate, complete, and up-to-date; (3) "purpose

77 Lubin, *supra* note 53, at 482.

78 For an account of interoperability specific to occupation rather than active hostilities, see LONGOBARDO, *supra* note 71, at 81–82.

79 Leah West's contribution in this volume surveys the interoperability literature and the conflict resolution model specifically; see Leah West (Chapter 7 of this collection). See also Lubin, *supra* note 53, at 481 and notes 112–13, discussing proposed conflict resolution heuristics. This view presupposes that the *lex specialis* principle, appropriately understood, does not dictate such a hierarchy and generally obscures the policy preferences at work. *See* Marko Milanovic, *The Lost Origins of Lex Specialis, in* THEORETICAL BOUNDARIES OF ARMED CONFLICT AND HUMAN RIGHTS, 78 (Jens David Ohlin ed., 2016).

80 Lubin, *supra* note 53, at 473 (citing to Kriangsak Kittichaisaree and Christopher Kuner, *The Growing Importance of Data Protection in Public International Law*, EJIL: TALK! (Oct. 14, 2015), available at https://www.ejiltalk.org/the-growing -importance-of-data-protection-in-public-international-law/); *compare* G.A. Res. 69/166, ¶ 4 (Dec. 18, 2014).

and storage specification and limitation" such that data should be kept in personally-identifiable form no longer than required for the express purpose it was collected; (4) individual participation, encompassing the right to know of and object to processing of personal data, and to rectify, block access to, and erase that data; (5) integrity and confidentiality, including reasonable protection from security breaches and other unauthorised disclosures; and (6) "due process, supervision and legal sanction" to ensure compliance with these principles, e.g. by establishing a data protection authority.[81]

I leave aside my doubts as to whether these norms are emerging beyond European frontiers[82] and assume their eventual place in the corpus of international human rights law.[83] I have more acute doubts whether these norms can be made interoperable with the law of occupation without exacerbating the tensions plaguing the latter regime.

The Strasbourg Court in *Big Brother Watch v. United Kingdom* defined the procedural safeguards required of bulk interception regimes in eight principles broadly similar to Lubin's six.[84] The court conceptualised mass surveillance's infringement upon privacy rights as a sliding scale: least upon the initial interception of data, increasing with its storage and automatic processing, and peaking upon review by an intelligence analyst.[85] In the court's analysis, however, the increasing infringement on privacy only warrants more exacting scrutiny of the State's procedural safeguards; it does not require proportionality by the substantive metric of greater functionality and effectiveness.[86] The court reserved judgments regarding the need for particular mass surveillance programmes to the State's margin of appreciation.[87] *Big Brother Watch* can thus be viewed as a further stage in the Strasbourg Court's so-called procedural turn towards inferring substantive compliance from procedural due diligence.[88]

The problem for interoperability purposes is that this procedural approach to digital privacy and data protection — examining the internal

81 Lubin, *supra* note 53, at 475–76.
82 *See* Report of the Special Rapporteur on the right to privacy, U.N. Doc. A/HRC/34/60, ¶ 15 (Sept. 6, 2017) (observing regression at national level in legislative regulation of surveillance).
83 Or perhaps even beyond the EU's frontiers – Norway argued in *Big Brother Watch* that the Strasbourg Court should not import "concepts and criteria" from the data protection jurisprudence of the Court of Justice of the European Union applying the EU Charter of Fundamental Rights. *See* Big Brother Watch v. United Kingdom [GC], Nos. 58170/13, 62322/14 & 24969/15, ¶ 310 (May 25, 2021).
84 *Id*. ¶ 361; *see also id.* ¶¶ 348–59.
85 *Id*. ¶ 330–31.
86 Monika Zalnieriute, *Procedural Fetishism and Mass Surveillance under the ECHR*, VERFASSUNGSBLOG (June 2, 2021), https://verfassungsblog.de/big-b-v-uk/.
87 Big Brother Watch, *supra* note 83, ¶ 347.
88 Zalnieriute, *supra* note 86; Eva Brems, *Procedural Protection: An Examination of Procedural Safeguards Read into Substantive Convention Rights*, *in* SHAPING RIGHTS IN THE ECHR 135 (Eva Brems & Janneke Gerards eds., 2013).

regulation of a surveillance regime's operations without scrutinising the regime's necessity and proportionality[89] — rests on a theory of *procedural democracy* which is inapposite in the context of military occupation. As Janneke Gerards has argued, procedural democracy theories support judicial deference until and unless the relevant legislative or administrative procedure is "suspected to be defective to the extent that even its own corrective mechanisms cannot be trusted any more".[90] Accordingly, the proceduralisation of data protection reflected by *Big Brother Watch* relies upon the "formal jurisdictional division of tasks" on the national plane, to say nothing of supranational judicial supervision.[91]

Military occupation does not admit of this jurisdictional division. Whether or not the occupying power establishes a special administration for the occupied territory, even one staffed heavily by civilians, "the government of an occupied territory is military *per definitionem*" and invariably defaults to a military posture.[92] Yael Berda has illustrated that establishing a civil administration as the occupation's bureaucracy in the 1980s and the Palestinian Authority as the local authority in parts of the occupied territory a decade later counterintuitively increased the involvement of the military and the Shabak in the daily affairs of the Palestinian population, as these institutions transitioned to indirect rule through control of the population registry and a permit regime.[93] When the second intifada erupted, the Shabak, "through its monopoly of intelligence and classification of Palestinians" according to the perceived security threat, solidified a dominance over the bureaucracy which it maintains today.[94]

Judicial review of the military commander's decisions does not change this equation. While judicial review is a distinctive feature of the Israeli occupation, it is premised on Israeli administrative law;[95] it is neither a requirement in the law of occupation nor a standard feature of occupation regimes.[96] Leaving aside questions over the purpose of judicial review in the occupation context,[97] its availability feeds the liberal

89 Big Brother Watch, *supra* note 83, Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque, ¶ 33 ("The margin of appreciation must be the same, both for designing the system and for operating it, and this margin is a narrow one…").
90 Janneke Gerards, *Pluralism, Deference and the Margin of Appreciation Doctrine*, 17 EUR. L. J. 80, 118 (2011).
91 Oddný Arnardóttir, *The "Procedural Turn" under the European Convention on Human Rights and Presumptions of Convention Compliance*, 15 INT'L J. CONST. L. 9, 33 (2017).
92 YORAM DINSTEIN, THE INTERNATIONAL LAW OF BELLIGERENT OCCUPATION, 65 (2d ed. 2019); Longobardo, *supra* note 71, at 87.
93 YAEL BERDA, LIVING EMERGENCY: ISRAEL'S PERMIT REGIME IN THE OCCUPIED WEST BANK 20–31 (2018).
94 *Id.* at 31–35.
95 DAVID KRETZMER & YAEL RONEN, THE OCCUPATION OF JUSTICE, 31 (2d ed. 2021).
96 EYAL BENVENISTI, THE INTERNATIONAL LAW OF OCCUPATION, 325–27 (2d ed. 2012).
97 See, e.g., Nimer Sultany, *Activism and Legitimation in Israel's Jurisprudence of Occupation*, 23 SOC. & L. STUD. 315 (2014).

impulse that "injustices are necessarily caused by 'lawlessness' and that applying more norms will always be beneficial".[98] Berda has shown how this impulse drove demands for a legally-defined and transparent Israeli permit regime for Palestinians, and how this effort ultimately backfired. Publication of the criteria for banning Palestinians from entering Israel satisfied "the norms of liberal administrative justice" but did nothing to rein in the discretion of the military, intelligence, and security services, other than to circumscribe their authority to make exceptions in individual cases.[99]

With this incongruence between procedural democracy and military occupation in mind, take Lubin's question of whether the law of occupation obligates Israel to conduct an impact assessment before deploying biometrics at checkpoints. Lubin reasons that the imperatives of data protection apply at checkpoints because the occupying power's activities there are administrative and bureaucratic, rather than military, in nature.[100] With respect, I cannot agree with that characterisation unless we are prepared to rethink the law of occupation, or to peek behind the curtain and make epistemological judgments about the nature and purpose of a given occupation.

Black-letter IHL regards checkpoints[101] as a manifestation of an occupying power's authority to regulate, restrict and temporarily suspend freedom of movement of civilians of the enemy nationality.[102] As an exercise of a military prerogative, they are fundamentally and invariably of a military character. Israel's choice to bureaucratise and digitise the checkpoints, with the effect that direct military-civilian encounters are reduced, does not change their function from military to administrative/bureaucratic. If data protection obligations attach at the checkpoints, it must for a reason other than their newfound banality.

Lubin's point, however, is that Israel's checkpoints ostensibly have little relation to this fundamental and invariable military character. They are not temporary and contravene the Geneva law's "idea of the personal freedom of civilians remaining in general unimpaired".[103] It is

98 Aeyal Gross, The Writing on the Wall: Rethinking the International Law of Occupation 396 (2017).
99 Berda, *supra* note 93, at 122–23.
100 Lubin, *supra* note 53, at 485.
101 I speak here only of checkpoints within the occupied territory, and not crossing points between the occupied territory and Israel. Given the territorial and functional integration of Israel/Palestine, due partly to settlements but also to the "economic annexation" of the occupied territory into Israel (*see* Benvenisti, *supra* note 96, at 241–44), Israeli jurisprudence concerning the occupied territory elides over the distinction between military security and Israeli national security. *See* Kretzmer & Ronen, *supra* note 95, at 136–37.
102 Convention (IV) Commentary, *supra* note 57, at 201–2.
103 *Id*. at 202 (Article 27's reservation clause does not countenance free movement "being suspended

questionable, then, whether the checkpoints are deployed consistent with the object and purpose of the law of occupation, i.e., for legitimate military interests that facilitate governing the occupied territory in accordance with IHL. If they rather serve to colonise the territory and abuse the protected population, an impact assessment of biometrics used at these checkpoints seems a misguided initiative.

One way to think beyond black-letter IHL is on the theory that the "normal" operation of checkpoints in accordance with security requirements, as opposed to their "exceptional" closure and re-militarisation, is a policing function governed by the law enforcement paradigm of human rights law. This is certainly true on the ground: virtually all the checkpoints are now run by private security companies rather than army personnel.[104] The private security guards who run those checkpoints in "normal" times clearly are neither combatants nor civilians taking a direct part in hostilities.[105] But the data gathering that occurs at checkpoints, and that enables their operation, remains a military prerogative. Moreover, decisions arising at checkpoints in "exceptional" times, justified on the basis of military necessity or military operations, must be made by military personnel.[106]

While I agree with Lubin that Palestinians do not lose their rights as data subjects because military rather than civilian authorities collect and process that data, there is something qualitatively different about data in the hands of the occupying power's armed forces. Although Lubin does not specify the source of the "purpose and storage specification and limitation" principle, one of the emerging norms he identifies, it might be located in the norm prohibiting otherwise-lawful restrictions on rights imposed for an improper purpose, reflected *e.g.* in article 18 ECHR and article 30 of the American Convention on Human Rights. This principle, which originates in French administrative law, starts from the presumption that the executive acts in good faith[107] and is constrained by functioning *contre-pouvoirs* (institutional controls).[108] The occupying power's control of data does not warrant a presumption against *détournement de*

in a general manner"); Handel, *Exclusionary Surveillance*, *supra* note 47, at 269 ("the checkpoint is not a surveillance apparatus but an uncertainty production post that is designed to control Palestinian movement – not to *regulate* it but to *minimize* it").

104 Leticia Armendáriz, The Privatization of Security in the Occupied Palestinian Territory, 20–25 (2016).

105 Private Security Companies in the Occupied Palestinian Territory: An International Humanitarian Law Perspective (Harvard Univ. Program on Humanitarian Pol'y and Conflict Res.), March 2008, at 9.

106 *Id.* at 13–14.

107 *See Khodorkovskiy v. Russia*, app. 5829/04 ¶ 255 (May 31, 2011).

108 See generally Aikaterini Tsampi, *The New Doctrine on Misuse of Power under Article 18 ECHR*, 38 Neth. Q. Hum. Rts. 134 (2020).

pouvoir (misuse of power) because (i) the relationship between the occupying power and the protected population is fundamentally an adversarial one and (ii) the concept of *contre-pouvoirs* is inapposite in the context of the military commander's unitary rule. The law of occupation, by its architecture, would thus not seem to admit of such a limitation: if intelligence gathering and storage is a legitimate security measure, then any bona fide military necessity would justify its use.

Let us revisit the Unit 8200 "refuseniks" who alleged that unit personnel "were instructed to keep any damaging details of Palestinians" lives they came across, including information on sexual preferences, infidelities, financial problems or family illnesses that could be "used to extort/blackmail the person and turn them into a collaborator".[109] The data collection should be distinguished from its potential misuses. An occupying power would insist that an enemy citizen's peccadillos (real or perceived) pose a threat to military security for the same reasons that infidelity, drug use or debts may be grounds for denying a security clearance to a prospective civil servant: they increase vulnerability to co-optation by groups proscribed by the military authorities, just as they do to recruitment as informants serving those authorities. The coordinated Western campaign against the Hamas social infrastructure in the occupied territory and its network of donors abroad is premised on just these assumptions: that "the mere provision of (often) free social services … suffices to mobilise support for the Islamist agenda" and that "the recipient community is deeply integrated into the operations and management of Islamic associations (such that its members are able to be indoctrinated and recruited)."[110] The reality is more nuanced, as Sara Roy has illustrated, and this recruitment scenario is quite reductionist.[111] Nevertheless, an occupying power would seem to have the prevailing "moral intuitions, … biases and preferences" of international authority on its side in claiming the collection and storage of personal data for this purpose as a reasonable security measure, recalling an occupying power's discretion to choose amongst security measures.[112] So the data collection would *prima facie* seem a legitimate security measure, recalling an occupying power's discretion in choosing such measures.

Misuse of that data for purposes of recruiting collaborators would not be for an absence of norms: Article 31 of Convention (IV) prohibits

109 Beaumont, *supra* note 74.
110 Sara Roy, Hamas and Civil Society in Gaza, 4 (2011).
111 *Id*.
112 Martti Koskenniemi, *Occupied Zone — "A Zone of Reasonableness"?*, 41 Isr. L. Rev. 13, 17 (2008).

an occupying power from obtaining information from protected persons, and by logical extension recruiting informants, through "physical or moral coercion".[113] The recruitment of collaborators nevertheless remains an enduring feature of modern occupations generally, and of the Israeli occupation.[114] Berda's cautionary tale of the unintended consequences of pursuing liberal justice in an illiberal, coercive context should give us pause. Do we genuinely need norms on data collection and storage to fill lacunae in IHL? Or are auxiliary norms that would constrain the technological enhancement of unlawful practices attractive because the primary norms against such practices have lost prescriptive force?[115] These are important questions, but not those I endeavour to explore in the remainder of this short contribution. Rather, in the next section, I query whether the worm-eaten law of occupation paradigm offers a sufficiently robust basis, even when combined with the evolving right to digital privacy and data protection in human rights law, for regulating the data practices of an occupying power.

IV
EPISTEMOLOGICAL QUESTIONS

The dust jacket to Yoram Dinstein's original monograph on the law of occupation calls the Israeli occupation of Palestinian territory the "paradigmatic illustration" of belligerent occupation.[116] That his second edition drops this characterisation speaks to a growing recognition that the Israeli occupation is anything but paradigmatic and that the law-of-occupation paradigm fails to capture its reality. Even for want of better contemporary examples, I have used the occupied Palestinian territory as a case study here with considerable hesitation.

The pre-eminence of Israel/Palestine in the contemporary law of occupation has reduced settlements and settlers to a topic within the law of occupation rather than a first principle of settler-occupations. The international lawyers who have countenanced this shift presumably

113 Geneva Convention (IV) art. 31; SHANE DARCY, TO SERVE THE ENEMY: INFORMERS, COLLABORATORS, AND THE LAWS OF ARMED CONFLICT 76–78 (2019)
114 *See generally* DARCY, id., at 24-28.; BERDA, *supra* note 93, at 60–65.
115 Alexander, *supra* note 75, at 125.
116 YORAM DINSTEIN, THE INTERNATIONAL LAW OF BELLIGERENT OCCUPATION, dust jacket and cover materials (1st ed. 2009).

have done so in the interest of cohesion — the desire not to fragment the law of occupation between short-term occupations, transformative occupations, settler-occupations, and other disfigurations of the paradigm — but at the expense of coherence. If the principles of IHL "operate a balance between the demands of humanity and the necessities of war", as Alain Pellet put it, the balance cannot be struck without reference to the war's objective.[117] The crisis in the law of occupation lies in the fact that its limitations on the objective of an occupation have not kept pace with IHL's limitations on the conduct of hostilities. This crisis is the theme of much contemporary scholarship on the law of occupation, and it cannot be ignored here.

Not all settler-occupations are alike, of course.[118] Situations like Israel/Palestine, where the occupying power seeks to exclude the protected population from the territory which it claims, and ultimately to disclaim responsibility for that population, must be distinguished from situations like Morocco/Western Sahara, where the occupying power claims the occupied territory *and* identifies the protected population as its citizens.[119] In the latter context, settlers and protected persons are, in theory, subject to the same data gathering methods *and* the same legal regime governing the data processing, usage and dissemination — the municipal law of the occupying power. Of course, Morocco's full and explicit exercise of sovereign powers in Western Sahara, like Russia/Crimea and other purported annexations, contributes nothing to the law of occupation.

In settler-occupations of the Israel/Palestine variety, meanwhile, settlers and protected persons encounter many of the same data gathering methods but are subject to different legal regimes governing data processing, usage and dissemination. Indeed, data harvesting in settler-occupations and the amount of data the State thereby acquires on settlers relative to its non-settler citizens might conceivably push the occupying power towards increasing data privacy protections in its municipal law. In the context of an indefinite occupation such as Israel/Palestine, the disparity in data protection between settlers and protected persons

117 Alain Pellet, *The Destruction of Troy Will Not Take Place, in* INTERNATIONAL LAW AND THE ADMINISTRATION OF OCCUPIED TERRITORIES 169, 187 (Emma Playfair ed., 1992).

118 For a comparative account of settler-occupations, *see generally* SETTLERS IN CONTESTED LANDS: TERRITORIAL DISPUTES AND ETHNIC CONFLICTS (Oded Haklai & Neophytos Loizides eds., 2015).

119 Thereby violating the basic principles of the law of occupation, namely that protected persons retain their nationality, do not acquire the nationality of the occupying power, and do not owe allegiance to the occupying power. The law of occupation, in theory, continues to govern notwithstanding these violations, as prescribed in Article 47 of Convention (IV).

acquires the character of systemic discrimination.[120] Insofar as human rights law is offered as a way to overcome IHL's silence on digital privacy and data protection, we must address the question of settlements and settlers, if only provisionally, lest we cherry-pick from the menu of human rights law while leaving aside its fundamental promise of non-discrimination.

Viewing international law as a communications process in which prescriptions are constantly challenged and are either reinforced by international authority or allowed to wither and die, one must question, however despairingly, whether the prohibition against settlements in occupied territory enjoys the prescriptive force that its elevated place in conventional IHL suggests,[121] even when their permanent and appropriative character is clear. International authority has declined to impose limits on extent of territorial change it would accept in a negotiated settlement that would end the Israeli occupation.[122] Further evidence of a frayed prescription lies in the fact that Israeli jurisprudence is widely accepted as a key component of the customary law of occupation, although premised on the understanding that the settlement project is a nonjusticiable political matter and a certain practical equivalence between settlers and protected persons.[123]

If settlers bend but do not break the law of occupation, one principle that cannot survive settlements is the notion of occupying power as trustee. It is nonsensical to speak of a settler-occupier acting as trustee of the protected population in administrative and bureaucratic affairs while it transforms the demographic composition of their territory and erodes the prospects of restoring popular sovereignty. Whether one reaches this conclusion from the premise that settlements fundamentally pervert the trust, as humanitarian lawyers are apt to,[124] or simply because occupying powers are not trustees, as military lawyers are apt to believe, matters

120 *See* Marco Longobardo, *Preliminary but Necessary: The Question of the Applicability of the Notion of Apartheid to Occupied Territory*, JUST SECURITY (Dec. 2, 2021), https://www.justsecurity.org/79381/preliminary-but-necessary-the-question-of-the-applicability-of-the-notion-of-apartheid-to-occupied-territory/ (concluding that "nothing in the law of occupation… would bar the application of the notion of apartheid to occupied territory", notwithstanding the distinction between the legal regimes of the occupying power and of the occupied territory).

121 Protocol I, *supra* note 52, art. 85(4)(a).

122 *See, e.g.*, S.C. Res. 2334 (Dec. 23, 2016) ¶¶ 1, 3, reaffirming that establishment of settlements in oPt "has no legal validity and constitutes a flagrant violation under international law" while declaring that the Council will not recognise any territorial changes "other than those agreed by the parties through negotiations"; U.N. Doc. S/2014/916 (Dec. 30, 2014) (draft resolution on parameters for Israeli-Palestinian permanent-status agreement, not adopted). On this topic, *see* Ardi Imseis, *Negotiating the Illegal: On the United Nations and the Illegal Occupation of Palestine, 1967–2020*, 31 EUR. J. INT'L L. 1055 (2020).

123 KRETZMER & RONEN, *supra* note 95, at 190–93, 217–31.

124 GROSS, *supra* note 98, at 36–39.

less than consensus on this point.[125] If we are called upon to decide between the law of occupation's traditional conservationist impulses and the legislative ambitions of self-professed "benevolent occupants",[126] in a settler-occupation the conservationist principle must prevail, recognising that this means a thinner law of occupation (or law of *an* occupation). The settler presence dictates, at minimum, that the conservationism of Hague law must prevail over the humanitarianism of Geneva law.

The question of settlements and settlers is thus relevant in identifying the source of the digital privacy and data subject rights of the occupied territory's protected population, assuming they have any. One could envisage locating these rights in (i) general international human rights law; (ii) an occupying power's general duty to "promote the interests of the civilian population";[127] (iii) the occupying power's domestic legislation; or (iv) the rights of settlers in the occupied territory, who are also subject to the authority of the military commander but may benefit from the extraterritorial application of wide swaths of the occupying power's domestic law and military orders applicable only to the settlements, as in the Israeli context.[128]

None of these approaches seems satisfactory. As examined in Part III, the principles comprising the right to digital privacy and data protection in human rights law remain nascent, at least outside the European context, and at least some of these principles are of questionable interoperability with the law of occupation. The application of Israeli domestic law *qua* Israeli law would be annexation.[129] Transposing Israeli domestic law to the occupied territory by military order would exceed the military commander's legislative authority. While this approach might promote the interests of the protected population in a narrow, decontextualised sense, in the context of a settler occupation it must be rejected as "the bear's hug" of the occupying power.[130] Certainly few would accept, for data privacy purposes or for any purpose, formal equivalence between settlers and protected persons. One might envisage, as a least-worst option and even at the risk of legitimating the illegitimate, the occupying power using its data handing and protection practices towards settlers as

125 Yoram Dinstein, The International Law of Belligerent Occupation 39 (2d ed. 2019).
126 Kretzmer & Ronen, *supra* note 95, at 143–47.
127 Lubin, *supra* note 53, at 483–84.
128 *See generally* Michael Karayanni, Conflicts in a Conflict: A Conflict of Laws Case Study on Israel and the Palestinian Territories 37–40, 72–76 (2014); Kretzmer & Ronen, *supra* note 95, at 222–26.
129 *Compare* Lubin, *supra* note 53, at 485 and note 127, characterising the non-application of Israel's biometrics law to the Palestinian population of the occupied territory as unjustified discrimination; *but see* Longobardo, *supra* note 120.
130 *See* Dinstein, *supra* note 125, at 132.

a *reference* in defining its duties towards protected persons, at least during the occupation's "normal" times and with respect to its administrative and bureaucratic aspects.

CONCLUSION

The challenge in locating a doctrinally satisfactory source for the digital privacy rights of protected persons and the data protection duties of an occupying power speaks to a classic legitimacy-versus-effectivity dilemma. When we speak of these rights and duties, are we envisaging the Platonic form of an occupation, in which the occupying power recognizes its status as such and thus the limits of its legislative authority, does not establish settlements, stakes no claim to any part of the occupied territory and seeks to end the occupation at the earliest opportunity? Or are we addressing the contemporary reality wherein the only occupying powers which acknowledge the applicability of the law of occupation also claim licence to establish settlements, undertake a political and economic transformation of the occupied territory, and so on? Put another way, if Hague Article 43 is a "mini-constitution" of an occupation regime,[131] can the law of occupation retain some semblance of universality when the few occupying powers of the modern era to have recognized the "constitutional" limits to their rule have nevertheless presented bespoke visions of *l'ordre et la vie publique* in the occupied territories? Any effort at developing universal digital privacy and data protection standards in times of armed conflict must reckon with this crisis in the law of occupation.

I do not suggest that the panoptic surveillance of occupied territory is acceptable. Nor do I suggest that efforts to regulate it are necessarily misguided or futile — only that such efforts pose fraught choices. IHL does not *per se* prohibit mass surveillance in occupied territory. The enquiry is rather defining where mass surveillance technologies and techniques stray beyond legitimate measures of control and security, which is a policy judgment. Human rights are a necessary but not sufficient component of this policymaking. The procedural approach to digital privacy and data protection emerging in human rights law is premised on a division of labour between legislator, data controllers and processors, and

131 BENVENISTI, *supra* note 96, at 107.

regulator. This approach is neither theoretically nor practically suited to the structure of military occupation — nor would such congruence be desirable. A swollen occupation bureaucracy devoted to the lawful operation of surveillance regimes would invariably blur the distinction between the "normal" state of self-determination/sovereign equality and the "exceptional" state of alien rule/suspended sovereignty that occupation represents.[132]

I close on this note of sobriety: the gap between the image and contemporary reality of occupation may be vast enough to defy pragmatic regulation, as the example of biometric checkpoints illustrates. Either we accept that the checkpoint expresses the military prerogative to regulate and restrict movement of enemy nationals for public safety and military security, i.e. that it results from the "exceptional" nature of occupation, in which case the appeal to their "normal" administrative and bureaucratic character as the source of data protection obligations must fail. Or we are prepared to contemplate that *ce n'est pas un point de contrôle* and to ask teleological questions regarding the checkpoints and the occupation regime itself.[133] A pragmatic approach to digital privacy and data protection in occupation, if neither grounded in black-letter law nor prepared to grapple with occupation as a normative phenomenon, would be doubly unsatisfactory.

132 Much as efforts to humanise means and methods of warfare are charged with sanctioning wars of indefinite duration; *see* SAMUEL MOYN, HUMANE: HOW THE US ABANDONED PEACE AND REINVENTED WAR (2021).

133 Handel, *supra* note 47, at 259–61; Hagar Kotef & Merav Amir, *Between Imaginary Lines: Violence and its Justification at Military Checkpoints in Occupied Palestine*, 28 THEORY, CULTURE & SOC'Y 55 (2011).

Chapter 6

The Right to Privacy and the Protection of Data for Prisoners of War in Armed Conflict

Emily Crawford [1]

INTRODUCTION

It is relatively uncontroversial nowadays to state that the law of armed conflict (LOAC) and international human rights law (IHRL) can and do apply concurrently and that persons in situations of armed conflict are entitled to have their international human rights respected.[2] In the context of prisoner of war (POW) detention, all POWs are entitled to have their fundamental human rights respected by the State[3] that claims control over them, while at the same time benefiting from the full suite of POW protections.

1 Associate Professor, University of Sydney.

2 On the relationship and interaction of the LOAC and IHRL, see further INTERNATIONAL HUMANITARIAN LAW AND INTERNATIONAL HUMAN RIGHTS LAW: PAS DE DEUX (Orna Ben-Naftali ed., 2011); RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW (Robert Kolb & Gloria Gaggioli eds., 2013).

3 This raises the specter of the extraterritorial applicability of human rights law, which is not uncontroversial. *See further* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011), in particular ch. 2. However, this chapter will follow the lead of Asaf Lubin:

One of the fundamental human rights to which POWs are entitled is the right to privacy — defined in international law as the right to not be "subjected to arbitrary interference with [one's] privacy, family, home or correspondence, nor to attacks upon [one's] honour and reputation."[4] Yet much of the detainee experience is anathema to the right to privacy. For example, POWs are under surveillance by the detaining power (DP) at all times and can have their personal correspondence and communications monitored and censored by the DP. Admittedly, the right to privacy under international law is framed as a right not to have one's privacy interfered with *arbitrarily or unlawfully*. Surveillance and monitoring pursuant to the rules on detention in an armed conflict are therefore not arbitrary but undertaken lawfully, because the POW meets certain criteria — namely, the POW is a captured enemy combatant.

The lawfully obtained personal data on POWs that can be gathered by a DP is noteworthy in volume and scope. Indeed, acquiring data on persons detained in the context of armed conflict is paramount. At the most basic level, it is fundamental for the detaining authority to know the country of origin of the POW, and other identifying information, for its own records. Under the law of international armed conflict,[5] parties

> Within the limits of this chapter, I do not wish to rehash the age-old debate around the extra-territorial application of human rights regimes. This chapter assumes that States must respect and ensure human rights to all individuals subject to their jurisdiction, power, or effective control, regardless of whether those individuals are situated within that States' territory.

Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives 471 (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., 2022). Whether persons held in detention by non-State actors are also to have their human rights respected and observed by such non-State actors is more problematic, but there are compelling arguments to suggest that non-State actors are under an obligation to respect the human rights of persons under their effective control. *See further* Non-State Actors and Human Rights (Philip Alston ed., 2005); Andrew Clapham, Human Rights Obligations of Non-State Actors (2006); Konstantinos Mastorodimos, Armed Non-State Actors in International Humanitarian and Human Rights Law: Foundation and Framework of Obligations, and Rules on Accountability (2016); Katherine Fortin, The Accountability of Armed Groups under Human Rights Law (2017).

4 As defined in G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948). See also similar provisions on privacy in the Convention on the Rights of the Child art. 16, Nov. 20, 1989, 1577 U.N.T.S. 3; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families art. 14, Dec. 18, 1990, 2220 U.N.T.S. 3; Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222; American Convention on Human Rights art. 11, Nov. 22, 1969, 1144 U.N.T.S. 123; Arab Charter on Human Rights arts. 16, 21, May 22, 2004, *reprinted in* 12 International Human Rights Reports 893 (2005).

5 Comprising Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention or GC III]; Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; and Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. Also adopted at the time was the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to

to the conflict must communicate information about a POW to the POW's country of origin and/or family[6] and to any other stakeholder, such as the protecting power,[7] the International Committee of the Red Cross,[8] or the Central Prisoners of War Agency.[9] This is only a fraction of the data that exists and can be collected regarding POWs — information regarding the personal effects they were carrying upon capture,[10] their physical and mental health,[11] and even what they are occupied with on a day-to-day basis[12] form a significant corpus of information that is or can be collected regarding POWs. Such data, of a highly personal nature, could be misused by a DP, or any other person into whose hands it fell, against the POW, their family and friends, and even their country of origin.

The LOAC contains no comprehensive rules on how such personal data is compiled and stored, or whether anything other than the most basic identifying information may be shared with other stakeholders — for instance, during prisoner transfer from one DP to another. In terms of rules regarding the privacy of POWs, including the protection of their personal information, all that exists in the LOAC are the generic rules that protect POWs from "insults and public curiosity"[13]—which could conceivably include protecting POWs from the exposure of personal information that might be of a private nature. Additionally, there are some limited rules on privacy-related matters, such as censoring personal correspondence[14] and when and how a POW may be placed under special surveillance — for instance, in the case of a POW who has previously escaped captivity.[15]

The primary sources of the LOAC—the Hague Regulations of 1907,[16] the Geneva Conventions of 1949,[17] and the Additional Protocols of 1977[18]—were adopted at a time when issues regarding privacy and data collection

the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem, Dec. 8, 2005, 2404 U.N.T.S. 261 adds an additional protected emblem—that of the Red Crystal—to the existing Red Cross, Red Crescent, and Red Lion and Sun emblems.

6 GC III, *supra* note 5, art. 70.
7 *Id.* art. 69.
8 *See, e.g., id.* arts. 9, 122.
9 *Id.* art. 123.
10 *Id.* art. 18.
11 *Id.* arts. 29–31.
12 For instance, if they are engaged in employment within or outside the detention facility, per *id.* arts. 51–57.
13 *Id.* art. 13.
14 *Id.* art. 76.
15 *Id.* art. 92.
16 Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539.
17 *Supra* note 5.
18 *Id.*

were not foremost in the minds of States and other stakeholders. However, in the last few decades, technology has developed to the point that the collection of data from individuals is far easier and far more comprehensive in scope than ever before. Alongside these technological developments have been the growth and expansion of IHRL and its own robust discourse on the individual right to privacy and the multitude of issues that arise from data collection and management. There has been no concomitant development in the LOAC to grapple with what rights to privacy POWs have and what rules should govern the collection, management, and communication of data on POWs and detainees.

This chapter will examine the question of POWs and their right to privacy, whether and how data collected on POWs must be managed, what implications arise regarding the data collected on POWs, and whether there are issues regarding privacy and the protection of personal data of POWs. In doing so, the chapter will draw on the rules of both the LOAC and IHRL to ascertain whether there is a gap in the law or whether the existing rules are sufficient. Due to space limitations, the chapter will focus solely on the issues of data protection and privacy of POWs (as opposed to detainees in international armed conflicts and persons detained in relation to non-international armed conflicts).[19]

I
THE RIGHT TO PRIVACY IN INTERNATIONAL LAW

Before assessing whether the LOAC adequately deals with the concept of the right to privacy and the protection of personal data, it is useful to first understand what is meant by a right to privacy and how the protection of personal data is fundamental to upholding that right. However, this is easier said than done: the literature on what exactly "privacy" means is vast, and there are competing and conflicting views on what privacy actually entails.[20] It has variously been theorized as:

19 For detailed analyses of the rights that accrue for security detainees in international armed conflicts and detainees in non-international armed conflicts, see further Lawrence Hill-Cawthorne, Detention in Non-International Armed Conflict (2016); Ryan Goodman, *The Detention of Civilians in Armed Conflict*, 103 American Journal of International Law 48 (2009); Jelena Pejic, *Procedural Principles and Safeguards for Internment/Administrative Detention in Armed Conflict and Other Situations of Violence*, 85 International Review of the Red Cross 375 (2005).

20 *See generally* Andrea Monti & Raymond Wacks, Protecting Personal Information: The

> a choice, a function, a desire, a right, a condition, and/or a need. Privacy has also been defined as the desire of individuals for solitude, intimacy, anonymity, and reserve. It has been defined widely as "the right to be left alone" and narrowly as a right to control information about one's self.[21]

It is not possible in a chapter of this scope to undertake an analysis of these differing philosophical theories of privacy. Instead, for the purpose of *this* chapter, it will be the international legal concept of privacy, as enshrined in treaty law, that will be used as the measure. That is to say: what does IHRL understand privacy to be?

A THE RIGHT TO PRIVACY IN INTERNATIONAL HUMAN RIGHTS LAW

Article 17 of the International Covenant on Civil and Political Rights provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[22] This provision is essentially replicated in other IHRL instruments, such as the Universal Declaration of Human Rights,[23] and other international and regional human rights instruments,[24] as well as significant non-binding statements from various UN bodies.[25] Neither the case law nor the General Comment[26] pertaining to Article 17 has thoroughly defined the right to privacy.[27] However, it is clear that the right to privacy under international law encompasses certain fundamental elements that relate to the "sphere of a person's life in which he or she can freely express his or her identity"[28] and that

Right to Privacy Reconsidered 9–10 (2019); Jon Mills, Privacy: The Lost Right 4–5 (2008); Alexandra Rengel, Privacy in the 21st Century 27–39 (2013); Ken Gormley, *One Hundred Years of Privacy*, 1992 Wisconsin Law Review 1335 (1992).

21 Sarah Joseph & Melissa Castan, The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary 533 (3d ed. 2013).

22 International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

23 Universal Declaration of Human Rights, *supra* note 4, art. 12.

24 *See, e.g.*, Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 4, art. 8; American Convention on Human Rights, *supra* note 4, art. 11; Convention on the Rights of the Child, *supra* note 4, art. 16; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, *supra* note 4, art. 14; Arab Charter on Human Rights, *supra* note 4, arts. 16, 21; International Convention on the Rights of Persons with Disabilities art. 22, Jan. 24, 2007, 2515 U.N.T.S. 3.

25 For a complete accounting of these documents, see further Lubin, *supra* note 3, at 468–69.

26 U.N. Human Rights Committee, *CCPR 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*, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988) [hereinafter *General Comment No. 16*].

27 Joseph & Castan, *supra* note 21, at 534.

28 Coeriel et al. v. The Netherlands, Communication No. 453/1991, ¶ 10.2, U.N. Doc.

the "notion of privacy revolves around protection of those aspects of a person's life, or relationships with others, which one chooses to keep from the public eye, or from outside intrusion."[29]

Specific aspects of the right to privacy have been identified by the Human Rights Committee and in the case law as comprising rights to family and home,[30] including the right not to have one's person or residence unlawfully or arbitrarily searched.[31] The right to privacy also entails that "[c]orrespondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited";[32] this right exists even for persons in detention—subject to appropriate, non-excessive censorship regimes.[33] In addition, professional duties of confidentiality—such as those of medical and legal professionals—must be respected,[34] and persons should not be made to undergo unlawful or arbitrary medical treatments.[35] The right to privacy includes the right to have one's honor and reputation respected and protected;[36] regulation based on one's private sexual behavior[37] or one's gender[38] may amount to an infringement of one's right to privacy.

CCPR/C/52/D/453/1991 (Dec. 9, 1994); *see also* Raihman v. Latvia, Communication No. 1621/2007, ¶ 8.2, U.N. Doc. CCPR/C/100/D/1621/2007 (Oct. 28, 2010).

29 Hopu and Bessert v. France, Communication No. 549/1993, ¶ 6, U.N. Doc. CCPR/C/60/D/549/1993/Rev.1. (July 29, 1997).

30 *General Comment No. 16*, *supra* note 26, ¶ 5; Vojnoviv v. Croatia, Communication No. 1510/2006, U.N. Doc. CCPR/C/95/D/1510/2006 (Mar. 30, 2009); Peiris v. Sri Lanka, Communication No. 1862/2009, U.N. Doc. CCPR/C/103/D/1862/2009 (Apr. 18, 2012); Ngambi v. France, Communication No. 1179/2003, U.N. Doc. CCPR/C/81/D/1179/2003 (July 9, 2004); Tornel et al. v. Spain, Communication No. 1473/2006, U.N. Doc. CCPR/C/95/D/1473/2006 (Mar. 20, 2009); Aumeeruddy-Cziffra et al. v. Mauritius, Communication No. 35/1978, U.N. Doc. CCPR/C/OP/1 at 67 (1984).

31 Rojas García v. Colombia, Communication No. 687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (Oct. 26, 2001); Yklymova v. Turkmenistan, Communication No. 1460/2006, U.N. Doc. CCPR/C/96/D/1460/2006 (July 20, 2009).

32 *General Comment No. 16*, *supra* note 26, ¶ 8.

33 Pinkney v. Canada, Communication No. 27/1978, U.N. Doc. CCPR/C/OP/1 at 95 (1985); Angel Estrella v. Uruguay, Communication No. 74/1980, U.N. Doc. CCPR/C/OP/2 at 93 (1990).

34 Cornelis van Hulst v. Netherlands, Communication No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999 (Nov. 1, 2004).

35 M.G. v. Germany, Communication No. 1482/2006, U.N. Doc. CCPR/C/93/D/1482/2006 (July 23, 2008); Brough v. Australia, Communication No. 1184/2003, U.N. Doc. CCPR/C/86/D/1184/2003 (Mar. 17, 2006).

36 *General Comment No. 16*, *supra* note 26, ¶ 11; Tshisekedi v. Zaire, Communication Nos. 241/1987 and 242/1987, U.N. Doc. CCPR/C/37/D/242/1987 (Nov. 29, 1989); Komarovski v. Turkmenistan, Communication No. 1450/2006, U.N. Doc. CCPR/C/93/D/1450/2006 (July 24, 2008); I.P. v. Finland, Communication No. 450/1991, U.N. Doc. CCPR/C/48/D/450/1991 (July 26, 1993); R.L.M. v. Trinidad and Tobago, Communication No 380/1989, U.N. Doc. CCPR/C/48/D/380/1989 (July 16, 1993); Sayadi and Vinck v. Belgium, Communication No. 1472/2006, U.N. Doc. CCPR/C/94/D/1472/2006 (Oct. 22, 2008).

37 Toonen v. Australia, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994).

38 Llantoy-Huamán v. Peru, Communication No. 1153/2003, U.N. Doc. CCPR/C/85/D/1153/2003 (Oct. 24, 2005); L.M.R. v. Argentina, Communication No. 1608/2007, U.N. Doc. CCPR/C/101/D/1608/2007 (Apr. 28, 2011); L.N.P. v. Argentina, Communication No. 1610/2007, U.N. Doc. CCPR/C/102/D/1610/2007 (Aug. 16, 2011). *See also* U.N. Human Rights Committee, *CCPR General Comment No. 28: Article 3 (The Equality of Rights Between Men and Women)*, ¶ 20, U.N. Doc. CCPR/C/21/Rev.1/Add.10 (Mar. 29, 2000).

B THE RIGHT TO PRIVACY IN THE INTERNATIONAL LAW OF ARMED CONFLICT

Under the LOAC, there are few rules that specifically protect a POW's privacy. Indeed, POWs are subject to numerous measures that would normally be considered an *infringement* on their privacy. Under the law of international armed conflict, once captured, POWs have their personal effects searched and can have some of their belongings temporarily confiscated.[39] They are held in camps where their daily activities may be monitored and tracked by the DP, including if they are put to work,[40] if they have received sums of money,[41] or if they have sent or received correspondence.[42] What is contained in such correspondence can be censored.[43] In addition to the "regular" surveillance to which a POW camp is subject, individual POWs may be subjected to heightened surveillance regimes if they have unsuccessfully attempted escape from detention.[44]

There are expansive rules that provide protections for POWs in relation to nearly all aspects of their physical and mental well-being. However, these rules — contained primarily in the Third Geneva Convention — contain little in the way of *specific* rules on privacy and safeguards regarding data collected about POWs. Instead, the Conventions provide generalized protections within which protections for one's privacy, particularly with regards to personal data, can be extrapolated. Foremost among these is Article 13 of the Third Geneva Convention, which provides that "[p]risoners of war must at all times be humanely treated"[45] and that POWs "must at all times be protected, particularly against acts of violence or intimidation and against insults and public curiosity."[46] While the right to privacy is not specifically mentioned in any of these articles, the newly updated Commentary to the Third Geneva Convention makes it clear that humane treatment, in the form of protection from public curiosity, is especially important from a privacy perspective, particularly because of advances in technology:

39 GC III, *supra* note 5, art. 18.
40 *Id.* art. 56, requiring the camp commander to keep records of when a POW is seconded to a work detachment.
41 *Id.* art. 64, requiring that accounts be kept for POWs that keep track of payments received, either as working pay or as remittances from the exterior.
42 *Id.* arts. 71–72, which outline how many pieces of correspondence a POW may send or receive.
43 *Id.* art. 76, which outlines how and why a DP may search and/or censor POW correspondence.
44 Pursuant to *id.* art. 92.
45 *Id.* art. 13(1).
46 *Id.* art. 13(2).

> Protection from public curiosity has gained particular relevance in the recent past owing to the rapid developments in communication technology and the growing involvement of mass media in the coverage of armed conflicts, together with the ubiquity of social media as a means of distributing both images and comment.[47]

Under the umbrella of humane treatment, the DP must therefore respect the privacy of POWs by not subjecting them to such public curiosity and must protect them from, for example, having identifying details or humiliating or degrading imagery or information promulgated publicly, for instance through social media.[48] Arguably, the absolute requirement to act humanely towards POWs would suggest that the release or distribution of private information about the POW to an unauthorized person or institution would amount to an infringement on the dignity of the POW and be contrary to the Conventions.

More specific provisions relating to privacy, such as the censorship of correspondence and special surveillance for failed escapees, are also structured to protect the detainee, with limitations placed on the DP's ability to censor and the kinds of special surveillance to which the detainee may be subject.[49] These obligations extend to any authority in control of the detainee or POW—under Article 12 of the Third Geneva Convention, if the DP decides to transfer a POW, it can only do so if it is transferring the POW to an authority that will likewise respect the provisions of the Convention.[50]

47 International Committee of the Red Cross, Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War ¶ 1563 (2020), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=3DEA78B5A19414AFC1258585004344BD [hereinafter 2020 GC III Commentary].

48 For example, the release of photographs of Saddam Hussein undergoing medical examination was condemned as a breach of the humane treatment requirement. *See further* Ian Roberts, *Saddam Hussein's Medical Examination Should Not Have Been Broadcast*, 328 BMJ 7430 (2004); David Stout, *U.S. Denounces Release of Candid Hussein Photos*, N. Y. Times, May 20, 2005, https://www.nytimes.com/2005/05/20/international/middleeast/us-denounces-release-of-candid-hussein-photos.html.

49 *See further* 2020 GC III Commentary, *supra* note 47, ¶¶ 3341–70, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=13C85487D2430A5DC1258585004DA270; *id.* ¶¶ 3830–37, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=1EEEAA738B611702C12585850054171B.

50 GC III, *supra* note 5, arts. 1, 12.

II
THE INTERNATIONAL LAW OF DATA PROTECTION

Moving now to the concept of data protection and its connection to the right to privacy, it is helpful to define what is meant by "data" and/or "personal data," of the kind which requires protection. For the purpose of this chapter, data is taken to mean information—whether in the form of text, images, audio clips, and/or visual footage. This information may or may not be stored digitally on computers, and may or may not exist separately in hard copy format—it is information that "can be read, viewed, heard, or otherwise sensually consumed by humans."[51] This kind of information is what Heather Harrison Dinniss terms "content-level data"[52]—data that "represents information which… is in principle intelligible to humans."[53] For Harrison Dinniss, content-level data can be distinguished from operational-level data, which is what would commonly be understood as computer code—software programs and operating systems that are necessary for computer systems to function.[54] In addition, it is also possible to have metadata—data about data (that is, information about a text, audio, or visual file created in digital form, such as the author, the date of creation, the size of the file, and, potentially, the geographical location of its creation). Finally, it is also possible to distinguish between personal and non-personal data—photos that reside in digital form on a person's computer or phone would be personal data, while the software program that allows someone to open the photo file would not be personal data.

A DATA PROTECTION UNDER INTERNATIONAL HUMAN RIGHTS LAW

The right to privacy necessarily includes the right to have personal information about oneself safely stored and protected from falling into the hands of others not authorized to access it. The connection between

51 Robin Geiss & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INT'L L. STUD 556, 560 (2021).
52 Heather Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISR. L. REV. 39, 41 (2015).
53 Geiss & Lahmann, *supra* note 51, at 560.
54 Harrison Dinniss, *supra* note 52, at 41.

privacy and data protection was highlighted by the Human Rights Committee in General Comment 16:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[55]

Privacy and data protection also necessitate data security — that the personal information stored within an analog or digital storage facility is kept confidential, secure, and accessible for those authorized to access the information. For analog material — for example, paper files on POWs containing information about their person — such material should be kept under lock and key, with access granted only to persons authorized to access it, and strict records kept of access, to ensure the integrity of the information contained within the files. In the digital context, data protection extends not just to the files themselves but to the computer systems that house the files — again, to ensure the confidentiality of the files, the integrity of the information contained therein, and that "stored information is accessible and processable whenever needed or desired."[56] For digital files, this would mean that the files and the systems containing them are protected from "adversarial cyber operations that delete targeted data"[57] or those that otherwise manipulate, corrupt, or unlawfully access data.

55 *General Comment No. 16*, *supra* note 26, ¶ 10.
56 Geiss & Lahmann, *supra* note 51, at 562.
57 *Id.*

Given the centrality of data protection to the right to privacy, it is noteworthy that there is little binding law regarding data protection under IHRL. The binding instruments have primarily come from the European sphere and include the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[58] the General Data Protection Regulation (GDPR),[59] and Article 8 of the Charter of Fundamental Rights of the European Union,[60] which provides that:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

In addition, there are some non-binding instruments that provide guidance on data protection, including the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data[61] and the UN Guidelines for the regulation of computerized personal data files.[62] These are joined by domestic laws from over 125 States.[63]

B DATA PROTECTION IN THE INTERNATIONAL LAW OF ARMED CONFLICT

If the IHRL on data protection is, at present, to borrow Lauterpacht's statement, "at the vanishing point,"[64] then laws on data protection in the LOAC are at the vanishing point of *that* vanishing point. There is general agreement among experts and practitioners that military operations that

58 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. 108.
59 Regulation (EU) No. 2016/679, 2016 O.J. (L 119) 1, 32–33 [hereinafter GDPR].
60 Charter of Fundamental Rights of the European Union 2012 O.J. (C 326).
61 C(80)58/FINAL, as amended on July 11, 2013 by C(2013)79.
62 Adopted by G.A. Res. 45/95, U.N. Doc. A/RES/45/94 (Dec. 14, 1990). *See also* International Law Commission, Report on the Work of its Fifty-Eighth Session, Annex IV: Protection of Personal Data in Transborder Flow of Information, U.N. Doc. A/61/10, *reprinted in* [2006] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 217, U.N. Doc. A/CN.4/SER.A/2006/Add.1.
63 *Data Protection and Privacy Legislation Worldwide*, UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Jan. 19, 2021).
64 Hersch Lauterpacht, *The Problem of the Revision of the Law of War*, 29 BRIT. Y'BOOK OF INT'L L. 360, 382 (1952).

destroy data physically (for example, a bombing raid that destroys a collection of paper files) would be governed by LOAC rules on targeting.[65] However, there is still debate over whether attacks, particularly digital attacks, that delete or corrupt digital data are governed by the LOAC—because, in theory, the data is not permanently lost and can presumably be recovered because it has been saved in another format or location. For some experts, if the data is not subject to destruction or damage that "is visible and tangible in the real world,"[66] then the data is not properly considered an "object" under the LOAC and is not subject to LOAC protections.[67] There is even less agreement as to whether simply accessing unlawfully the data of protected persons such as POWs (in the absence of causing damage to such files) would be governed by the LOAC,[68] because "cyber operations that target the confidentiality of data will, unless something unforeseen happens, harm neither the system itself not the stored data"[69] and would arguably not reach the level of "attack" as defined in the LOAC.[70]

For persons in POW detention, considerable amounts of data may be retrieved and retained. From the moment a POW is captured, the DP is permitted to collect data such as the name, rank, date of birth, and any army, regimental, personal, or serial number of a POW;[71] what physical items the POW is carrying at the time of capture;[72] where the POW will be housed;[73] what kinds of work they might do on a given day;[74] what kinds and amounts of food they eat;[75] what religion they observe;[76] how many letters and parcels they send and receive, including their provenance, destination, and contents;[77] and whether the detainee has any medical

65 Michael Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations*, 101 Int'l Rev. Red Cross 333, 340 (2019).
66 Geiss & Lahmann, *supra* note 51, at 565.
67 Schmitt, *supra* note 65, at 340; Michael Schmitt, *International Cyber Norms: Reflections on the Path Ahead*, 111 Netherlands Mil. L. Rev. 12 (2018). For a contrary position, see Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 Isr. L. Rev. 55, 73 (2015); Tim McCormack & Rain Liivoja, *Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello*, 15 Y'book Int'l Humanitarian L. 45 (2012).
68 Geiss & Lahmann, *supra* note 51, at 563.
69 *Id*.
70 Defined in Article 49 of AP I, *supra* note 5, as "acts of violence against the adversary, whether in offence or in defence," and generally considered to include, as a minimum, kinetic damage. See further the debate on the definition of "attack" in the Commentary to Rule 92 in Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael Schmitt ed., 2nd ed. 2017).
71 GC III, *supra* note 5, art. 17.
72 *Id.* art. 18; GC IV, *supra* note 5, art. 97.
73 GC III, art. 22; GC IV, *supra* note 5, art. 83.
74 GC III, *supra* note 5, arts. 50–57; GC IV, *supra* note 5, arts. 95–96; AP II, *supra* note 5, art. 5(1)(e).
75 GC III, *supra* note 5, art. 26; GC IV, *supra* note 5, art. 89; AP II, *supra* note 5, art. 5(1)(b).
76 GC III, *supra* note 5, art. 37; GC IV, *supra* note 5, art. 93; AP II, *supra* note 5, art. 5(1)(d).
77 GC III, *supra* note 5, arts. 71–76; GC IV, *supra* note 5, arts. 107–12; AP II, *supra* note 5, art. 5(2)(b).

conditions or ailments.[78] Beyond the already acknowledged LOAC rules on humane treatment, there are no specific laws that outline how or even whether a DP must protect such information from, for example, being accessed by external actors or even lawfully provided to third parties by the DP itself.

III
POWS, PRIVACY, AND DATA

As noted above, POWs are subject to significant interference with their privacy, and considerable amounts of data on them are accrued during their detention. However, it should *also* be noted that, as provided in Article 17 of the International Covenant on Civil and Political Rights and as noted in General Comment 16, only *unlawful* interference with one's privacy is prohibited: "'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[79]

The question then becomes: if data on POWs is lawfully obtained, and the privacy of the POW is lawfully circumscribed, what, then, is the problem? The problem lies in the fact that POWs are in a uniquely vulnerable position, reliant as they are on their captors to protect and care for them. There is a distinct possibility that the information gathered about their physical and mental condition, their place of origin, their family connections, their religious affiliations, and so on could be used against them, either by those who are detaining them or by third parties—not unforeseen, given that the POW is in the hands of the "enemy" during an armed conflict.

Indeed, this kind of abuse was evidenced in relation to persons detained by U.S. authorities in Afghanistan, following the 2001 invasion. On capture, detainees were stripped of clothing and frequently left naked in front of their captors.[80] U.S. personnel guarding the detainees engaged in "taking photographs and video taping [detainees] for their personal

78 GC III, *supra* note 5, arts. 29–31; GC IV, *supra* note 5, arts. 91–92; AP II, *supra* note 5, art. 5(1)(a).
79 *General Comment No. 16*, *supra* note 26, ¶ 3.
80 Laurel E. Fletcher & Eric Stover, Guantánamo and Its Aftermath: U.S. Detention and Interrogation Practices and Their Impact on Former Detainees 30 (2008).

use"[81] and threatened detainees with photos of their family to "make [them] think there was a possibility that [their] family"[82] was suffering adverse impacts as a result of the detainee's capture.

It is not difficult to imagine equivalent violations of POW privacy and data that could be justified on the basis of legitimate data collection—for example, a DP employing facial ID unlocking technology during POW processing and interrogation to access a POW's phone and social media accounts, as well as any media stored on a device or application. Other sensitive personal information, such as banking or medical information that is resident on a device or application, could also be a possible target. Indeed, accessing such information does not even need the consent of the POW.[83] This information could then be used against the POW as, for example, part of a coercive interrogation.

Given that there is little in the way of LOAC rules that act to protect POW data in such situations, IHRL could step in to address these gaps. Data protection regimes, particularly the GDPR, ensure that private data is subject to strict processing rules, including that:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[84]

The GDPR also contains protections that entitle persons to, *inter alia*, have their data erased,[85] as there are strict controls over the transfer of personal data to third parties.[86] These rules would seem to address a number of gaps that exist in the LOAC regarding data collection and protection.

However, the utility of the GDPR in situations of armed conflict is limited in two key ways. First, the GDPR is limited jurisdictionally: it only "applies to the processing of personal data in the context of the activities

81 *Id.* at 31.
82 *Id.* at 37.
83 *See, e.g.*, Davey Winder, *Apple's iPhone FaceID Hacked in Less Than 120 Seconds*, FORBES, Aug. 10, 2019, https://www.forbes.com/sites/daveywinder/2019/08/10/apples-iphone-faceid-hacked-in-less-than-120-seconds/?sh=5152168621bc. A basic Google search will bring up multiple sites that indicate how to hack personal accounts on numerous types of social media, including Facebook, Instagram, and WhatsApp.
84 GDPR, *supra* note 59, art. 9(1).
85 *Id.* art. 17.
86 *Id.* arts. 44–50.

of an establishment of a controller or a processor in the Union";[87] where the data "processing activities are related to" either "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union" or "the monitoring of their behaviour as far as their behaviour takes place within the Union";[88] or where data is processed "by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."[89] Therefore, if the POWs are not located within European Union jurisdiction, as outlined by Article 3 of the GDPR, the GDPR rules do not apply.

The second limitation is contained in Article 2 of the GDPR, which provides that it does not apply to:

> issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.[90]

The "national security" limitation would, as Geiss and Lahmann point out, "seem to preclude the application of this legislation from any State activities in relation to conduct during situations of armed conflict."[91]

One solution could be to apply a broad interpretative framework to existing definitions of terms such as "attack," to reconceive data as being an "object" susceptible to attack in the same way that physical property can be kinetically damaged.[92] In this way, POW data could conceivably benefit from the protections that the person of the POW, and the physical installations used to house POWs, enjoy under the LOAC. However, given the paucity of State practice and academic support for such an approach, this solution seems unlikely to happen. Another approach would be, as Geiss and Lahmann argue, "to take, as a starting point, the principles of existing data protection, data security, and other pertinent legal frameworks and attempt to apply them to contemporary armed

87 *Id.* art. 3(1).
88 *Id.* art. 3(2).
89 *Id.* art. 3(3).
90 *Id.* preamble ¶ 16.
91 Geiss & Lahmann, *supra* note 51, at 568.
92 *See generally* Mačák, *supra* note 67.

conflicts."[93] In doing so, the more developed IHRL rules on data could serve as important gap fillers for the LOAC regime.

Another solution could be to follow the trend in LOAC rule development over the last 30 years[94] and create a sui generis non-binding instrument that sets out the relevant data protection and privacy rules that should be applied in all situations of armed conflict (including POW detention). Such an instrument could follow the framework established by the UN Standard Minimum Rules for the Treatment of Prisoners,[95] now known as the Mandela Rules.[96] The Mandela Rules were first adopted as the Standard Minimum Rules by the UN in 1955[97] and were designed as guidelines on the basic minimum requirements necessary for housing persons in detention[98]—essentially, a set of "best practice" guidelines. The Rules contain numerous provisions regarding the health, welfare, and well-being of prisoners. In the years following their adoption, over 60 States used the Rules to inform their own domestic prison legislation. The Rules have now been adopted and used in most States.[99] From the perspective of detainee privacy and data protection, most relevant are Rule 1, which affirms that "[a]ll prisoners shall be treated with the respect due to their inherent dignity and value as human beings"; Rule 6, which states that prisoner files should be carefully managed and that "[p]rocedures shall be in place to ensure a secure audit trail and to prevent unauthorized access to or modification of any information contained in

93 Geiss & Lahmann, *supra* note 51, at 570.

94 *See generally* ANTON PETROV, EXPERT LAWS OF WAR: RESTATING AND MAKING LAW IN EXPERT PROCESSES (2020); EMILY CRAWFORD, NON-BINDING NORMS IN INTERNATIONAL HUMANITARIAN LAW: EFFICACY, LEGITIMACY, AND LEGALITY (2021).

95 Adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Geneva in 1955, and approved by the Economic and Social Council by its resolutions 663 C (XXIV) of July 31, 1957, and 2076 (LXII) of May 13, 1977.

96 G.A. Res. 70/175, U.N. Doc. A/Res/70/175 (Dec. 17, 2015).

97 Standard Minimum Rules for the Treatment of Prisoners, First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, U.N. Doc. A/CONF/6/1, Annex I, A (1956). The 1955 rules were themselves a development of earlier work undertaken by the International Penal and Penitentiary Commission in 1926. On the drafting background, see further William Clifford, *The Standard Minimum Rules for the Treatment of Prisoners*, 66 AM. J. INT'L L. 232 (1972); Daniel L. Skoler, *World Implementation of the United Nations Standard Minimum Rules for Treatment of Prisoners*, 10 J. INT'L L. & ECON. 453, 454–55 (1975).

98 Skoler, *supra* note 97, at 455.

99 *See* U.N. Secretary-General, *Crime Prevention and Criminal Justice: Progress Made in the Implementation of General Assembly Resolutions 50/145 and 50/146*, ¶ 51, U.N. Doc. A/51/327 (Oct. 1, 1996). *See also* the meetings of the UN-established Open-Ended Intergovernmental Expert Group on the Standard Minimum Rules for the Treatment of Prisoners, UNITED NATIONS OFFICE OF DRUGS AND CRIME, https://www.unodc.org/unodc/en/justice-and-prison-reform/ieg-standards.html (last visited Jan. 19, 2021); Open-Ended Intergovernmental Expert Group Meeting on the United Nations Standard Minimum Rules for the Treatment of Prisoners, Background Note, Vienna, 31 January – 2 February 2012, § 3.1, https://www.unodc.org/documents/justice-and-prison-reform/AGMs/Background_note.pdf; Council of Europe, Recommendation of the Committee of Ministers to Member States on the European Prison Rules, Rec(2006)2 (Jan. 11, 2006), https://wcd.coe.int/ViewDoc.jsp?id=955747; NIGEL RODLEY & MATT POLLARD, THE TREATMENT OF PRISONERS UNDER INTERNATIONAL LAW 393 (3rd ed. 2009).

the system"; and Rule 9, which states that all prisoner records "shall be kept confidential and made available only to those whose professional responsibilities require access to such records." Additional rules serve to protect the prisoner's right to privacy, including limits on physical searches of a prisoner's accommodation and person.[100] An instrument on data protection and in armed conflict could incorporate similar rules to those of the Mandela Rules to specifically protect persons in POW detention.

The adoption of a non-binding document on data protection and privacy in armed conflict would not be a radical step, or necessarily an exercise in *lex ferenda*, even with the paucity of LOAC rules on privacy and data protection for POWs. As Asaf Lubin notes, while "there is still considerable fragmentation concerning core principles that govern this space,"[101] general trends regarding data protection in international law can be discerned, including, and most pertinently for POWs (and indeed, other detainees in situations of armed conflict), that:

> [d]ata undergoing processing shall be kept in a form that permits identification of data subjects for no longer than is required for the purpose for which it is stored… that data should be protected by reasonable security safeguards from unauthorized or accidental access, destruction, use, or modification… [and that there should be] a mechanism for ensuring due process, supervision, and legal sanction, such as through a data protection authority, to ensure that data controllers and processors comply with these principles.[102]

Given the emerging customary and treaty law on questions of data protection, the issuance of a manual or other guidelines on the law on data protection in the LOAC could therefore arguably be a justifiable exercise in applying IHRL rules to LOAC situations.

100 Rules 50–52.
101 Lubin, *supra* note 3, at 475.
102 *Id.* at 14.

CONCLUDING COMMENTS

For POWs, concerns about their privacy and the protection of their personal data may not necessarily be at the forefront of their thoughts upon capture. However, given the vast array of material collected on POWs, the paucity of LOAC rules regarding what may be done with that material, and the potential for abuse of the data in question, it is incumbent on stakeholders, such as States, intergovernmental organizations, and civil society, to consider the question of privacy and data protection of POWs in more detail. IHRL has much to offer in this context and could provide useful instruction for future practice in armed conflicts, whether that manifests itself as customary law, treaty law, or some non-binding mechanism.

Digital Rights and Surveillance Technologies

Chapter 7

Face Value: Precaution versus Privacy in Armed Conflict

Leah West[1]

INTRODUCTION

Following the American withdrawal from Afghanistan in August 2021, Taliban forces moved through the country quickly, claiming control of not only villages but also the arms and military equipment left behind by US forces. The group seized a vast arsenal of weapons, vehicles, and even helicopters that could significantly enhance the Taliban's combat power.[2] Also left behind were devices known as Handheld Interagency

1 Assistant Professor of International Affairs, Norman Paterson School of International Affairs, Carleton University. I am grateful to Ken Watkin, Ido Rosenzweig, the contributors to this text, and participants of the Fourth Early Career Researchers Workshop on Terrorism and Belligerency for their helpful comments on earlier drafts. Funding for part of this research was provided by the Minerva Center for the Rule of Law under Extreme Conditions, University of Haifa Faculty of Law and the Geography and Environmental Studies Department.

2 Zachary Cohen & Oren Liebermann, *Rifles, Humvees and Millions of Rounds of Ammo: Taliban Celebrate Their New American Arsenal*, CNN, Aug. 21, 2021, https://www.cnn.com/2021/08/21/politics/us-weapons-arsenal-taliban-afghanistan/index.html.

Detection Equipment (HIDE), used to collect, store, and upload biometric information collected from individuals in the field. These devices were first used in 2002 to identify Taliban and Al-Qaeda prisoners in detention centres in Afghanistan.[3] By 2011, the *New York Times* was reporting that an Afghan citizen "would almost have to spend every minute in a home village and never seek government services to avoid ever crossing paths with a biometric system."[4]

The term "biometrics" refers to both a characteristic and a process. As a characteristic, it means "a biological or behavioral feature of an individual (such as the iris, fingerprint, or voice pattern) that can be measured and used for automated recognition."[5] As a process, the term refers to "the automated means of measuring and comparing these features, in order to establish the identity of an individual."[6]

Military forces leverage biometrics to establish "identity dominance" over the enemy.[7] Unlike official/identity documents that can be forged or shared, biometrics are much less susceptible to alteration and forgery. They offer a more distinctive and definitive means of identifying the enemy, "denying him the anonymity he needs to hide and strike at will."[8]

In Afghanistan, information collected by HIDEs included a person's facial photograph, iris scan, fingerprints, and biographical information. Coalition Forces used the data and devices to identify insurgents, verify the identity of locals and third-country nationals seeking to access bases and facilities, and link people to security events and criminal activity.[9] All data compiled by US forces was stored indefinitely in the Department of Defense's (DoD) Automated Biometric Identification System (ABIS) and used in combination with "watch lists" to facilitate the detention and targeting of persons of interest who posed a threat to coalition forces and Afghan security.[10] In February 2007, the International Security Assis-

3 Dep't of Def. Biometrics Management Off., Department of Defense Biometric Standards Development Recommended Approach (2004), https://www.hsdl.org/?view&did=449571.

4 Thom Shanker, *To Track Militants, U.S. Has System That Never Forgets a Face*, N. Y. Times, July 13, 2011, https://www.nytimes.com/2011/07/14/world/asia/14identity.html; Centre for Army Lessons Learned, *U.S. Army Commander's Guide to Biometrics in Afghanistan* (2014), https://public-intelligence.net/call-afghan-biometrics/ [hereinafter *U.S. Army Commander's Guide*].

5 William C. Buhrow, Biometrics in Support of Military Operations: Lessons from the Battlefield (2017), 8.

6 *Id*.

7 John D. Woodward, *Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism,* Rand (2005), https://www.rand.org/pubs/reprints/RP1194.html.

8 Buhrow, *supra* note 5, at 1.

9 Nina Toft Djanegara, *Biometrics and Counter-Terrorism: Case Study of Iraq and Afghanistan,* Privacy International (2021), https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf; *see also U.S. Army Commander's Guide*, *supra* note 4, at i.

10 *U.S. Army Commander's Guide*, *supra* note 4.

tance Force (ISAF) implemented the US biometric system as part of its force protection and broader security efforts in Afghanistan.[11] Finally, in 2011, coalition forces partnered with the Afghan government to conduct "biometric enrolment" of the population to support the development of the country's digital identity card, known as the e-Tazkira.[12]

Despite US forces' extensive collection efforts, assessments by the US Government Accountability Office (GAO) in 2008 and 2011 warned that there were gaps in the US military's policies and procedures around the collection and storage of personal information.[13] Defence officials responded that the reason the biometrics program did not even meet basic information technology standards was that it had been developed to meet an urgent operational need.[14] In essence, officials argued that when first introduced, the technology and data were necessary to counter the battlefield threat; protecting Afghan nationals' privacy and informational security was simply not a priority. It was not until 2013, after 11 years of collection, that DoD established the Defence Forensics and Biometrics Agency to oversee all of the military's biometrics programs. The agency lists "protecting privacy" as one of its five core objectives.[15]

Yet despite the establishment of this agency, in the immediate aftermath of the Taliban's takeover, many feared that the group would leverage the abandoned HIDE machines and the data compiled by them to root out and punish those who had worked with coalition forces or the Afghan government.[16] Little is known about what, if any, safeguards were in place to ensure that the data collected by coalition forces remaining on the devices or shared with the Afghan government could not be accessed or leveraged by the Taliban or other malicious actors to target civilians.[17] Once again, US forces appeared to ignore the privacy interests of Afghans for the sake of operational expediency.

11 Pierre Meunier, Qinghan Xiao & Tien Vo, *Biometrics for National Security: The Case for a Whole of Government Approach* (2013), https://cradpdf.drdc-rddc.gc.ca/PDFS/unc124/p537494_A1b.pdf, 2.5.

12 Library of Congress, *Afghanistan: Distribution of Controversial Electronic Identity Cards Launched*, LOC, June 19, 2018, https://www.loc.gov/item/global-legal-monitor/2018-07-19/afghanistan-distribution-of-controversial-electronic-identity-cards-launched/; *see also U.S. Army Commander's Guide*, *supra* note 4, at i.

13 U.S. Gov. Accountability Off., *DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies* (2011), https://www.gao.gov/products/gao-11-276; *see also* U.S. Government Accountability Office, *DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing* (2008), https://www.gao.gov/new.items/d0949.pdf.

14 *Id.* at 11.

15 Defense Forensics and Biometrics Agency, *Core Objectives*, DFBA (2020), https://www.dfba.mil/functions/policy.html.

16 Rina Chandran, *Afghans Scramble to Delete Digital History, Evade Biometrics*, Reuters, Aug. 17, 2021, https://www.reuters.com/article/afghanistan-tech-conflict/afghans-scramble-to-delete-digital-history-evade-biometrics-idUSL8N2PO1FH.

17 Colin Freeze, *Fearing Reprisals, Afghans Rush to Scrub Digital Presence after Taliban Takeover*, Globe and Mail, Aug. 21, 2021, https://www.theglobeandmail.com/canada/article-fearing-reprisals-afghans-rush-to-scrub-digital-presence-after-taliban/.

Since the initial deployment of HIDEs in 2002, biometrics programs have proven to be an effective offensive and defensive tool in armed conflicts. In 2017, the GAO conducted a follow-up study in which it noted that since 2008, the biometrics program led the US DoD "to capture or kill 1700 individuals and deny 92,000 individuals access to military bases."[18] As an operations officer deployed in Kandahar in 2010–2011, my job relied on intelligence collected through a variety of means, including the persistent use of drones, surveillance balloons, audio sensors, communications intercepts, and information collected directly from Afghans, through either human connection or the collection of biometrics. We deployed HIDEs machines widely to collect data not only about those who wanted access to military facilities but also about those who visited district centres, made claims for damages from forces, or otherwise engaged with coalition forces. I was personally involved in an operation to detain a prolific maker of IEDs (improvised explosive devices) after fingerprints found on an IED were matched to a biometric record on file; that same individual was a human source for another agency and was previously given access to a military installation.

Biometric collection was critical to the coalition strategy to gain identity dominance over the enemy. In Afghanistan's long-running counter-insurgency, battles were fought in built-up areas. Combatants could go months without picking up a weapon and interacted openly with coalition forces. Under such circumstances, identifying friend from foe was incredibly challenging but necessary to the mission. Yet I never once thought of the privacy rights of the local population; nor did any operational policy demand that I consider their privacy interests. My experiences occurred in an era before facial recognition, before everyone carried a smartphone and social media platforms like Facebook and WhatsApp were prolifically relied upon in the region. Today, these tools generate troves of information that can be leveraged in connection with biometrics to not only gain a tactical advantage over the enemy but also protect civilians in the communities within which they are operating.

This chapter explores the tension between the operation and legal requirement to gather intelligence in an armed conflict and the privacy rights of the local population that may be affected by modern surveillance and analytical tools. It does so by using a case study, namely the deployment of facial recognition technology (FRT) in an armed conflict.

18 U.S. Gov. Accountability Off., *DOD Biometrics and Forensics: Progress Made in Establishing Long-Term Deployable Capabilities, but Further Actions Are Needed* (2017), https://www.gao.gov/assets/gao-17-580.pdf.

This case study highlights the existence of this tension. It reveals a set of legal obligations that arise during an armed conflict that both necessitate and limit the use of modern surveillance technology. It also identifies core policy and procedural questions that military leaders need to consider before deploying FRT to meet those obligations.

FRT is an appropriate case study because combining biometric data, like that amassed on the battlefield by US forces in Afghanistan and subsequently in Iraq and Syria,[19] with this technology is the next development in the race for identity dominance. Facial recognition is a biometric tool used primarily to automatically identify, verify, or authenticate a person's identity. In short, it analyzes key facial features and compares those features to other representations of an individual's face. In the future, FRT may also identify *potential* threats and individuals *contemplating* criminal or dangerous behaviour. Various studies suggest that artificial intelligence can recognize individuals registering suspicious behaviour from facial expressions, characteristics, involuntary gestures,[20] and estimated heart rate.[21] Thus, rather than relying on a fingerprint or iris scan to identify known combatants, FRT could give soldiers the ability to identify, in real-time, known and previously unknown enemy combatants at a distance, be it through the use of facial recognition glasses or the deployment of surveillance cameras mounted on structures, vehicles, or aircraft.

Chinese security officials are already using this technology at border crossings, transitways, and large security events.[22] Facial recognition glasses worn by security agents record video that is instantly cross-referenced against a database of images to identify known criminals. Once identified, the individual's name can be searched against additional databases to quickly provide agents with a plethora of information about the target. Similarly, Israel has incorporated FRT into its checkpoint and surveillance systems within the Occupied Palestinian Territories.[23]

19 Djanegara, *supra* note 9.

20 For an overview, see Isha Pandya & Deepti Theng, *Tracking Suspicious Behaviour Using Facial Expression Recognition Techniques: A Survey* 5:6 IJCSN 948 (2016).

21 Mossaad Ben Ayed et al., *Suspicious Behavior Recognition Based on Face Features*, IEEEAccess (2019), https://www.researchgate.net/publication/336541463_Suspicious_Behavior_Recognition_Based_on_Face_Features; Dana Liebelson, *Why Facebook, Google, and the NSA Want Computers That Learn Like Humans*, MOTHER JONES, Sept.–Oct. 2014, https://www.motherjones.com/media/2014/09/deep-learning-artificial-intelligence-facebook-nsa/.

22 Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*, WALL STREET JOURNAL, Feb. 7, 2018, https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353; Paul Mozer, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N. Y. TIMES, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

23 Keren Weitzberg, *Biometrics and Counter-Terrorism: Case Study of Israel/Palestine,* PRIVACY INTERNATIONAL (2021), https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf.

The use of FRT to identify combatants in an armed conflict is promising not simply because of the obvious efficiency and security benefits it offers but also from the perspective of international humanitarian law (IHL). A cardinal principle of IHL is that of distinction and the related precautionary principle. This principle provides that parties to an armed conflict must, at all times, distinguish between combatants and non-combatants. Customary law requires that in both international armed conflicts (IACs) and non-international armed conflicts (NIACs), military leaders do everything feasible to verify that attack objectives are not civilian and take all feasible precautions to minimize incidental civilian casualties when selecting the means and methods of attack.

Complying with these obligations was arguably easier when wars were waged between two uniformed State militaries on the battlefield. Increasingly, however, armed conflicts, be they international or non-international, are waged amid the population. Often, combatants are not members of State militaries; nor do they wear uniforms or openly carry arms. As such, the use of FRT to scan a crowd of faces and run those images against a database of known combatants and non-combatants could significantly enhance operational effectiveness and ensure compliance with IHL. Not only would it allow for the more efficient use of violence, but FRT deployment could also augment a soldier's decision-making and save the lives of innocent civilians. That said, the use of FRT in peacetime by law enforcement and border agents has come under increasing scrutiny. Human rights advocates are concerned with the tools' implications for privacy, free expression, and freedom of assembly.[24] Additionally, the recognition algorithms that power FRT have, to date, proven to be biased, resulting in false positives and false negatives disproportionately impacting racial minorities.[25]

This chapter does not revisit each of these concerns, although these risks would persist with FRT deployment by armed forces. Instead, I raise the potential use of FRT to explore the tension that arises between the quest for identity dominance and knowledge of the battlespace promoted by IHL and the privacy rights of civilians living through an armed conflict. Ultimately, this chapter argues that we must consider the privacy implications of facial recognition technology before its widespread use in armed conflict so that military commanders can incorporate the

24 *See, e.g.*, *Facial Recognition*, Canadian Civil Liberties Association (2020), https://ccla.org/facial-recognition/; Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC, July 5, 2020, https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/.

25 Rep. of the U.N. High Commissioner for Human Rights, para 32, U.N. Doc. A/HRC/44/24 (2020); Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U.L. REV. 1109, 1121 (2017).

necessary privacy-protective measures and processes into their operational protocols.

This chapter proceeds in three parts. It begins in Part I with a general overview of the IHL principles of distinction and precaution, and the right to privacy under IHL and international human rights law (IHRL). Part II explains how to identify conflicts between the norms and rules of IHL and IHRL and applies the complementary approach proposed by Oona Hathaway. This part concludes that the right to privacy and the principle of precaution are not in conflict; except in the rare instances of formal derogation, they apply concurrently in an armed conflict. Finally, Part III argues that the degree of control a party has over territory or a population, and the level and nature of the threat of violence, significantly impact what each obligation requires. Arguably, as State actors gain control over a territory and population and the level of violence declines, the need and challenge of routinely making snap decisions about an individual or group's combatant status decreases. As such, the need to rely on the widespread use of highly intrusive technology to comply with the precautionary principle diminishes. Conversely, as an armed conflict shifts from the uneasy end of the control/violence spectrum to the other, what is required to comply with the human right to privacy increases. This part concludes by warning military commanders that they must prepare for this shift when deploying surveillance technology like FRT. It proposes a function-based approach to designing policies and procedures capable of adapting to these evolving privacy obligations.

I LEGAL OVERVIEW

A DISTINCTION AND PRECAUTION UNDER IHL

IHL, or the law of armed conflict, regulates the conduct of hostilities. This body of law applies only after an armed conflict arises and applies for the duration of the conflict. Once an armed conflict develops, be it a NIAC or IAC, then IHL applies to all States and non-State parties to the conflict. IHL comprises both customary rules and treaties, most significantly the Hague Regulations of 1907, and the four Geneva Conventions and their Additional Protocols. The former sets out the rules for conducting war,

while the latter focuses on protecting the victims of war. Only a limited number of these treaty rules apply to NIACs, but the general principles codified in these treaties apply in all conflicts.

The core principle of IHL is distinction, which requires that military operations be directed at "military objectives."[26] Military objectives include "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[27]

This customary principle is codified in Articles 48, 51(2), and 52(2) of AP I, to which no reservations have been made.[28] Article 48 stipulates:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

Put simply, the principle of distinction partitions people into two categories: combatants and non-combatants. Combatants are members of the armed forces who are party to an armed conflict, excluding medical and religious personnel. Non-combatants are civilians (unless and for as long as they directly participate in hostilities), persons *hors de combat*, and medical and religious military personnel. Combatants may target and kill other combatants without that conduct constituting a war crime. Conversely, civilians may not be targeted, although they do not enjoy absolute protection against being killed.[29]

IHL also requires belligerents to distinguish themselves from the civilian population.[30] Nevertheless, it is not uncommon in modern warfare for members of organized armed groups, especially in NIACs, to not wear uniforms or to not identify themselves as combatants. Armed

26 Protocols Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, art. 48 [hereinafter *AP 1*].

27 *Id.* art. 52(2).

28 Protocols Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, art. 48.

29 International Committee of the Red Cross, *Customary IHL, Rule 1. The Principle of Distinction between Civilians and Combatants*, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1#:~:text=international%20armed%20conflicts-,Rule%201.,not%20be%20directed%20against%20civilians.

30 *AP 1*, *supra* note 26, art. 44; common art. 3.

groups who do not comply with IHL may also purposely seek to gain tactical advantage by blending in with the civilian population. Additionally, members of armed groups may only support or participate in hostilities intermittently, giving rise to the complicated dilemma of the "baker by day, soldier by night."[31] Civilians are only protected against attack "unless and for such time as they take a direct part in hostilities."[32] The level of participation that invalidates a civilian's protected status, and for how long civilians lose their protected status after they put down their rolling pin and pick up a weapon, is the subject of detailed guidance by the International Committee of the Red Cross (ICRC) but remains contested by the international community.[33]

IHL also prohibits indiscriminate attacks. This means that attacks not specifically directed at a precise military objective are unlawful. The same is true for attacks that employ a method or means of combat that cannot be targeted or whose effects cannot be limited to a military objective or combatants.[34] In other words, any attack must be narrowly tailored to the military objective. Given all of the above, one quickly realizes how the use of FRT could significantly enhance a military commander's capacity to identify the enemy and comply with their humanitarian obligations.

Despite these requirements, IHL accepts that civilians and civilian objects may be collateral damage. Civilians may, however, only be injured or killed where the impact is proportionate to the concrete and direct military advantage gained.[35] This rule of proportionality "establishes a link between the concepts of military necessity and humanity."[36]

Tied to the concepts of both proportionality and distinction is the precautionary principle. This customary rule is codified in Article 57 of AP I, which sets out a number of targeting rules. Most notably for the purpose of this chapter, the law requires: "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects," and with respect to attacks, "those who plan or decide upon an attack shall *do everything feasible* to

31 For more, see Craig Forcese & Leah West, *Killing Citizens: Core Legal Dilemmas in the Targeted Killing of Canadian Terrorist Fighters Abroad*, 54 CAN Y.B. INT'L. L. 134, 168 (2017).

32 International Committee of the Red Cross, *Customary IHL, Rule 6. Civilians' Loss of Protection from Attack*, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule6.

33 International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2009) at 33ff, https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf.

34 *AP 1, supra* note 26, art. 51(4).

35 International Committee of the Red Cross, *Customary IHL, Rule 14. Proportionality in Attack*, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14.

36 Canada, Office of the Judge Advocate General, *Law of Armed Conflict Manual: At the Operational and Tactical Levels*, B-GJ-005-104/FP-02 (Ottawa: Department of National Defence, 2001), at 2-2.

verify that the objectives to be attacked are neither civilians nor civilian objects."[37]

According to the ICRC Commentary on Article 57, before the provision was adopted, the phrase "everything feasible" was discussed at length.[38] Some delegations, including the British one, understood the words to mean "everything that was practicable or practically possible, taking into account all the circumstances at the time of the attack, including those relevant to the success of military operations."[39] The commentary suggests this last requirement is too broad, as it could give the success of the mission precedence over humanitarian obligations. Instead, the requirement is that necessary identifications be carried out in a timely manner to spare the civilian population to the furthest extent possible.[40] As J.-F. Quéguiner explains, "When taking precautions in attack, armed forces cannot be required to do the objectively impossible, nor can they be content with merely doing what is possible."[41]

Complying with the precautionary principle is, therefore, largely reliant on the collection, analysis, and sharing of information about potential targets, which is dependent on the capabilities and technical resources of a party to the conflict.[42] This does not mean that all parties to a conflict must acquire, possess, and deploy the most sophisticated means of technology.[43] The Commentary notes, "Some belligerents might have information owing to a modern reconnaissance device, while other belligerents might not have this type of equipment."[44] Those States possessing advanced technology are required to use it if it offers the most effective and reasonable means of obtaining reliable information.[45] "In other words," explains Michael Schmitt, "belligerents bear different legal burdens of care determined by the precision assets they possess."[46]

However, simply because a State has a specific intelligence capacity, like FRT, does not necessarily mean that a military commander must leverage that asset in all cases. Interpreting the "everything feasible"

37 *AP 1*, *supra* note 26, art. 57 [emphasis added].
38 *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, at 680–82 (Yves Sandoz, Christophe Swinarski & Bruno Zimmerman eds, International Committee of the Red Cross, 1987).
39 *Id.* at 680.
40 *Id*.
41 Jean-François Quéguiner, *Precautions under the Law Governing the Conduct of Hostilities*, 88:864 IRRC 793, 809–10 (2006).
42 *Id.* at 797.
43 Michael N. Schmitt, *Precision Attack and International Humanitarian Law*, 87:859 IRRC 445, 460 (2005).
44 *Commentary*, *supra* note 38, at 682.
45 Quéguiner, *supra* note 41, at 798.
46 Schmitt, *supra* note 43, at 460.

standard requires "common sense and good faith."[47] One must consider the time needed to leverage that asset and process additional information, the extent to which it would clarify existing uncertainty, competing demands for the asset, and any potential risks associated with its deployment.[48] Those risks could include privacy implications for the civilian population and the failure to comply with a State's obligations under IHRL.

Thus, the phrase "everything feasible" is highly contextual. As Frederik Rosen writes, "due precaution may build on years of intelligence or on a sound, split-second judgment."[49] However, he adds, generally speaking, "Once a belligerent purchases equipment and supplies it to its forces in the field, it must be used if it is available, makes good military sense and will minimize civilian impact."[50]

B PRIVACY UNDER IHRL AND IHL

IHRL governs the conduct of States in their relations with individuals and groups subject to their jurisdiction. Made up of both treaty and customary obligations, human rights law applies at all times.

Numerous international and regional human rights treaties protect the right to privacy. First, Article 12 of the *Universal Declaration of Human Rights* stipulates that "No one shall be subjected to *arbitrary* interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[51]

Similarly, Article 17 of the International Covenant on Civil and Political Rights stipulates:

1. No one shall be subjected *to arbitrary or unlawful* interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.[52]

47 *Commentary*, *supra* note 38, at 680.
48 Schmitt, *supra* note 43, at 461.
49 Frederik Rosen, *Extremely Stealthy and Incredibly Close: Drones, Control and Legal Responsibility*, 19:1 J. CONF. & SEC. L. 113, 127 (2014).
50 *Id.* at 462.
51 Universal Declaration of Human Rights, art. 12, Dec. 10, 1948, U.N.G.A. Res. 217 A(III) (1948) [emphasis added].
52 International Covenant on Civil and Political Rights, art. 17, *adopted* Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter *ICCPR*] [emphasis added].

Article 8 of the European Convention on Human Rights also provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right *except such as is in accordance with the law and is necessary in a democratic society* in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[53]

Likewise, Article 11 of the American Convention on Human Rights specifies that "Everyone has the right to have his honor respected and his dignity recognized" and that "No one may be the object of *arbitrary or abusive* interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation."[54] Similarly worded privacy rights are also embedded in a number more narrow human rights instruments,[55] leading some scholars to argue that the right to privacy is part of customary international law.[56]

Persistent surveillance and the collection, retention, processing, and sharing of a person's biometric data by a State party to any of these treaties trigger these provisions' application. A 2020 Report of the UN High Commissioner for Human Rights noted that routine audiovisual surveillance used in combination with FRT "brings about significant risks for the enjoyment of human rights,"[57] including not only the right to privacy

53 European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, *adopted* Nov. 4, 1950, ETS 5 (entered into force Sep. 3, 1953) [emphasis added].

54 American Convention on Human Rights, art. 11, *adopted* Nov. 22, 1969, 1144 U.N.T.S. 123 (entered into force July 18, 1978) [hereinafter *ACHR*] [emphasis added].

55 Organization for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL (Sept. 23, 1980); Convention on the Rights of the Child, art. 16, *adopted* Nov. 20, 1989, 1577 U.N.T.S. 3 (entered into force Sept. 2, 1990); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, art. 14, *adopted* Dec. 18, 1990, 2220 U.N.T.S. 3 (adopted Dec. 18, 1990, entered into force July 1, 2003), arts. 16, 21; Arab Charter on Human Rights, 12 I.H.R.R. 893 (entered into force Mar. 15, 2008); and International Convention on the Rights of Persons with Disabilities, art. 22, *adopted* Jan. 24, 2007, 2515 U.N.T.S. 3 (entered into force May 3, 2008).

56 Alexandra Rengel, Privacy in the 21st Century (Martinus Nijhoff, 2013), at 108; Arvind Pillai & Raghav Kohli, *A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and Other State Practice* (2017), Oxford U Comparative L Forum 3.

57 Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. U.N. Human Rights Council, Report of the United Nations High Commissioner for Human Rights, 44th Sess., June 24, 2020, U.N. Doc. A/HRC/44/24, paras. 30–31.

but also that of freedom of assembly and expression. Citing the European Court of Human Rights, the report went on to note: "A person's image constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Recording, analysing and retaining someone's facial images without her or his consent constitute interference with a person's right to privacy."[58] Deploying FRT in, for example, built-up areas and urban centres means that "these interferences occur on a mass and indiscriminate scale, as this requires the collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system."[59]

Crucially, under each human rights instrument, the protection of privacy is not absolute. Intrusions into an individual's private life may be permitted so long as they comply with certain criteria. After canvassing the jurisprudence of treaty-interpreting bodies and UN human rights bodies and rapporteurs, Asaf Lubin identified five general principles that, if met, permit States to engage in activities that interfere with one's enjoyment of their right to privacy.[60] The first principle Lubin identifies is *legality*, meaning that interferences must be regulated by laws that are public, accessible, clear, precise, and non-discriminatory.[61] Second, intrusions must be *necessary* for the achievement of a legitimate aim in a democratic society.[62] Third, any invasion of privacy must be *proportionate* to the achievement of that aim. Fourth, there must be *adequate safeguards* and processes in place to ensure "information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it."[63] Finally, where a State violates any of these principles, affected persons must have access to effective *remedies.*[64]

What is necessary to comply with each of these principles is highly context-specific. Thus, what may be proportionate and necessary when, for example, there is a direct and immediate threat to life may not be when the State's objective is less pressing or tangentially related to the

58 *Id.* at 33, citing *Reklos and Davourlis v. Greece*, para. 40, 1234/05 Eur. Ct. H.R. 2009.
59 *Id*.
60 Asaf Lubin, *The Right to Privacy and Data Protection under International Humanitarian Law and Human Rights Law, in* Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives 468–71 (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., Edward Elgar, 2022).
61 *Id.* at 8.
62 *Id.*
63 *Id.* at 8–9; U.N. Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), para 10, U.N. Doc. HRI/GEN/1/Rev.1 (Apr. 8, 1988).
64 *Id.* at 9.

intrusion. Nevertheless, where a State complies with these principles, searches, surveillance, and data collection and analysis, whether general or targeted, may be permissible under human rights law.

What is more, the human rights instruments referenced above permit States to derogate from certain obligations (including those concerning privacy) during an emergency that "threatens the life of the nation,"[65] including armed conflicts. While the wording varies slightly, to formally derogate, each instrument requires that States notify other parties to the treaty and identify which provisions it is derogating from and why. This notification requirement significantly raises the political costs of derogation.[66] Scholars contend that it is for this reason that States rarely formally derogate from their human rights obligations.[67]

Where and when do a State's human rights obligations apply? The answer to this question varies because of the slightly different language in the application provisions of human rights instruments and how their relevant interpretive bodies construe those provisions. Generally, a State owes human rights obligations to those subject to its jurisdiction, which includes, at a minimum, those within the State's sovereign territory. However, States may exercise jurisdiction extraterritorially and therefore may owe certain rights to those who fall under their effective control. What degree of control is necessary, and how a State can achieve that level of control, is subject to debate and disagreement between international and regional adjudicative bodies and is the subject of numerous academic studies.[68] In brief, there are two generally recognized means of extending a State's human rights obligations abroad: (1) when a State exercises physical control over foreign territory (the spatial model),[69] and (2) when a State exercises physical control over an individual (or individuals) in foreign territory (the personal model).[70] Notably, much of

65 *See, e.g.*, *ICCPR*, *supra* note 52, art. 4; *ECHR*, *supra* note 53, art. 15; *ACHR*, *supra* note 54, art. 27.

66 Oona A. Hathaway et al., *Which Law Governs During Armed Conflict: The Relationship between International Humanitarian Law and Human Rights Law*, 96:6 MINN. L. REV. 1883, at 1925 (2012).

67 *Id.*; *see also* Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AJIL 119, at 135–36 (2005).

68 *See, e.g.*, MICHAL GONDEK, THE REACH OF HUMAN RIGHTS IN A GLOBALIZING WORLD: EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES (2009); SIGRUN I. SKOGLY, BEYOND NATIONAL BORDERS: STATES' HUMAN RIGHTS OBLIGATIONS IN INTERNATIONAL COOPERATION (2006); MARKO MILANOVIĆ, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLE AND POLICY (2011); Marko Milanović & Tatjana Papić, *The Applicability of the ECHR in Contested Territories*, 67 ICLQ 779 (2018); Samantha Besson, *The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts To*, 25 LEIDEN J. INTL. L. 857 (2012).

69 *Drozd and Janousek v. France and Spain*, 52 Eur. Ct. H.R. 1992; *Gentilhomme v. France*, 441 Eur. Ct. H.R. 2002; *X and Y v. Switzerland*, 9 DR 57 (1977).

70 *See Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion [2004] I.C.J Rep. 136 [*Wall Case*]; UNHRC, *Mohammad Munaf v. Romania*, U.N. Doc. CCPR/C/96/D/1539/2006 (2009) at 14.2; UNHRC, *Lopez v. Uruguay*, U.N. Doc. CCPR/C/13/D/52/1979 (1981); *Al-Skeini and Others v. United Kingdom* 1093 Eur. Ct. H.R. (2011) [*Al-Skeini*]; *Jamaa v. Italy*,

the case law recognizing the extraterritorial application of human rights instruments arises from situations of armed conflict. Notably, uncertainty about IHRL's extraterritorial application may be another reason why derogations are unlikely when a State is a party to an armed conflict abroad. Formal derogation would signal a State's acceptance that IHRL governs their foreign conduct and expose its actions to judicial scrutiny by human rights bodies.

Does this mean the right to privacy ceases if no State has effective control over a population or territory? In short, no. Some elements of the right to privacy protected by IHRL are also protected under IHL. Article 46 of the Fourth Hague Convention on the Regulations concerning the Laws and Customs of War on Land stipulates:

> Family honour and rights, the lives of persons, and private property, as well as religious convictions and practice, must be respected. Private property cannot be confiscated.[71]

This article, like most of the substantive provisions of the Hague Conventions, is considered customary international law. Article 27 of Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, universally ratified, expands on this obligation:

> Protected persons 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… However, the Parties to the conflict may take such measures of control and security in regard to protected persons as may be necessary as a result of the war.[72]

Similarly, Article 75 of AP I mandates that an occupying force shall respect "the person, honour, convictions and religious practices" of all persons subject to its power.[73]

55 EHRR 627 (2012); *Al-Saadoon v. United Kingdom*, 49 EHRR SE95 (2009); *Medvedyev v. France*, 51 EHRR 899 (2010); *Öcalan v. Turkey*, 282 Eur. Ct. H.R. (2005); *Issa v. Turkey*, 629 Eur. Ct. H.R. (2004).

71 *Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, Oct. 18, 1907, art. 46.

72 *Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War*, 75 U.N.T.S. 287, art. 27 (GC IV).

73 AP I, *supra* note 26.

The language of Article 27 of GC IV is largely consistent with Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Unfortunately, there has been very little written about the scope of privacy protections under the Geneva Conventions. It is clear from the provision that privacy rights are not absolute. However, whether the right to privacy under IHL includes the full range of protections afforded by various human rights instruments is untested and, given the fact that IHL applies equally to State and non-State parties to a conflict, highly questionable. At the very least, the ICRC commentary on this article explains that the fundamental right to the protection of one's honour includes respect for a person's physical and intellectual integrity. Stemming from the need to respect one's integrity is the obligation that "individual persons' names or photographs, or aspects of their private lives must not be given publicity."[74]

Because of the uncertainty regarding the scope of IHL's privacy protections, the remainder of this chapter will focus on the right to privacy during an armed conflict under IHRL.

II
PRIVACY AND PRECAUTION — A COMPLEMENTARY RELATIONSHIP

The previous section established that in times of armed conflict, IHL governs the conduct of all parties to that conflict. By contrast, IHRL governs the actions of State governments in relation to those subject to their jurisdiction. In practice, this means that two distinct bodies of law can and do govern the actions of States during an armed conflict, a fact that is now firmly accepted by the International Court of Justice,[75] the UN Security Council,[76] and universal and regional human rights bodies.[77]

74 O.M. Uhler and H. Coursier (eds), *Commentary to Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War* (ICRC, 1958), 201.

75 International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of July 8, 1996, [1996] ICJ Reports, at 226 [hereinafter *Nuclear Weapons Advisory Opinion*]; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of July 9, 2004, [2004] ICJ Reports, at 136 [hereinafter *Wall Case*]; ICJ, Case Concerning Armed Activities on the Territory of the Congo (*D.R.C. v. Uganda*), Judgment of Dec. 19, 2005, para. 216 [hereinafter *DRC v. Uganda*].

76 S.C. Res. 1019, U.N. Doc. S/RES/1019 (Nov. 9, 1995) and S.C. Res. 1034, U.N. Doc. S/RES/1034 (Dec. 21, 1995) (in regard to former Yugoslavia); S.C. Res. 1635, U.N. Doc. S/RES/1635 (Oct. 28, 2005) and S.C. Res. 1653, U.N. Doc. S/RES/1653 (Jan. 27, 2006) (Great Lakes region).

77 *See, e.g.*, United States of America, U.N. Doc. CCPR/C/USA/ CO/3/Rev1 (Dec. 18, 2006); United

Thus, as long as there is no derogation and the right to privacy does not conflict with a State's obligations under IHL, there is no basis to suggest that a home State is not entirely bound by its privacy obligations to those within its territory.[78] Moreover, where a State exercises effective control over foreign territory or persons during an armed conflict, that State will have obligations vis-à-vis the privacy of individuals subject to their control.

Still, the 20-year Global War on Terror (GWOT) has highlighted that the principles and rules under IHL and IHRL are often inconsistent and, in some instances, diametrically opposed. The most obvious and widely analyzed example is the right to life protected under various human rights instruments and customary IHRL, and the right under IHL to target and kill enemy combatants (and where proportionate and necessary, to injure or kill civilians.)[79] In the first decade of the GWOT, several scholars studied the relationship between IHRL and IHL and proposed methods for resolving conflicts between the two sets of obligations when they arise.[80]

In 2012, Professor Oona Hathaway and her students surveyed that scholarship and the existing jurisprudence.[81] They identified three theoretical approaches to understanding the relationship between the two bodies of law: the displacement model, the complementarity model, and the conflict resolution model. The displacement model, which suggests that in times of armed conflict, IHL displaces human rights law, has now largely fallen out of favour.[82] The basis for this argument is that, in times of conflict, IHL is *lex specialis* (specialized law) and therefore supersedes IHRL, the *lex generalis* (general law). In other words, the two bodies of law are mutually exclusive. As noted above, jurisprudence and opinions of various adjudicative bodies have repeatedly affirmed that human rights

Kingdom, U.N. Doc. CCPR/C/GBR/CO/6 (July 30, 2008; *Abella v. Argentina* (Case no 11.137, Report no 55/97, IACmHR, Nov. 18, 1997); *Al-Skeini and Others v. UK* (Application no 55721/07, ECtHR GC, July 7, 2011).

78 For more on this position, see Lubin, *supra* note 60.

79 For a full discussion, see Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98:1 AJIL 1, 8–10 (2004); *see also* Geoffrey Corn, *Mixing Apples and Hand Grenades: The Logical Limit of Applying Human Rights Norms to Armed Conflict*, 1(1) J INTL. HUM LEGAL STUD. 52, 74–84 (2010).

80 *See, e.g.*, Cordula Droege, *The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict*, 40:2 ISRAEL LAW REV. 310 (2007); Noam Lubell, *Challenges in Applying Human Rights Law to Armed Conflict*, 860 INTL. REV. RED CROSS 737 (2005); William H. Boothby, *Making Sense of the Human Rights Law/Law of Armed Conflict Conundrum: A Practical Proposal*, *in* CONFLICT LAW (2008); Françoise J. Hampson, *The Relationship between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body*, 90:871 INTL. REV. RED CROSS 549 (2008); Orna Ben-Naftali (ed), INTERNATIONAL HUMANITARIAN LAW AND INTERNATIONAL HUMAN RIGHTS LAW (2011); William A. Schabas, *Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum*, 40:2 ISRAEL L. REV. 592 (2007).

81 Hathaway et al., *supra* note 66.

82 *Id.* at 1894.

law continues to apply during armed conflict. As Noam Lubell and Nancie Prud'homme wrote in 2016, "The existence of a relationship between international human rights law and LOAC [the law of armed conflict] is now widely accepted. Their concurrent application is at present more or less a fait accompli but there remain debates on the nature of their interaction."[83]

This second approach identified by Hathaway et al. is the complementary model. This model holds that both IHL and IHRL apply during armed conflict and must be interpreted in light of one another.[84] The basis for this approach is that both humanitarian and human rights law share a common goal: to protect human life and dignity.[85] This model provides that IHL can be used to inform our interpretation of a State's human rights obligations during hostilities in a way that allows us to avoid conflict between the two legal doctrines. For example, in its *Nuclear Weapons Advisory Opinion*, the International Court of Justice (ICJ) found it appropriate to use IHL to interpret what constituted an "arbitrary deprivation of life," as prohibited by Article 6 of the ICCPR.[86] As in that case, the language, structure, and purpose of the two norms will often make it relatively easy to resolve any tension between IHL and IHRL rules.

The third approach is the conflict resolution model, which asserts that IHL and IHRL are complementary during an armed conflict unless there is a conflict. When a conflict arises, a decision-maker must select either the IHL or the IHRL rule, recognizing that the application of one may lead to a breach of the other.

We know from Part 1 that IHL requires that a State with the capacity to use advanced technology (like FRT) to distinguish combatants from non-combatants more accurately is obligated to do so. At the same time, IHRL tells us that the mass collection of biometric data and persistent surveillance of a population infringes upon the right to privacy guaranteed under numerous human rights instruments. Viewed in absolute terms, these two well-established rules of international law pull States in opposing directions. To determine what effect this tension has on a State's legal obligations, we need to consider Hathaway's models.

As explained above, practice and precedent have moved beyond the displacement approach to conflict resolution. It is insufficient to suggest that due to the existence of an armed conflict, States no longer owe

83 Noam Lubell & Nancie Prud'homme, *Impact of Human Rights Law*, *in* ROUTLEDGE HANDBOOK OF THE LAW OF ARMED CONFLICT 106, 107 (Rain Liivoja & Tim McCormack eds., 2016).
84 Hathaway et al., *supra* note 66, at 2012.
85 *Id*.
86 *Nuclear Weapons Advisory Opinion*, *supra* note 75, para. 25.

privacy rights to those within their territory or subject to their jurisdiction.[87] Instead, we must ask whether these two obligations can be applied and interpreted in a way that complements each other (i.e., can conflict be avoided) or whether an actual conflict exists. To do so, Hathaway tells us we must determine whether the rules are in a "relationship of interpretation" or a "relationship of conflict."[88]

I propose that in an armed conflict, the protection of privacy and IHL's targeting rules are always in a relationship of interpretation. As such, their relation can be understood using the complementary approach. This argument is persuasive because the right to privacy is not absolute. It is a right to be free from arbitrary and unlawful intrusions into one's private life by the State. A State may take actions that engage a person's right to privacy, but so long as those actions are prescribed by law, necessary, and proportionate, and there are adequate safeguards, those actions will be consistent with IHRL. Moreover, what is necessary, proportionate, and adequate is highly contextual and fact-dependent. As the ICJ remarked in its *Nuclear Weapons Advisory Opinion*, we can use IHL to help us interpret what is necessary, proportionate, and adequate in an armed conflict, be it an IAC, NIAC, or a prolonged occupation.

For example, the precautionary principle under IHL stipulates that military commanders must do everything feasible to verify that attacked objectives are not civilian and take all feasible precautions when selecting a means and method of attack to minimize incidental civilian casualties. These rules obligate States to take positive steps to collect intelligence and conduct surveillance so that they can efficiently and effectively distinguish friend from foe.[89] Therefore the need to comply with the Geneva Conventions must influence our interpretation of whether using a surveillance technique or program like FRT is necessary and proportionate under IHRL during an armed conflict.

Recall, however, that States with FRT capabilities are not obligated in every instance to use this technology to comply with Article 57 of *AP 1.* If there are alternative means of safely and efficiently verifying the nature of the target and satisfying the precautionary principle while having less of an impact on civilians, a State with FRT does not need to use it in every instance. Where possible, the IHRL right to privacy should, therefore, also

87 For more on this, see Lubin, *supra* note 60; Benjamin Waters, *An International Right to Privacy: Israel Intelligence Collection in the Occupied Palestinian Territories*, 50 GEORGETOWN J INTL. L. 537 (2019).

88 Hathaway et al., *supra* note 66, at 1905.

89 Lubin, *supra* note 60, at 486, *citing* Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia (June 13, 2000), http://www.icty.org/en/press/final-report-prosecutor-committeeestablished-review-nato-bombing-campaign-against-federal, para. 50.

influence the choice of surveillance programs and techniques employed by military commanders, or at the very least, the safeguards and procedures adopted to govern their use.

IHL accepts that, given the nature of war, it is not always possible to select the least intrusive means of complying with Article 57. Moreover, it may be impossible, in the face of ongoing violence, to decide and ensure that information collected on the battlefield is only that which is necessary, let alone that the information is recorded and stored accurately in a fair, transparent, and consensual process. Nevertheless, the right to privacy, interpreted in light of IHL, is flexible enough to apply in times of severe insecurity and violence.

III
OPERATIONALIZING THE RIGHT TO PRIVACY

In an armed conflict, the right to privacy and the precautionary principles must be interpreted in light of one another. This argument is sustainable because both obligations are highly contextual. Therefore, what is required to satisfy privacy and precaution is not static but driven by facts and must reflect the operational environment. While this flexibility is critical to the joint application of the rules around precaution and privacy, it will also create significant uncertainty for those tasked with interpreting and applying the law. This ambiguity is primarily a result of the fact that armed conflicts are not static environments. The early years of the war in Afghanistan may be characterized as an occupation, with widespread and protracted violence between organized armed forces. That conflict ultimately evolved into a large multinational stability and counterinsurgency operation in partnership with the Afghan government and, in later years, became a counterterrorism and training mission. However, this evolution was not linear; there were times later in the conflict when heavy fighting occurred between the Taliban and coalition forces.

All this is to say that what qualified as necessary and proportionate violations of privacy in the name of Afghan and coalition security at the outset of the conflict were vastly different from what would have qualified as necessary and proportionate intrusions in recent years. Likewise, the challenges of complying with IHL, specifically the principle of distinction

and precaution, varied significantly over the 20-year conflict, especially as the mission moved from sustained force-on-force fighting into more targeted covert and law-enforcement-like operations. Yet throughout the conflict, US forces continued to collect, analyze, and use biometric data collected from Afghans to maintain identity dominance over the enemy. As far as has been reported, there was no additional consideration to the privacy rights of the country's civilian population.[90] This practice was inconsistent with IHRL.

The balance between the privacy rights of civilians and the operational necessity to leverage advanced surveillance techniques to comply with the precautionary principles is not fixed. I suggest that where that balance lies depends on two factors: (1) a State's effective control over a population or territory; and (2) the threat and level of violence.

Both factors are routinely relied upon to determine what measures a State must undertake to meet its legal obligations under IHL and IHRL. For example, in the *Targeted Killings Case*, Israel's Supreme Court held that, per the State's human rights obligations, a civilian taking direct part in hostilities should not be attacked if it is possible to use less harmful means.[91] (This limit, the Court held, was derived from the IHL principle of proportionality.[92]) Instead, said the Court, "if it is possible to arrest, interrogate and prosecute a terrorist who is taking a direct part in hostilities, these steps should be followed."[93] However, the Supreme Court recognized that taking less harmful measures is not always feasible. It noted explicitly that consideration must be given to the risk to life for soldiers and civilians and whether the military controlled the territory where the operation would take place.[94] As Ken Watkin explains, "control and risk (to both soldiers and civilians) are intimately intertwined."[95]

More recently, in *Georgia v. Russia (II)*, the Grand Chamber of the European Court of Human Rights (ECtHR) held that the level of violence or "the context of chaos" in an armed conflict is an important consideration when determining whether a foreign military (in this instance Russia) has effective control, and by consequence, the scope of that State's human rights obligations.[96] The ECtHR explained:

90 Whether such privacy considerations were ever taken into account is unclear from reporting and official records. I intend to research this question further.
91 *Public Committee Against Torture v. Government* [2006] (2) IsrLR 459, at 501 [*Targeted Killings Case*].
92 *Id.*
93 *Id.*
94 *Id.* at 501–2.
95 KENNETH WATKIN, Fighting at the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict, 223 (2016).
96 *Georgia v. Russia (II)*, 2021 Eur Ct HR.

> that in the event of military operations—including, for example, armed attacks, bombing or shelling—carried out during an international armed conflict one cannot generally speak of "effective control" over an area. The very reality of armed confrontation and fighting between enemy military forces seeking to establish control over an area in a context of chaos means that there is no control over an area.[97]

However, once Russia gained control over the area of Georgia in question and effectively occupied the region, the Court held that the spatial model of extraterritorial jurisdiction triggered the application of Article 1 and the full scope of the ECHR.[98] The Court also found that when it came to Article 2 and the deprivation of life, the personal jurisdiction model was not applicable in the "active phase of hostilities."[99] However, the Court did find that where Russia detained persons in the active phase of hostilities, the personal model of asserting jurisdiction would satisfy Article 1. Moreover, the Court decided that the context of chaos did not impact Russia's procedural obligation under Article 2 to investigate potentially unlawful uses of lethal force committed during the active phase of the conflict.[100]

Unfortunately, what the ECtHR failed to account for in its reasoning is that the level of violence, and therefore a State's effective control, not only shift in a non-linear fashion across time but also may vary geographically.[101] This fact is especially apparent in the context of Afghanistan. The complexity of that operating environment is often explained using Kurlak's concept of the "three-block war."[102] On one block, forces engage in traditional armed conflict; on the second, they conduct peacekeeping or stabilization operations; and on the third, they provide humanitarian aid.

Nevertheless, for the purpose of this chapter, the *Georgia v. Russia (II)* decision is helpful in two respects. First, it affirms that effective control

97 *Id.* para. 126.
98 *Id.* para. 174.
99 *Id.* para. 144.
100 *Id.* para. 332.
101 Marko Milanovic explains this succinctly: "The question of whether continued, intense fighting precludes a finding of effective control over territory is a perfectly valid one.... The problem with the Court's reasoning here is its *categorical* nature. It's one thing to say that control over territory is a very fluid thing, especially in a very short time-frame and with respect to a relatively small area of territory, as on the facts of this case. But it is in principle perfectly possible for an invading army to gradually establish reasonably stable control over areas of enemy territory, as it advances through it, even though the hostilities may still be happening on the fringes of that territory." *Georgia v. Russia No. 2: The European Court's Resurrection of Bankovic in the Contexts of Chaos*, EJIL: TALK!, Jan. 25, 2021, https://www.ejiltalk.org/georgia-v-russia-no-2-the-european-courts-resurrection-of-bankovic-in-the-contexts-of-chaos/.
102 Charles C. Krulak, *The Strategic Corporal: Leadership in the Three Block War*, MARINE CORP. GAZETTE, Jan. 1991, at 18, 20–21.

and the level of violence are key factors when determining the scope of a foreign State's extraterritorial human rights obligations during an armed conflict. Second, it recognizes that what is required to comply with IHRL can vary throughout a single conflict.

What does this mean in practice? In times of sustained and intense violence, we should expect that a State's privacy obligations vis-à-vis those within its territory or effective control will be minimal and likely consistent with the limited protections afforded under IHL. Instead, the emphasis should be on the State's obligation to collect the necessary intelligence and analysis to comply with the precautionary principles. However, as the level of control over territory increases and the threat of violence decreases, intrusions upon privacy will become less justifiable.

Recalling the five privacy principles, it would, therefore, be inconsistent with IHRL to deploy an intrusive FRT program at the height of a conflict and then continue to employ and even expand the use of that program as the nature of the conflict evolves, and with it, the range of privacy-invasive activities that are necessary and proportionate in the face of that conflict. As a conflict moves along the spectrum of insecurity and violence, so too does a State's privacy obligations to those subject to its jurisdiction. A State's surveillance and biometrics programs and its operational procedures must, therefore, be able to adapt to meet those changing obligations.

For this reason, policies and procedures need to be built into the development of FRT before it is deployed widely in armed conflict. Those policies should reflect privacy principles, evolving data protection norms,[103] and a State's domestic or regional data protection obligations.[104] At a minimum, they should address the following questions:

- Under what circumstances may FRT be deployed, and by who?
- What data will the FRT draw on to identify individuals?
    - How revealing or invasive is the use of that data in conjunction with FRT?
    - How will false positives and false negatives be corrected?

103 *See* Lubin, *supra* note 60, at 475–76.

104 Notably, many data protection regimes permit necessary and proportionate legislated exceptions from most data protection principles and obligations where required for national security, defence, public security, and the prevention of crime. *See, e.g.*, *General Data Protection Regulation*, (EU) 2016/679, art. 23.

- Will data be collected through the use of FRT? (E.g., name, location, date/time, associations)
    - If so, how will that data be stored and secured, and for how long?
    - Who has access to that data?
    - For what purposes can that data be used, processed, and shared?
    - What will be done with the data once the armed conflict is over?
- What are the consequences for improper use of FRT or the resulting data, and procedures for reporting improper use?

Additionally, policies must account for the fact that what IHRL requires in terms of respect for privacy will shift along the spectrum of conflict. Therefore, an appropriate way to account for fluctuating privacy obligations would be to consider what function or task the State's forces are carrying out and set policies and procedures for FRT use and data collection consistent with those activities. Alternatively, returning to the concept of the three-block war, FRT policies and privacy protections should reflect the "block" on which forces are operating. Thus, on the first block, policies around FRT use will be the least restrictive, reflecting IHL's targeting rules and aligning closely with IHL privacy protections. On the second block, FRT policies might look more like privacy regimes regulating domestic and foreign intelligence collection and surveillance. Finally, on the third block, FRT use might be regulated similarly to its deployment in a law enforcement context. Adapting this function-based approach is consistent with the practice of calibrating rules of engagement around the use of force for each "block."[105]

Ultimately, the technical capacity and policies must exist so that military commanders can appropriately modify the use of FRT as a conflict moves along the spectrum of insecurity and violence. Deploying intrusive and indiscriminate technology to meet an urgent battlefield need does not absolve a State of its human rights obligations for however long an armed conflict endures.

105 WATKIN, *supra* note 95, at 15.

CONCLUSION

FRT can enhance a military commander's capacity to identify and distinguish combatants from non-combatants in armed conflicts. Given the nature of today's modern conflicts, this surveillance tool could significantly reduce civilian casualties and increase military effectiveness, two of the underlying aims of IHL. However, the widespread and indiscriminate use of FRT also poses significant privacy risks, protected by numerous international and regional human rights instruments.

At first glance, the use of FRT may appear to pit a State's obligations under IHL against its IHRL obligations. Nonetheless, this chapter sought to establish that the principle of distinction and precaution and the right to privacy are not in true conflict but rather maintain a relationship of interpretation that can be resolved using the complementarity approach. As such, in an armed conflict, a State's human rights obligations vis-à-vis privacy should be interpreted in a manner that not only recognizes the unique context of war but also is consistent with IHL's targeting rules. Nevertheless, when employing FRT, what is required to comply with a State's privacy obligations is likely to vary (and vary considerably) over the course of an armed conflict. As such, commanders must be prepared to adapt the use of FRT and have the policies, procedures, and safeguards in place to meet their changing obligations. Therefore, it is recommended that States adopt a function-based approach to ensure that the necessary policies and technical capabilities exist to meet these obligations before deploying FRT in an armed conflict.

Chapter 8

The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts

Eliza Watt[1]

INTRODUCTION

The use of unmanned aerial vehicles (UAVs, or drones),[2] satellite imagery and other data collection techniques are a vital part of intelligence gathering methods used in armed conflicts.[3] Information collection facilitated

1 Dr Eliza Watt is a Lecturer in Law at Middlesex University, London, United Kingdom; a Visiting Lecturer at British Law Centre, University of Warsaw, Poland; and a guest speaker at the College of Information and Cyberspace, National Defense University, Washington D.C. USA. I wish to thank Professor Laurent Pech for his careful reviewing and commenting on this paper. Many thanks to Dr Russell Buchan and Dr Asaf Lubin for their generous guidance and feedback on the earlier drafts. I am also grateful to the participants of the 2021 NATO CCDCOE Berlin Scholars Workshop for their commentary and observations.

2 *See* Ben Knight, *Guide To Drones*, DW (June 30, 2017), https://www.dw.com/en/a-guide-to-military-drones/a-39441185.

3 Geneva Convention for Amelioration of the Conditions of the Wounded and Sick in Armed Forces in the Field; 1949 Geneva Convention for the Amelioration of the Conditions of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea; Geneva Convention Relative to the Treatment of Prisoners of War; Geneva Convention Relative to the Protection of Civilian Persons in Time of

by drones has a direct impact on a broad range of combat operations, from the ability to locate potential military objects (such as missile launchers) and mark them for destruction, in support of strategic and operational reconnaissance missions and detecting enemy movements, to supporting the safety of the ground forces through detecting surprise attacks and in identifying combatants who may be lawfully targeted.

This latter deployment of surveillance drones is particularly controversial, because the obtained data has been used for targeted killings,[4] including by armed drones.[5] The legality of such operations has been the subject of scrutiny at the United Nations (UN) and European levels and assessed chiefly in the context of international human rights law (IHRL)[6] (principally in relation to the arbitrary deprivation of life) and under the law of the use of force (*jus ad bellum*)[7] and international humanitarian law (IHL, or *jus in bello*). Nevertheless, to date little attention has been paid to States' use of UAVs for surveillance purposes and its impact on non-combatants' privacy. Yet, their constant presence causes "considerable and under-accounted-for harm to the daily lives of ordinary civilians, beyond death and physical injury",[8] terrorising men, women and children, thus giving rise to anxiety and psychological trauma among those exposed to persistent observation.

The primary legal regime that applies in situations of armed conflict is IHL. However, the relevant treaties, namely the Hague Regulations of 1899 and 1907, the Geneva Conventions I–IV of 1949 (Geneva Conventions) and their Additional Protocols of 1977 (AP I and AP II)[9] do not directly address the impact of belligerents' intelligence operations on civilians' privacy and data protection rights. Conversely, peacetime State surveillance, including mass interception and collection of foreign

War, common art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S.135 [hereinafter Common art. 2]. In the main text, referred to collectively as "Geneva Conventions".

4 For the definition of targeted killing, see Philip Alston (Special Rapporteur), *Report on Extrajudicial, Summary or Arbitrary Executions*, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) ¶ 1 [hereinafter A/HRC/14/24/Add.6].

5 *See id.*; INTERNATIONAL HUMAN RIGHTS AND CONFLICT RESOLUTION CLINIC, LIVING UNDER DRONES. DEATH, INJURY AND TRAUMA TO CIVILIANS FROM US DRONE PRACTICES IN PAKISTAN, (Stanford Law School 2012) [hereinafter LIVING UNDER DRONES].

6 *See also* Ben Emmerson (Special Rapporteur), *Report on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/HRC/25/59 (Mar. 11, 2014) [hereinafter A/HRC/25/59]; Eur. Consult. Ass., Drones and Targeted Killing: The Need to Uphold Human Rights and International Law, Doc. No. 13731 (2015), 7 ¶ 18 [hereinafter CoE Report 2015]; Christof Heyns et al., *The International Law Framework Regulating the Use of Armed Drones*, 65 INT. COMP. LAW Q. 791 (2016).

7 *See* A/HRC/14/24/Add.6, *supra* note 4; Heyns et al., *supra* note 6.

8 LIVING UNDER DRONES, *supra* note 5, ¶ vii.

9 Protocol Additional to the Geneva Conventions of 12 August, 1949, and relating to the Protection of Victims of International Armed Conflicts June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

communications, is subject to a complex set of privacy and data protection standards set out in international and regional human rights conventions, including Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR),[10] Article 8 of the European Convention on Human Rights 1950 (ECHR),[11] together with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[12]

With the advancements in drone technology and the increase in their deployment in armed conflicts, privacy concerns loom large, yet they remain unaddressed in the existing IHL framework. Consequently, this chapter asks how the right to privacy of civilians can be protected during inter-State hostilities and examines what role IHRL may have in safeguarding this right, and ultimately inquires into whether there is a need for specific regulation of intelligence gathering operations by drones.

The study begins by outlining States' use of UAVs and the impact of prolonged surveillance in war zones (Part I). Against this backdrop, Part II analyses the application of IHL and IHRL rules in such circumstances. Specifically, it identifies the interplay between these legal regimes from the perspective of intelligence gathering operations. The chapter argues that in such cases IHRL rules apply alongside IHL. Furthermore, it identifies that the principle of constant care set out in Article 57(1) of AP I to the Geneva Conventions and established under the general customary principle of precautions in attack has a significant role to play in bridging the gap left by the IHL to ensure respect of civilians' privacy and data protection rights. Part III discusses the relevance of the rules on privacy of communications to drone surveillance in armed conflict and considers when and how States are allowed to derogate from, or otherwise limit, this right. Moreover, it proposes introducing minimum data protection and privacy safeguards for drone surveillance, the latter akin to those stipulated by the European Court of Human Rights (ECtHR) for bulk collection of foreign communications.

10 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

11 European Convention for the Protection of Human Rights and Fundamental Freedoms amended by Protocols Nos 11 and 14, Nov. 4, 1950 E.T.S. 5 [hereinafter ECHR].

12 Charter of Fundamental Rights of the European Union, Oct. 2, 2000, C. 3031 [hereinafter EU Charter].

I
THE USE OF DRONES AND ITS IMPLICATIONS IN WAR ZONES AND BEYOND

A STATES' USE OF DRONES IN MILITARY OPERATIONS

Armed drones were initially operated by a handful of States, including the US, the United Kingdom (UK), Israel and Russia, in a number of combat zones, such as Afghanistan, Pakistan and Yemen, with the predominant aim of targeted killings. Recent reports attest to their increasing usage, with at least another ten States having conducted drone strikes, thirty-nine States with armed drones and twenty-nine States developing new generation armed drone technology.[13]

Drones for military use were originally designed for intelligence gathering and surveillance purposes. Equipped with high definition live-feed video, thermal infrared cameras, heat sensors, radar and mobile phone interception technology, together with such tools as licence plate readers, face recognition software and GPS trackers, UAVs allow for continuous surveillance and loitering over potential targets and/or areas and gathering of data which is then retained on military databases and shared among armed forces and intelligence agencies. With the changing nature of warfare, numerous regions across the world are seen as "battlefields" of the "global war on terror", as opposed to areas where an international armed conflict exists. Consequently, unrestricted long-term surveillance by drones is becoming commonplace.[14] Commenting on these themes on 31 August 2021[15] when marking the end of war in Afghanistan and the withdrawal of US troops, US President Joe Biden explained that the terror threat has spread beyond Afghanistan and metastasised across the world. This is one of the reasons behind US policy swaying away from the deployment of "thousands of American troops and spending billions of dollars a year in Afghanistan (to) fight a ground war",[16] and why the

13 Peter Bergen et al., *World of Drones*, NEW AMERICA (July 30, 2020), https://www.newamerica.org/international-security/reports/world-drones/.
14 CoE Report, *supra* note 6, ¶ 24 at 8.
15 *Remarks by President Biden on the End of the War in Afghanistan*, THE WHITE HOUSE (Aug. 31, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/.
16 *Id.* at 6.

President announced that US methods of engagement in future conflicts would be more remote in nature. This seems also to be the preferred policy goal of other governments and organisations, such as the European Union and the North Atlantic Treaty Organization. As drones are likely to proliferate, it becomes necessary to consider their impact on civilians, and this is addressed next.

B CIVILIAN IMPACT OF PROLONGED DRONE SURVEILLANCE AND PRIVACY IMPLICATIONS

States' UAV use has been shown to have a considerable detrimental effect beyond the death, injury and destruction immediately caused by drone strikes.[17] For example, the presence of US drones in Pakistan has reportedly caused substantial levels of fear and stress in the local population, with accounts of the experience of living under constant surveillance as harrowing.[18] Apart from common symptoms of anticipatory anxiety and post-traumatic stress disorder, persistent drone surveillance has had a negative effect on educational opportunities; on burial traditions and willingness to attend funerals; on economic, social and cultural activities; and it undermines community trust. In addition, the impact on non-combatants' privacy and data protection rights in situations of sustained drone surveillance is significant and manifold.

First, such practices are harmful, as they encroach on the respect for an individual's existence as a human being and his or her autonomy. These notions form the essence of the legal right to privacy guaranteed, *inter alia*, by Article 17(1) of the ICCPR and Article 8 of the ECHR which stipulate the right to privacy, family, home and correspondence. Second, they likely implicate the right to family life under the aforementioned provisions. Drone surveillance has been shown to impede civil liberties, including participation in social events, thus hindering familial relationships. Third, the notion of privacy also extends to the protection of individuals' homes.[19] In that sense, the "home" epitomises "a place of refuge where one can develop and enjoy domestic peace, harmony and

17 LIVING UNDER DRONES, *supra* note 5, at 73.

18 HUMAN RIGHTS CLINIC, THE CIVILIAN IMPACT OF DRONES: UNEXAMINED COSTS, UNANSWERED QUESTIONS, COLUMBIA LAW SCHOOL AND CENTRE FOR CIVILIANS IN CONFLICT (2012), 81 [hereinafter CIVILIAN IMPACT OF DRONES].

19 *See also* ICCPR, *supra* note 10, art. 17; ECHR, *supra* note 11, art. 8; U.N. Human Rights Committee, General Comment No.16: Article 17 (Right to Privacy), ¶ 5, U.N. Doc. HRI/GEN//1/Rev. 1 (Apr. 8, 1988) [hereinafter General Comment 16].

warmth without fear of disturbance".[20] Its protection relates not only to dwellings *per se*, but also covers areas over which ownership (or any other legal title) extends, including outside spaces, such as a garden.[21] It follows that every invasion of that sphere which occurs without consent of the affected individual interferes with the right to privacy.[22] Consequently, forced or clandestine trespassing, electronic surveillance practices, listening devices, covert CCTV cameras and video surveillance[23] have all been held to amount to interfering with the protected rights. Fourth, drone surveillance also instils a constant feeling of being watched which, as shown by Jeremy Bentham's Panopticon project,[24] serves as a deterrent to leading a relatively unconstrained existence. In the situation of armed conflicts, this is exacerbated as it engenders fear of a possible drone attack. Fifth, as observed by Harry Wingo, writing in the context of law enforcement agencies' use of non-lethal drones to respond to shooting accidents in the US, "surveillance drones raise privacy concerns because of their ability to harness powerful camera technology along with precision flight and pursuit capabilities that result in "drone stare"—the ability to observe persons in ways that have been previously impossible".[25] Such surveillance, especially when a drone is not visible epitomises what Michel Foucault called "the power of the gaze",[26] which creates a control mechanism by the watchers over the watched. This invariably introduces anxiety that alters how those under constant observation behave, think and interact.

Another implication of ubiquitous drone surveillance is from the perspective of data protection[27] and relates to the subsequent processing of personal information which includes images (such as those of individuals, houses, vehicles, vehicle licence plates), sound geolocation data and any other electromagnetic signals. Those subject to UAVs presence are likely to be unaware that the processing of their personal data is carried out, how such information is intended to be used and by whom. In addition, the volume of the gathered material far outpaces the operators'

20 William A. Schabas, Nowak's CCPR Commentary: U.N. International Covenant on Civil and Political Rights, 485 (N.P. Engel, 3rd ed., 2019) [hereinafter Nowak's Commentary].
21 *Id.*
22 Nowak's Commentary, *supra* note 20, at 486.
23 *See also* Peck v. United Kingdom Eur. Ct. H.R. 2003-I; Perry v. United Kingdom 39 Eur. Ct. H.R. 2003-IX.
24 *See* Jeremy Bentham, The Works of Jeremy Bentham (William Trait, 1838–43).
25 Harry Wingo, *Set Your Drones to Stun: Using Cyber Secure Quadcopters to Disrupt Active Shooters*, 17(2) Journal of Information Warfare 55, 59 (2018).
26 Michel Foucault, Discipline and Punish: The Birth of the Prison (Vintage Books 1979).
27 Privacy and data protection are related but not identical rights. Unlike privacy, data protection "regulates the processing of an individual's personal data—be it private or non-private" whereas "privacy protects an individual against intrusions in to his private sphere". Kriangsak Kittchaisaree, Public International Law in Cyberspace, 59 (Springer 2017).

capabilities to process and analyse it, thus creating an information overload, or "data crush", consequently making it almost impossible for the relevant personnel to make sense of and effectively use that information for operational purposes.[28] To help quickly turn enormous quantities of data into actionable intelligence, some military forces have utilised artificial intelligence (AI) and machine learning (ML) technologies with the assistance of private sector industries. A case in point is the US Department of Defense Project Algorithmic Warfare Cross-Functional Team (Project Maven).[29] Since 2017, its specialist algorithms that are capable of searching, identifying and categorising objects of interest within colossal volumes of material including from surveillance drones have reportedly increased efficiency and enabled decision making on the battlefield. The success of the Maven Project arguably marks the beginning of "information-age war", as the militaries are moving away from hardware-centric organisations towards being driven by AI and ML. As a result of these and similar developments, acquisition of data via drone collection is likely to increase in the future.

For at least a decade the UN,[30] a number of European institutions[31] and human rights mandate holders[32] have grappled with the issues of States' use of armed drones in conflict zones. In essence, to date these efforts have focused mainly on their deployment in extraterritorial lethal operations and the implication this has on a number of international law rules, including State sovereignty, IHL (principles of distinction, necessity and proportionality) and IHRL pertaining to the right to life. Little, or no attention has been paid to privacy and data protection of non-combatants, but there can be no doubt that these concerns call for the setting out of international normative standards due to the likely future omnipresent

28 CIVILIAN IMPACT OF DRONES, *supra* note 18, at 40.

29 Richard H. Shultz and Richard D. Clarke, *Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare*, MODERN WAR INSTITUTE (Aug. 25, 2020), https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.

30 *See also* U.N. Human Rights Council, Ensuring Use of Remotely Piloted Aircraft or Armed Drones in Counter-Terrorism and Military Operations in Accordance with International Law, Including International Human Rights Law and Humanitarian Law, (Mar. 28, 2014) U.N. Doc A/HRC/25/L.32; UN Human Rights Council, Ensuring Use of Remotely Piloted Aircraft or Armed Drones in Counter-terrorism and Military Operations in Accordance with International Law, Including International Human Rights and Humanitarian Law, (Mar. 19, 2015) UN Doc A/HRC/28/L.2.

31 *See also* Eur. Consult. Ass., Drones and Targeted Killings: the Need to Uphold Human Rights and International Law (Jan. 27, 2015); European Parliament, Written Declaration on the Use of Drones for Targeted Killings, (Jan. 16, 2012) DC\889077EN.doc; Nils Melzer, Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare (2013); EU Parliament, Resolution of 27 February 2014 on the Use of Armed Drones, (Feb. 27, 2014) 2014/2567(RSP); European Parliament, Resolution of 28 April 2016 on Attacks on Hospitals and Schools as Violations of International Humanitarian Law, (Apr. 28, 2016) (2016/2662(RSP)).

32 A/HRC/25/59, *supra* note 6.

use of drone technology. However, one question that needs to be addressed from the outset is why should this particular surveillance method be subject to specific regulation? After all, militaries have long used other long-term and pervasive techniques to gather intelligence, such as satellites. This is simply because satellite and drone technologies are different and therefore complementary, rather than rivalling each other because they are designed for different purposes. The former, being remote from the Earth's surface, provide a "macro" perspective of the given area and therefore much lower level of detail and resolution which is not useful when high accuracy is required. UAVs fill in this gap, as they operate at much lower altitudes than satellites and therefore give a "micro" view. Consequently, they are far more intrusive due to the specific and accurate information they gather and because they are easier to operate and are more manoeuvrable. This necessitates more emphasis on privacy and data protection when militaries engage in drone surveillance in and outside of combat zones as discussed below.

II
THE APPLICATION OF IHL AND IHRL TO PROLONGED DRONE SURVEILLANCE IN ARMED CONFLICT

IHL seeks to limit the effects of an armed conflict by protecting those who are not, or who are no longer, participating in the hostilities and by restricting the means and methods of warfare. IHL distinguishes between international armed conflicts (IAC) and non-international armed conflicts and this classification is crucial as different rules apply in each situation. Thus, an international armed conflict is defined in the common Article 2(1) to the Geneva Conventions as that which may "arise between two or more [States], even if the state of war is not recognized by one of them".[33] The 2016 International Committee of the Red Cross' (ICRC) revised Commentary to Geneva Convention I provides that "the determination of (IAC) existence within the meaning of Article 2(1) must be based solely on the prevailing facts demonstrating *de facto* existence

33 Common art. 2, *supra* note 3.

of hostilities between the belligerents, even without a declaration of war".[34] All four Geneva Conventions and Additional Protocol I apply to an IAC, whether or not it constitutes a declared war, regardless of parties' to the conflict recognizing it as such. Conversely, a non-international armed conflict entails a situation when the opposing parties are States and organised armed groups, or only armed groups and is subject to a more limited range of rules than those applicable to an IAC, set out in Article 3 common to the four Geneva Conventions and Additional Protocol II.

IHRL is a body of rules prescribing States' obligations to respect, protect and fulfil human rights of individuals. The high watermark in the development of this branch of international law was the adoption by the United Nations General Assembly of the Universal Declaration of Human Rights in 1948,[35] a document which for the first time in history enumerated basic civil, political, economic, social and cultural rights applicable to all. These rights were subsequently restated in, *inter alia*, the ICCPR. Generally, the rights stipulated in the human rights treaties are divided into two categories, namely absolute and qualified rights. States cannot derogate from absolute rights, such as those set out in the ICCPR, including the right to life (Article 6), the right not to be subjected to torture (Article 7) and slavery (Article 8) even in cases of emergency. By contrast, qualified rights, such as the right to privacy (Article 17), can be limited, or derogated from, as they must be balanced against public interest and can therefore be interfered with, subject to the stipulated conditions provided therein.

IHL and IHRL developed separately and differ in a number of key areas. First, IHRL predominantly applies in times of peace, whilst IHR is intended to operate during war, or an armed conflict. Second, IHRL deals with the relationship between a State and an individual. It obliges States to respect and ensure human rights to all individuals within their territory and subject to their jurisdiction.[36] In comparison, IHL aims to limit the effects of armed conflict and as such, it regulates the conduct of hostilities by State parties, recognising that when a situation of armed conflict exists between them a balance must be struck between humanity and military necessity. Finally, unlike some qualified human rights, the law of war cannot be derogated from, as it is specifically designed to

34 ICRC, Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Filed, Geneva 12 August 1946. Commentary of 2016. Article 2: Application of the Convention, https://ihl-databases.icrc.org/ihl/full/GCI-commentary.
35 Universal Declaration of Human Rights, Dec. 10, 1948, U.N.G.A. Res 217 A(III) (1948).
36 ICCPR, *supra* note 10, art. 2(1); ECHR, *supra* note 11, art. 1.

protect those who do not take part in the hostilities such as civilians, medical and religious military personnel (non-combatants), together with those who have ceased to participate in the conflict, such as wounded, shipwrecked and sick combatants and prisoners of war. This protection extends to respect for their lives, their physical and mental integrity, affords them legal guarantees and ensures that they be treated humanely in all circumstances.

Notwithstanding these differences between the two regimes, it has been recognized that there is a complementary nexus between IHL and IHRL in armed conflicts. Thus, the International Court of Justice (ICJ),[37] the Human Rights Committee (HRC), international tribunals[38] and some States[39] acknowledge that these bodies of law apply concurrently. To this end, the ICJ in the *Nuclear Weapons* Advisory Opinion[40] and in the *Wall* Advisory Opinion[41] held that the protection offered by human rights conventions, including the ICCPR, does not cease in times of war and/or armed conflict, except by operation of a derogation of the kind to be found in Article 4 of the ICCPR. In its General Comment 31, the HRC confirmed this conceptual parallel between IHL and IHRL, stating that:

> the Covenant applies also in situations of armed conflict to which the rules of international humanitarian law are applicable. While, in respect of certain Covenant rights, more specific rules of international humanitarian law may be specifically relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive.[42]

Nevertheless, it remains far from settled how these legal frameworks apply to specific situations and if any normative conflict arises between the rules in question due to their different scope and content, how it is to be resolved. International jurisprudence and academic opinion[43] offer

37 Legality of the Use or Threat of Nuclear Weapons, Advisory Opinion [1996] I.C.J Rep.226 [hereinafter Nuclear Weapons Advisory Opinion]; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion [2004] I.C.J Rep. 136 [hereinafter Wall Advisory Opinion].

38 Prosecutor v. Kunarac et al., (2001) I.C.T.Y ¶¶ 467, 471.

39 US DoD, Law of War Manual, ¶ 1.6.3.1 (2016); Germany, Federal Ministry of Defence, Law of Armed Conflict-Manual- Joint Service Regulation, ¶ 105 (2013).

40 Nuclear Weapons Advisory Opinion, *supra* note 37, ¶ 24.

41 Wall Advisory Opinion, *supra* note 37, ¶ 106.

42 U.N. Human Rights Committee, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 11, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004) [hereinafter General Comment 31].

43 *See also* Oona A. Hathaway et al., *Which Law Governs During Armed Conflict—The Relationship*

differing viewpoints. According to one approach, the IHL as *lex specialis* takes precedence over the application of the IHRL, whereas another holds that IHRL[44] complements IHL by filling its gaps, or as its interpretative tool.[45] The relationship between these two branches of law is often analyzed with reference to specific rights, such as the right to life,[46] the right to fair trial,[47] the prohibition of arbitrary detention[48] and in the context of military responses to terrorism.[49] However, perhaps one of the areas where this dichotomy is both most visible and difficult to reconcile is in the field of intelligence gathering, as it takes place in peacetime and during armed conflict alike. In the former situation, the question of which regime applies is relatively uncomplicated — these operations are mandated by both domestic statutes vesting surveillance powers to designated State organs, together with human rights law aimed at protecting individuals' privacy rights against a State's arbitrary and unlawful interference. In the context of armed conflict, the answer is more complex. This is because the law of war is the main legal framework, but as already noted, it pays little direct attention to the issue of protection of privacy. This matter is discussed next.

A INTELLIGENCE GATHERING AND PRIVACY IMPLICATIONS IN SITUATIONS OF IAC UNDER IHL

During armed hostilities, the main role of States' intelligence gathering operations is the identification of military targets. This is underpinned by the principle of distinction which is set out in Article 48 of AP I. Accordingly, to ensure respect for and protection of civilian populations and civilian objects, the parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian and

Between International Humanitarian Law and Human Rights Law, 96:6 Minn. L. Rev. 1883 (2012); William Schabas, *Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum*, 40:2 Israel L. Rev. 592 (2007).

44 Hathaway et al., *supra* note 43.

45 Nicholas Tsagourias and Alasdair Morrison, International Humanitarian Law. Cases, Materials and Commentary, 55 (Cambridge University Press 2018).

46 U.N. Human Rights Committee, Draft General Comment No. 36, Article 6: Right to Life, U.N. Doc. CCPR/C/GC/R.36/Rev (2015); U.N. Human Rights Council, *Report of the International Commission of Inquiry on Libya*, U.N. Doc. A/HRC/19/68 (2012); Al-Skeini and Others v. United Kingdom 55721/07 Eur. Ct. H.R. 2011; Case of the Santo Domingo Massacre v. Columbia 259 Inter-Am. Ct. H.R. 2012.

47 U.N. Human Right Committee, General Comment No. 32, Article 14: Right to Equality Before Courts and Tribunals and to a Fair Trial, U.N. Doc. CCPR/C/GC/32 (2007); Case of Castilla Petruzzi et al. v. Peru 52 I.A.Ct.H.R. 1999.

48 U.N. Human Rights Committee, General Comment No. 35, Article 9: Liberty and Security of Person, U.N. Doc. CCPR/C/GC/35 (2014); Hassan v. United Kingdom 29750/09 Eur. Ct. H.R. 2014.

49 Inter-American Commission on Human Rights, Report on Terrorism and Human Rights, OEA/Ser.L/V/II.116 Doc. 5 Reve. 1 corr. (2002).

military objectives and direct their operations only against the military objectives.[50]

In addition, the rule of target verification contained in Article 57(2)(a)(i) of AP I obliges those who plan or decide an attack to do "everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives".[51] To comply with these requirements, warring States are required to engage in intelligence gathering, surveillance and reconnaissance to identify the nature of the possible target to ensure that they only attack lawful military objectives.

Belligerents must also comply with the principle of proportionality[52] which prohibits attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which *would be excessive in relation to the concrete and direct military advantage anticipated*".[53] This obligation recognizes, however, collateral damage to civilians and civilian objects as part of an armed conflict. Nevertheless, those in charge of attacks must strike a balance between the military value of the destruction, neutralisation, or capture of the target and the incidental harm that the attack may cause to civilians. Intelligence gathering therefore aids the process of determination of such matters as whether there are civilians, or civilian buildings in the vicinity of the target, as well as the nature and the scale of harm likely to result from the attack.

Of equal significance in this context is also the principle of constant care stipulated in Article 57(1) of AP I, which provides that "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects".[54] Although the principle is not defined in IHL, it has been described as "the obligation of conduct, i.e. a positive and continuous obligation aimed at risk mitigation and harm prevention and the fulfilment of which requires the exercise of due diligence".[55] The rule has been referred to as a "general principle", as against one setting out specific obligations on States. That said, the use of the word "shall" in Article 57(1) is legally binding on the parties to AP I and as a consequence it applies to all domains of warfare and all levels

50 AP I, *supra* note 9, art. 48.
51 *Id.* art. 57(2)(a)(i).
52 *Id.* arts. 51(5)(b), 57(2)(a)(ii) and 57(2)(b).
53 *Id.* art. 51(5)(b) (emphasis added).
54 *Id.* art. 57(1).
55 International Law Association Study Group on the Conduct of Hostilities in the 21st Century, The Conduct of Hostilities and International Humanitarian Law. Challenges of 21st Century Warfare. 93 INT'L. L. Stud.322 (2017) [hereinafter ILA Study Group].

of operations.[56] However, since the title to Article 57 refers to "precautions in attack", this provision is often read as applying only in situations of attacks (i.e. "acts of violence against the adversary, whether in offence or in defence")[57] and therefore in conjunction with the scenarios enumerated in Article 57(2)–(5). This view seems quite limited though, as it has been advanced that the obligation to take constant care to spare civilian population must necessarily apply to the entire range of military operations, not only to attacks.[58] This broader reading is preferable because on the more restrictive interpretation, Article 57 would only pertain to attacks and specific situations set out in sub-paragraphs 2–5,[59] thus discounting a whole spectrum of military activities. Of note in this context is the ICRC Commentary on AP I (ICRC Commentary) which interprets "military activities" for the purposes of Article 57 as a term which "shall be understood to mean any movements, manoeuvres and *other activities whatsoever carried out by the armed forces with the view to combat*".[60] The doctrine of constant care must therefore be construed as a "stand-alone" obligation, that is, in addition to the general rules of taking precautionary measures in attacks contained in Article 57(2)–(5).[61] Some States, such as the UK, support such an expansive interpretation of this provision. Thus, the UK Manual of the Law of Armed Conflict[62] considers "military operations" to be a wider term than "attack", as they include the movement and deployment of armed forces.[63] The document further asserts that "the commander will have to bear in mind the effect on the civilian population of what he is planning to do and take steps to reduce that effect as much as possible. In planning or deciding on, or carrying out attacks, however, those responsible have more specific duties."[64] Therefore, based on the premise that the duty of constant care applies throughout the entire spectrum of combat operations, the next section examines whether it can serve to close the normative gap in the IHL framework by placing privacy and data protection obligations on States' intelligence operations.

56 *Id.* at 43.
57 AP I, *supra* note 9, art. 49(1).
58 ILA Study Group, *supra* note 55, at 42.
59 AP I, *supra* note 9, art. 57(2)–(5).
60 ICRC, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) 8 June 1977. Commentary of 1987. Precautions in Attack, ¶ 2191 (1987) (emphasis added).
61 ILA Study Group, *supra* note 55, at 43.
62 UK MoD, The Manual of the Law of Armed Conflict (Oxford University Press 2003).
63 *Id.* footnote 187 to ¶ 5.32.
64 *Id.* ¶ 5.32.1.

B INTELLIGENCE GATHERING AND PRIVACY IMPLICATIONS IN SITUATIONS OF IAC UNDER IHRL

International treaties, including the ICCPR and the ECHR, place an obligation on each State party to respect and ensure to all individuals the rights recognized in these instruments, including the right to privacy contained in Article 17 and Article 8 respectively. As drone surveillance is often conducted extraterritorially, the question that arises is whether States are bound by their treaty obligations in such instances. The matter of extraterritorial application of human rights treaties is not entirely settled, but as a general rule States owe human rights obligations predominantly to those who are within their territory. However, when a State exercises effective control over foreign area (the spatial model),[65] or physical control over an individual in a foreign country (the personal model),[66] then the human rights duties will extend beyond its borders.

As a general rule, States must adopt legislative or other measures to give effect to the rights stipulated in the treaties and provide effective domestic remedies for their violation. However, these requirements are subject to two caveats. First, States may derogate from their treaty obligations by temporarily suspending certain rights during public emergencies. Second, they may limit non-absolute rights and freedoms on the basis of permissible limitations clauses. The next part discusses both these mechanisms in the context of the right to privacy.

1 *Derogations*

According to Article 4(1) of the ICCPR in times of officially proclaimed public emergency which threatens the life of the nation, a State party to the Covenant may derogate from some of its obligations[67] which includes Article 17.[68] States can do so by adopting derogating measures, but these must be of an exceptional and temporary nature. Moreover, prior to a State invoking Article 4 a number of conditions must be met.[69] First, the situation has to amount to a public emergency, which threatens the life of the nation.[70] Although not every disturbance or catastrophe qualifies

65 Wall Advisory Opinion, *supra* note 37, ¶¶ 107–13.
66 General Comment 31, *supra* note 42, ¶ 10; *Al-Skeini*, *supra* note 46, ¶ 131.
67 ICCPR, *supra* note 10, art. 4(1).
68 *Id.* art. 4(1). However, art 4(2) lists a number of non-derogable rights.
69 *See* U.N. Human Rights Committee, CCPR General Comment No 29: Article 4: Derogations During A State of Emergency, U.N. Doc. CCPR/C/21/Rev.1/Add.11. (Aug. 31, 2001) [hereinafter General Comment 29].
70 ICCPR, *supra* note 10, art. 4(1).

as a public emergency, an international armed conflict falls within the meaning of "public emergency" stipulated in Article 4(1) and consequently gives States the right to derogate from certain human rights.[71] Secondly, a relevant government organ must officially proclaim a state of emergency.[72] Such prior pronouncement is a technical pre-requisite for the application of Article 4, as without it any derogation from the Covenant's rights will constitute a violation of international law.[73] Further, the language of Article 4(1) makes an explicit reference to the principle of proportionality, stating that the Covenant rights may be derogated from only "to the extent strictly required by the exigencies of the situation".[74] This provision represents the most important limitation on permissible derogation measures and requires that "the degree of interference and the scope of the measure must stand in a reasonable relation to what is actually necessary to combat an emergency threatening the life of the nation".[75] Whether or not States comply with the principle of proportionality when taking measures to derogate is subject to review by the HRC.[76] In addition, Article 4(3) requires State parties to immediately inform the other State parties through the UN Secretary-General of the provision(s) it has derogated from and the reasons for such measures.[77] The duty of notification is essential, as not only does it enable the HRC to discharge its functions when assessing whether the measures taken by the State were strictly required by the exigencies of the situation, but it also permits other State parties to monitor compliance with the provisions of the Covenant.[78] Thus far, there appears to be not a single country that has taken measures to derogate from Article 17 specifically on the grounds of the existence of, or the involvement in an armed conflict.

Unlike Article 4 of the ICCPR, Article 15 of the ECHR allows States to derogate from their Convention obligations not only "during public emergencies threatening the life of the nation", but also in the time of war.[79] However, as in the case of Article 4 of the ICCPR by virtue of Article 15(2) of the ECHR, States may derogate from Article 8, but must meet both

71 General Comment 29, *supra* note 69, ¶ 3.
72 *Id.* ¶ 2.
73 Nowak's Commentary, *supra* note 20, ¶ 17.
74 ICCPR, *supra* note 10, art. 4(1)
75 Nowak's Commentary, *supra* note 20, ¶ 26.
76 ICCPR, *supra* note 10, art. 40(2).
77 *Id.* art. 4(3); General Comment 29, *supra* note 69, ¶ 17.
78 General Comment 29, *supra* note 69, ¶ 17.
79 Lawless v. Ireland (no. 3) 332/57 Eur. Ct. H.R. 1961 ¶ 28.

the substantive[80] and the procedural[81] requirements set forth in Article 15(1) and (3) respectively. In the context of armed conflicts, the ECtHR considered the issue of derogation from Article 5 of the ECHR (right to liberty and security) in *Hassan v. United Kingdom*,[82] but there seem to be no specific instances thus far of States derogating from Article 8 obligations on the grounds of war or similar public emergency.

2 *Permissible Limitations*

States may be justified in limiting non-absolute rights on the basis of proscribed purposes, such as national security; public order, health, safety and morals; together with the protection of rights and freedoms of others.[83] Permissible limitations are subject to two conditions. First, the limitation must be proscribed by domestic law in that it has to have a clear legal basis.[84] This means that the law authorising the limitation of the given right must be publicly accessible, sufficiently precise and cannot confer unfettered discretion on those in charge of its execution.[85] Secondly, it must pursue a legitimate aim,[86] be reasonable, necessary and proportionate.[87] Thus, the restriction has to be necessary to achieve a legitimate objective, be rationally connected to attaining that purpose and be no more restrictive than required to do so.

As already observed, governments rarely choose to derogate from the obligations to protect the right to privacy, preferring instead to rely on permissible limitations clauses.[88] Recent decades have attested to a discernible trend in the practice of States restricting this right on the

80 ECHR, *supra* note 11, art. 15(1) stipulates three conditions, namely that: (1) there must be a public emergency threatening the life of the nation; (2) the measure taken in response to it must be strictly required by the exigencies of the situation; and (3) the measures taken must be in compliance with the Contracting Party's other obligations under international law.

81 *Id.* art. 15(3) requires that there is some formal or public act of derogation and that notice of derogation, measures adopted in consequence of it and of ending the derogation, is communicated to the Secretary-General of the Council of Europe.

82 Hassan v. United Kingdom (GC) 29750/09 Eur. Ct. H.R. 2014.

83 *See also* ICCPR, *supra* note 10, arts. 12(3), 18(3), 19(3), 21, 22; ECHR, *supra* note 11, arts. 9, 10, 11.

84 General Comment 16, *supra* note 19, ¶ 3.

85 *See also* General Comment 16, *supra* note 19, ¶ 8; U.N. Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); U.N. Human Rights Committee, Concluding Observations, Switzerland, ¶ 46, U.N. Doc. CCPR/C/CHE/CO/4 (July 27, 2017); Malone v. United Kingdom 8691/79 Eur.Ct.H.R. 1984; Zakharov v. Russia [GC] 47143/06, ¶ 228 Eur.Ct.H.R. 2015 (*Zakharov*); Szabó v. Hungary, ¶ 89, 48725/17 Eur. Ct. H.R. 2017 (*Szabó*).

86 *See* ICCPR, *supra* note 10, arts. 12(3), 18(3), 21 and 22(1); ECHR, *supra* note 11, art. 8(2); Martin Scheinin (Special Rapporteur), *Report on the Promotion and Protection of Human Rights while Countering Terrorism*, ¶¶ 17–18, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); *Zakharov*, ¶ 237.

87 *See also* U.N. Human Rights Committee, General Comment No. 27: Article 27 (Freedom of Movement), ¶¶ 14–15, U.N. Doc. CCPR/2/21/Rev1/Add9 (Nov. 2, 1999); S and Mapper v. United Kingdom, ¶ 118, 30562/04 Eur. Ct. H.R. (Dec. 4, 2008); *Zakharov*; *Szabó*; C-311/18 Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems, 2020, ¶ 185 ECLI:EU:C:2020:559.

88 U.N. Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, ¶ 15, U.N. Doc. A/HRC/27/37 (June 30, 2014) (A/HRC/27/37).

basis of new, or amended legislation that allows for far reaching State surveillance (such as bulk collection of communications' content and metadata) to facilitate fighting serious crime and cross-border terrorism. A case in point is the UK Investigatory Powers Act 2016;[89] the French Intelligence Act 2015;[90] and the Swedish Signals Intelligence Act 2016.[91] There are a number of reasons as to why the permissible limitations mechanism is preferable to derogations. First, States may find it difficult to show that the circumstances in question *de facto* threaten the life of the nation, as not every volatile situation necessarily reaches the threshold of an armed conflict within the meaning of common Article 2(1) to the Geneva Conventions. Second, permissible limitations are perceived as giving States sufficient leeway to achˇieve effective emergency responses, without having to give formal notification, or indeed provide reasons as to why they seek to do so and when the derogation would end. In addition, the limitations procedure seems to be more permissible in relation to the proportionality criteria which is common to the derogation and limitations powers. Under Article 4 of the ICCPR this must be justified by the exigencies of the situation, which is "a requirement that relates to the duration, geographical coverage and material scope of the state of emergency and any measures of derogation resorted to because of the emergency".[92] Furthermore, States must provide careful justification not only for their decision to proclaim a state of emergency, but also for any specific measure based on such a proclamation.[93] This can be contrasted with the interpretation of the proportionality criteria for the purposes of permissible limitations particularly in the context of the ECtHR case law addressing foreign surveillance of communications. The Strasbourg Court has long recognized that States face a difficult task of balancing national security and human rights, thus granting them a wide margin of discretion in regard to the implementation of security measures.[94] Finally, in a situation of armed conflict, States likely place little weight on their duty to respect and protect the right to privacy, as the requirements to adhere to other international law obligations, predominantly those set out by the rules of *jus in bello,* are probably considered as more pressing.

89 Investigatory Powers Act c. 25 2016.
90 French Intelligence Act (Law 2015-912) 2015.
91 Swedish Signals Intelligence Act 2016.
92 General Comment 29, *supra* note 69, ¶ 4.
93 *Id.* ¶ 5.
94 *See* Weber and Saravia v. Germany 54934/00 Eur. Ct. H.R. 2006; Liberty and Others v. United Kingdom 58234/00 Eur. Ct. H.R. 2008; Centrum För Rättvisa v. Sweden [GC] 3552/08 Eur. Ct. H.R. 2021; Big Brother Watch and Others v. United Kingdom 58170/13; 62322/14; 2460/15 Eur. Ct. H.R. 2021 (*Big Brother Watch*).

Equally, they might disregard the need for a formal derogation from privacy rights or even not countenance that they are bound by privacy and data protection obligations.

Bearing this in mind, the next section addresses the question of whether the right to privacy set out in international treaties applies in IAC and if so, how can they provide the normative foundations for States' drone surveillance operations.

III
THE RIGHT TO PRIVACY AND PROLONGED DRONE SURVEILLANCE IN ARMED CONFLICT — THE IHRL/IHL NEXUS

Privacy is not defined in international human rights treaties, but in essence it is "the presumption that individuals should have an area of autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals".[95] IHRL expressly recognizes privacy as a fundamental right and a rule of customary international law. A dense body of law and opinion has recently been developed at the UN and European levels pertaining to the right to privacy as a result of States' mass surveillance of digital communications, but the resultant courts' interpretation appears to be rather obfuscated. Thus, the UN human rights bodies and mandate holders acknowledge arbitrary interference and violation of this right, chiefly because bulk acquisition and retention of communications is seen as inherently disproportionate.[96] In contrast, the ECtHR has taken a more permissive stance, holding that such methods of intelligence gathering are an indispensable tool for States to safeguard national security, when that is undertaken in accordance with adequate safeguards and oversights mechanisms, which the Court's Grand Chamber set out in 2021 in *Big Brother Watch v. UK.*[97] Drone surveillance in situations of armed conflict is

95 A/HRC/25/59, *supra* note 6, ¶ 28.
96 *See* U N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/68/167 (Jan. 21, 2014); U.N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/69/166 (Feb. 10, 2015); U.N. General Assembly Resolution, The Right to Privacy in the Digital Age, U.N. Doc. A/Res/71/199 (Dec. 19, 2016).
97 *Big Brother Watch*, *supra* note 94.

equally if not more intrusive than bulk interception of digital communications in peacetime, as it directly encroaches on the privacy of home and family life, as well as data protection rights. With the increase in these activities and their almost certain spill over to situations which cannot be readily pigeonholed as an armed conflict in legal terms, it becomes imperative that militaries become mindful that privacy and data protection are legally binding rights also during hostilities in the absence of States' expressly derogating from them. The next section explores how this can be achieved.

A THE DUTY OF CONSTANT CARE AND DRONE SURVEILLANCE

The conceptual bridging of the IHRL/IHL gap in this context is the principle of constant care set out in Article 57 (1) of the AP I discussed above. As it likely applies to all military operations, it should arguably be extended to intelligence gathering by drones, placing a duty of care on military leaders to respect the privacy and data protection rights of civilian populations in their decision-making cycle. It is submitted that such a progressive interpretation of Article 57(1) could fill in the normative lacuna left by the IHL for at least five reasons.

First, it has been acknowledged that the constant care principle requires the commander to bear in mind the effects on the civilian population of what he or she is planning to do and take steps to reduce those effects as much as possible. This is recognized, *inter alia*, by the drafters of the *Tallinn Manual 2.0* in the context of States' cyber operations. To this end, the commentary to Rule 114 states that "in cyber operations, the duty of care requires commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon".[98] This supports a contention that Article 57(1) should capture all military activities associated with combat, including intelligence collection. Such an expansive interpretation of this provision is also garnering academic support. Thus, Asaf Lubin advocates that in the digital age, Article 57(1) should apply to "all informational operations necessary to support military activities", such as intelligence collection

98 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Michael N. Schmitt & Liis Vihul eds., Cambridge University Press 2017), Rule 114, ¶ 4 [hereinafter Tallinn Manual 2.0].

and broader data collection by any actor, including private contractors and civilian intelligence agencies, provided the necessary nexus exists between gathering, storing, processing and sharing and advancing combat.[99] Based on this reasoning, obtaining data from drone surveillance conducted with the view of combat throughout the entire spectrum of military operations should conceivably fall within the ambit of Article 57(1). This will place the necessity of amassing vast amounts of drone data within commanders' contemplation and entail a proportionality assessment. Thus, in implementing drone surveillance measures, militaries will be under an obligation to strike a balance between attaining the legitimate aim of target identification and safeguarding individuals' privacy rights, by imposing geographical and temporal limits on the surveillance and the amount of the collected data.

Second, the duty of care is constant which means it is of continuous nature and therefore does not have time limitations. The word "constant" according to the *Tallinn Manual 2.0* denotes that:

> the duty to take care to protect civilians and civilian objects is of a continuing nature throughout cyber operations; all those involved in the operation must discharge the duty. The law admits of no situation in which, or time when, individuals involved in the planning and execution process may ignore the effects of their operations on civilians or civilian objects. In the cyber context, this requires situational awareness at all times, not merely during the preparatory stage of an operation.[100]

It follows that duty of constant care likely arises at all stages of armed conflict — that is, before, during and after active hostilities.[101] Based on this reading, all information operations, including drone surveillance of civilians, irrespective of the stage of hostilities at which they are conducted, must be subject to this obligation.

Third, it is submitted that Article 57(1) should be interpreted in such a way as to recognize the type of harm inherent in prolonged surveillance, including continuous fear and trauma associated with a possible drone attack, interference with privacy and data protection implications. Admittedly the wording of Article 57(1) does not refer directly to harm,

99 Asaf Lubin, *The Duty of Constant Care and Data Protection in War*, *in* BIG DATA AND ARMED CONFLICT: LEGAL ISSUES ABOVE AND BELOW THE ARMED CONFLICT THRESHOLD 10 (Laura A. Dickinson and Edward Berg eds., Oxford University Press, forthcoming, 2022).

100 TALLINN MANUAL 2.0, *supra* note 98, Rule 114, ¶ 5.

101 *See* Lubin, *supra* note 99, at 11.

stating merely that civilians and civilian objects must be spared. Article 57(2) then goes on to refer to "attacks" setting out a list of precautions that must be taken. This indicates that the drafters of AP I contemplated that the harm to civilian population is of a physical nature, such as death, personal injury and damage to civilian objects. However, as recognized by Lubin, in the information age there is a bundle of individual rights that have *digital* manifestation — that is, privacy, anonymity, access to information, online freedom of expression, digital autonomy and dignity, together with intellectual property.[102] As the right to privacy extends to the privacy of home and family life, individuals deserve protection against the harm caused by unrestrained drone surveillance by foreign militaries in particular because the strategic planning of militaries is increasingly swaying towards relying on technological tools such as machine learning and AI to enhance their military capabilities and decision making processes.[103] For this reason the duty of constant care should extend beyond physical harm and apply to protecting civilians from being subject to arbitrary interference with all aspects of their privacy, including the right to have a private sphere, that allows for autonomy and dignity.

Fourth, the duty of constant care should necessitate the adherence to the minimum data protection standards. This entails the protection of the data gathered in pursuance of intelligence operations from unrestricted collection, retention, processing and sharing. Strong support for such a progressive interpretation of Article 57(1) has been advanced in academic writing. For example, Lubin postulates that without any specific IHL rules in place, the duty of constant care as a data protection rule "stands as the only possible lighthouse that could guide militaries in discharging their duty".[104] In practical terms this would require commanders to take reasonable steps to reduce where feasible the negative effects on civilians of the information operations, through transplanting some of the fundamental principles of data protection such as that of fair, transparent and lawful processing onto the military theatre of operations.[105] To this end, fairness dictates that the collection and further processing of personal data must be carried out in such a way as not to interfere unreasonably

102 *Id.* at 14.

103 *See also* Stew Magnuson, *DoD Making Big Push to Catch up on Artificial Intelligence*, NATIONAL DEFENSE MAGAZINE (Mar. 16, 2017), https://www.nationaldefensemagazine.org/articles/2017/6/13/dod-making-big-push-to-catch-up-on-artificial-intelligence; Cade Metz, *As China Marchers Forward on A.I. the White House is Silent*, NEW YORK TIMES (Feb. 12, 2018), https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html.

104 Lubin, *supra* note 99, at 16.

105 *See also* Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, Jan. 28 1981, ETS 108 art. 5(a); General Data Protection Regulation, Apr. 27, 2016, OJ L 119, (GDPR) art. 5(1)(a).

with data subjects' privacy-related interests. This connotes proportionality in the balancing of interests of data subjects and data controllers and means that personal data must be "relevant" and "not excessive" in relation to the purpose for which it is processed.[106] Furthermore, the processing of personal data must be transparent for the data subjects, which means that data must not be processed surreptitiously, whilst data subjects must not be deceived as to the nature and purpose of the processing.[107] The principle of lawfulness requires that data processing may only be carried out pursuant to legal basis, which must specify the circumstances where such processing may be lawfully conducted.[108] As drone surveillance falls within military intelligence operations, the legality, fairness and transparency principles should apply, necessitating that the processing of data obtained through such methods complies with these basic requirements.

The prerequisite that surveillance be conducted on the basis of domestic law is also a fundamental principle of the right to privacy set out in, *inter alia,* Article 17 of the ICCPR and Article 8 of the ECHR. In interpreting this basic condition, the HRC stated that "interference authorised by States can only take place on the basis of the law, which itself must comply with the provisions, aims and objectives of the Covenant".[109] Moreover, in accordance with the principle of foreseeability, the law must be sufficiently clear to give an adequate indication of the circumstances and conditions empowering public authorities to resort to surveillance. In accordance with this stipulation, the ECtHR in the context of State interception of foreign communications developed minimum procedural standards in the 2006 case of *Weber v. Germany*[110] which laid down basic guarantees that a surveillance law must meet to be compliant with the ECHR. These safeguards have since been widened by the Grand Chamber of the ECtHR in *Big Brother Watch* v. *United Kingdom* and require the domestic legal frameworks to stipulate: (1) the grounds on which bulk interception may be authorised; (2) the circumstances in which an individual's communications may be intercepted; (3) the procedures to be followed for granting authorisation; (4) the procedures to be followed for selecting, examining and using intercepted material; (5) the precautions to be taken when communicating the material to other parties; (6) the limits on the duration of the interception, the storage of the intercept material and

106 Lee A. Bygrave, Data Privacy Law (Oxford University Press 2014), 148.
107 *Id.* at 147.
108 *See also* GDPR, art. 6(3).
109 General Comment 16, *supra* note 19, ¶ 3.
110 *See* Weber and Saravia v. Germany 54934/00 Eur. Ct. H.R. 2006, ¶ 95.

the circumstances in which such material must be erased or destroyed; (7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and (8) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[111] Drone surveillance—seen in the light of the principle of constant care—should be underpinned by the positive and continuous obligation of risk mitigation and harm prevention. This requires establishing minimum procedural safeguards which in turn entails adopting legislation delineating the circumstances in which such surveillance may be lawfully conducted. In practical terms, a starting point might be that the carrying out of drone surveillance is assessed on the basis of the aforementioned eight criteria and subject to *ex post* review of the reasons for the retention, sharing and other utilisation of drone data.

What can be concluded from the above analysis is a need for a two-pronged approach to prolonged drone surveillance in war zones. The first is to develop clear standards of when drones may be present in a given area setting out temporal and geographical limitations, together with the minimum procedural standards for conducting such surveillance. The second is to develop rules that address the processing, retention and sharing of the obtained data, imposing minimum data protection standards encompassing the concepts of legality, fairness and transparency. The rationale for this is the principle of constant care which must be interpreted to reflect the general aims of the Geneva Conventions and the Additional Protocols, namely to spare civilians from harm in times of war and to provide minimum protection to the victims of armed conflict by setting standards of humane treatment.

CONCLUSION

This chapter analyzed the issues concerning States' deployment of drones in wartime and the problems this creates outside of the usually discussed breaches of *jus ad bellum*, *jus in bello* and the right to life under international human rights law. Having demonstrated an individual and

111 *Big Brother Watch*, *supra* note 94, ¶ 361.

collective surge in the use of surveillance drones both in the context of international armed conflict and outside it, this chapter argued for a dualistic approach to these practices. The first necessitates developing procedural safeguards for States' deployment of surveillance drones. To assist in this, the set of guarantees stipulated by the ECtHR in the 2021 *Big Brother Watch* decision may be a useful benchmark to guide decisions made by militaries regarding the use of UAVs to obtain intelligence. This is due to the apparent similarities between these two methods of data acquisition, including their indiscriminate nature and the vast amounts of material obtained. The second is establishing data protection standards in line with the principles of legality, fairness, transparency and proportionality. Underpinning this contention is the principle of constant care which places a duty on military commanders to protect civilians throughout the entirety of military operations and means that those involved in the planning and execution process must not ignore the effects of their operations on civilians. In the digital age, this demands consideration be given to privacy and data protection rights of non-combatants in armed conflicts.

Chapter 9

The Use of Cable Infrastructure for Intelligence Collection During Armed Conflict: Legality and Limits

Tara Davenport[1]

INTRODUCTION

Since the first submarine telegraph cable was laid from Dover to Calais in 1850, submarine fiber optic cables (the successor of submarine telegraph cables) have emerged as one of the most important innovations of our time. Ninety-nine percent of the world's telecommunications are transmitted through fiber optic cables.[2] As of 2021, approximately 464 submarine cable systems transmit dozens of Terabytes of data per second, crisscrossing vast expanses of the seabed and traversing different jurisdictions until they reach a cable landing station onshore.[3] These

1 Assistant Professor at the Faculty of Law, National University of Singapore (NUS) and a Senior Research Fellow at the Centre for International Law (CIL) at NUS.

2 Douglas Main, *Undersea Cables Transport 99% of International Data*, NEWSWEEK, Apr. 2, 2015, https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072.

3 Douglas R. Burnett, *Submarine Cable Security and International Law*, 97 INT'L L. STUD. 1659, 1668 (2021).

submarine cables facilitate a wide variety of services that we take for granted, from phone and internet banking to email and social media. They have unsurprisingly been described as "critical communications infrastructure" and as "vitally important to the global economy and the national security of all States."[4] While fiber optic cables are used primarily for the transmission of communications data, they are also utilized for other purposes. For example, militaries depend on fiber optic cables for both defense and warfare purposes;[5] oil and gas industries utilize them for platforms connectivity;[6] and the placement of scientific sensors on such cables facilitates oceanographic data collection.[7]

This chapter focuses on one specific use of cable infrastructure (consisting of both submarine fiber optic cables laid on the seabed and cable landing stations), namely, its use by States for intelligence collection during armed conflict, which can be crucial in facilitating the success of military operations both defensive and offensive.[8] For example, during World War I, Britain cut all but one of Germany's undersea cables and tapped the remaining one, which enabled the British to read any message sent through it, including the Zimmerman telegram, which nudged a reluctant United States (US) into the war.[9] In peacetime, the ubiquity of cable infrastructure has provided opportunities for States to conduct mass surveillance ostensibly for national security purposes.[10] In 2013, Edward Snowden disclosed that the national security agencies of both the US (National Security Agency or NSA) and the United Kingdom (UK) (GCHQ or Government Communications Headquarters) had been "tapping directly into the Internet's backbone," namely fiber optic cables, to gather vast amounts of data concerning multiple actors including State actors, officials of international organizations, religious leaders, corporations,

4 UN General Assembly Resolution 65/37 ¶ 121 (Dec. 7, 2010).
5 For example, the US Department of Defense Global Information Grid, which is a "globally, interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel." Global Information Grid, National Security Agency, https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-04-858/html/GAOREPORTS-GAO-04-858.htm (last visited Dec. 26, 2021).
6 Wayne F. Nielsen & Tara Davenport, *Submarine Cables and Offshore Energy in Submarine Cables*, *in* SUBMARINE CABLES: HANDBOOK ON LAW AND POLICY, 351 (Douglas Burnett et al. eds., 2014).
7 Lionel Carter & Alfred H.A. Soons, *Marine Scientific Research Cables in Submarine Cables*, *in* BURNETT et. al., *supra* note 6, 323
8 Marco Longobardo, *(New) Cyber Exploitation and (Old) International Humanitarian Law*, 77 ZAORV 809, 812 (2017).
9 *From Australia to Zimmerman: A Brief History of Cable Telegraphy during World War One*, *in* INNOVATING IN COMBAT: TELECOMMUNICATIONS AND INTELLECTUAL PROPERTY IN THE FIRST WORLD WAR, http://blogs.mhs.ox.ac.uk/innovatingincombat/files/2013/03/Innovating-in-Combat-educational-resources-telegraph-cable-draft-1.pdf.
10 ELIZA WATT, STATE SPONSORED CYBER SURVEILLANCE: THE RIGHT TO PRIVACY OF COMMUNICATIONS AND INTERNATIONAL LAW 74 (2021).

non-governmental organizations, and suspected terrorists.[11] In 2015, reports of Russian submarines and spy ships patrolling areas near submarine cables in US waters prompted concerns from American and NATO security forces.[12] Most recently, the Trump administration called for the boycott of Chinese cable equipment manufacturers and telecommunications operators due to concerns that China is using cables to collect intelligence.[13]

The methods used to tap cable infrastructure for intelligence collection are shrouded in mystery and the prevalence of this activity cannot be determined with certainty.[14] First, it is said that tapping can be done by "inserting backdoors during the cable manufacturing process."[15] Reportedly, any company that builds cables could potentially be requested by a government to build backdoors into the equipment before deployment.[16] This possibility prompted US concerns about Huawei's involvement in a variety of cable building projects.[17] Second, it is speculated that intercept probes can be installed at cable landing stations that capture the fiber optic light and make a copy of it.[18] This may not alert an operator that tapping has occurred as there is no service interruption.[19] This was the method that was reportedly used by the NSA and GCHQ.[20] The third method, according to some reports, is the direct tapping of submarine cables on the seabed, which involves the use of specially equipped submarines or underwater unmanned vehicles which would lift the cable and install a device to collect the data that passes through them.[21] Such physical tapping on the seabed is said to be necessary when cable-landing stations

11 RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 4 (2018).
12 David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables are Too Close for US Comfort*, N. Y. TIMES, Oct. 25, 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html (last visited Apr. 4, 2022).
13 Laurie Clarke, *Geopolitical tensions over subsea cables may have big implications for internet infrastructure*, TECH MONITOR, Aug. 19, 2021, https://techmonitor.ai/policy/geopolitics-of-submarine-cables-us-china-facebook (last visited Dec. 26, 2021).
14 Jason Petty, *How Hackers of Submarine Cables May be Held Liable under the Law of the Sea*, 22 (1) CHI. J. INT'L LAW 260, 266.
15 Pierre Morcos & Collin Wall, *Invisible and Vital: Undersea Cables and Transatlantic Security*, CSIS COMMENTARY, 11 June 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security (last visited Dec. 26, 2021)
16 Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, ATLANTIC COUNCIL REPORT, Sept. 13, 2021, 15, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/, (last visited Apr. 4, 2021).
17 *Id*.
18 Petty, *supra* note 14, at 266; Morcos & Wall, *supra* note 15.
19 *Id.*
20 Ewen MacAskill, Julian Borger, Nick Hopkins & James Ball, *GCHQ taps fibre-optic cables for secret access to world's communications*, GUARDIAN, Jun 21, 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last visited Dec. 21, 2021).
21 The submarine USS Jimmy Carter was reportedly equipped with the ability to tap undersea cables and eavesdrop on communications passing through them: see *New Nuclear Sub is said to Have Special Eavesdropping Ability*, N. Y. TIMES, Feb. 20, 2005.

are on foreign soil.[22] On the other hand, it has also been argued that this method is "so technically challenging that little is publicly known about specific methods and which countries have these capabilities."[23] Challenges include "identifying the fiber of interest, copying the data, decrypting it, and evading monitoring systems that detect even minor changes in traffic or physical interference."[24] The methods discussed above involve both close and remote access—probes (for example) which are installed usually require some human intervention, but the appropriated information is usually transmitted back to the operator via the Internet. It can also occur prior to armed conflict or during armed conflict. After data has been intercepted from cable infrastructure, it is retained and specific selectors are applied and examined by analysts, after which the "final product" is used, including the sharing of data with third parties.[25]

This chapter will explore gaps and uncertainties in the international law governing the utilization of cable infrastructure for intelligence collection in armed conflict. Given that such activity can be described as a type of cyber operation,[26] this chapter will examine the law applicable during armed conflict (Part I) as well as other fields of law that are traditionally applicable during peacetime, such as the law of the sea and international human rights law, on the basis that these regimes may also be applicable during armed conflict (Part II). While the secretive nature of cyber operations obfuscates attempts to delineate applicable norms, this chapter will argue that the use of cable infrastructure for intelligence collection in armed conflict does not exist in a legal vacuum. Indeed, each field of law examined herein contains rules which can be applied, albeit uneasily, to this activity and, more importantly, demonstrates that it is not an untrammeled entitlement of States but one that is subject to certain limits that are increasingly converging.

22 *Id*.

23 Jonathan E. Hillman, *Securing the Subsea Network: A Primer for Policy Makers,* CSIS RECONNECTING ASIA PROJECT, Mar. 9, 2021, 10, https://www.csis.org/analysis/securing-subsea-network-primer-policymakers (last visited Apr. 4, 2022).

24 *Id*.

25 Big Brother Watch and Others v. United Kingdom, App no 58170/13, ¶ 272 (Sept. 13, 2018) [BBW v. UK], ¶ 325.

26 While there is no general consensus on a definition of cyber operations, the 2016 US Military Manual's definition provides a good starting point: operations that involve the "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyber space." They "use cyber capabilities, such as computers, software tools, or networks" and "have a primary purpose of achieving objectives or effects in or through cyberspace." US DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL (Updated Dec. 2016), 16.1.2. See also the definition in TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 258 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

A few qualifications are in order. First, this chapter does not engage with the question of *when* an armed conflict arises (and the debates that accompany this question).[27] It proceeds on the basis of a broad definition of armed conflict as a "resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State," [28] thus encompassing both international and non-international armed conflict. Second, while this chapter covers non-international armed conflict which involves non-State actors, its analysis is confined to activities that can be attributed to a State, bearing in mind that States are most likely to have the financial and technological resources necessary to engage in such tapping.[29] Third, this chapter is concerned with intelligence collection that occurs during armed conflict, although it will examine the extent to which certain peacetime regimes may be applicable to this activity. Fourth, while some cable infrastructure is exclusively used for military purposes by the military,[30] this chapter limits its analysis to dual-use cable infrastructure that has both civilian and military uses.[31] Fifth, this chapter focuses on the use of cable infrastructure to gain information without affecting the functionality of the system or deleting the data transiting therein, and will only address to the extent relevant the applicable law when intelligence collection leads to damage to the cable.

27 *See, e.g.*, Dapo Akande, *Classification of Armed Conflicts*, *in* THE OXFORD GUIDE TO INTERNATIONAL HUMANITARIAN LAW 29 (Ben Saul & Dapo Akande eds., 2020).

28 Prosecutor v. Tadic (Decision on Defence Motion for Interlocutory Appeal on Jurisdiction) IT-94-1-AR72 (2 October 1995), ¶ 63. *See also* International Committee on the Red Cross (ICRC), COMMENTARY ON THE FIRST GENEVA CONVENTION, CONVENTION I FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND THE SICK IN THE ARMED FORCES IN THE FIELD (CUP, 2016), at 80, ¶ 219.

29 DJ Pangburn, *Wiretapping Undersea Fiber Optic Cables is Just a Matter of Money*, VICE, Jul. 23, 2013, https://www.vice.com/en/article/wnnmv9/undersea-cable-surveillance-is-easy-its-just-a-matter-of-money (last visited Apr. 4, 2021).

30 Ashley Roach, *Military Cables*, *in* BURNETT et. al., *supra* note 6, 323.

31 For example, for the United States, a significant percentage of military communications are transmitted over civilian networks. *See* HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR 187 (2012).

I
THE LAWS APPLICABLE IN ARMED CONFLICT

A LEGALITY OF THE USE OF CABLE INFRASTRUCTURE FOR INTELLIGENCE COLLECTION

International humanitarian law (IHL) and the law of neutrality are the most salient regarding the use of cable infrastructure for intelligence collection in armed conflict, but neither provides a complete answer on the legality and limits of this activity. Intelligence collection has traditionally been deemed necessary to meet military objectives in armed conflict. The 1863 Lieber Code recognized that "deception in war is admitted as a just and necessary means of hostility, and is consistent with honourable warfare."[32] Under Article 24 of the 1907 Hague Regulations on the Laws and Customs of War on Land (Hague Regulations), "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[33] Article 37(2) of the 1977 Additional Protocol I of the 1949 Geneva Convention on the Protection of Victims of International Armed Conflict (AP I) similarly recognizes that "ruses of war are not prohibited."[34] Moreover, an attacking State is compelled to gather certain information in order to verify the nature of the object of the attack and its consequences, and intelligence collection is necessary for the State to implement the applicable principles of distinction and proportionality.[35] Accordingly, in contrast to the uncertainty that characterizes the legality of intelligence collection (and its different permutations) in peacetime, IHL views intelligence collection in armed conflict undertaken for the success of a military operation as lawful.[36]

32 Francis Lieber, Instructions for the Government of the Armies of the United States in the Field, art. 101, (Washington, Apr. 24, 1863) [hereinafter Lieber Code].

33 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 Jul. 29, 1899, 32 Stat. 1803, 187 Consol. T.S. 456 [hereinafter HR].

34 Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, adopted Jun. 8, 1977, U.N. Doc. A.32/144/Annex II (1977) [hereinafter AP I].

35 *Id.* art. 57 (2) (a); Longobardo, *supra* note 8, at 813.

36 Longobardo, *supra* note 8, at 813; JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 123 et seq. (Martinus Nijhoff 1995). The peacetime practice of intelligence collection is more contested, with different views being put forth that international law neither prohibits nor allows peacetime intelligence collection, that it is legal, that it is illegal, or that it is subject to certain limits. For a sampling of these different views, see, for example, Simon Chesterman, *The Spy Who Came in From the Cold War: Intelligence and International Law*, 27 (4) MICH. J. INT'L L 1071 (2006); Asaf Lubin,

However, the *means* by which intelligence collection is undertaken is not extensively regulated. IHL only explicitly regulates one specific permutation of intelligence collection, namely espionage. Under IHL, either civilians or members of the armed forces commit espionage if they (1) obtain or endeavor to obtain information relevant for the conduct of armed conflict and transmit this information to one of the parties to the conflict;[37] (2) act clandestinely or under false pretenses;[38] and (3) carry out such activities in a territory controlled by a belligerent or adverse party.[39] If spies are captured, they are not entitled to prisoner of war status unless they return to their armed forces before being captured and are subject to the domestic criminal law of the State that captures them.[40] Chesterman observes, "spies… bear personal liability for their acts but are not war criminals as such and do not engage the international responsibility of the State that sends them."[41] IHL has also evolved to recognize certain basic guarantees in the treatment of spies.[42]

The use of cable infrastructure for intelligence collection does not fall neatly within IHL conceptions of espionage. It is also an uneasy fit with more contemporary permutations of espionage, namely, cyber espionage. While there is no universally accepted definition of cyber espionage in times of armed conflict, the Tallinn Manual 2.0 provides a useful starting point subject to the caveat that it does not necessarily reflect existing international law.[43] It defines cyber espionage in armed conflict as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party."[44] The information must be gathered on behalf of a party to the conflict.[45] The Tallinn Manual 2.0 further notes that "cyber espionage and other forms of intelligence gathering do not *per se* violate the law of armed conflict."[46]

The Liberty to Spy, 61 HARV. INT'L L. J. 185 (2020); BUCHAN, *supra* note 11, at 4–8.

37 Lieber Code, *supra* note 32, art. 88; HR, *supra* note 33, art 29; AP I, *supra* note 34, art. 46 (2).

38 Lieber Code, *supra* note 32, art. 88; HR, *supra* note 33, art. 29; AP I, *supra* note 34.

39 Lieber Code, *supra* note 32, art. 83; HR, *supra* note 33, art. 29; AP I, *supra* note 34.

40 Chesterman, *supra* note 36, at 1081.

41 *Id*.

42 *See* Longobardo, *supra* note 8, at 819–21.

43 The Tallinn Manuals were prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defense Center of Excellence. TALLINN MANUAL 2.0, issued in 2017, updated the first Tallinn Manual to cover cyber operations in both peacetime and times of armed conflict. There is debate on how authoritative the TALLINN MANUAL 2.0 is and whether "it is reflective of existing international law, or merely the articulation of the views of an international group of experts on how international law should be applied to cyberoperations." *See* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112:4 AM. J. INT'L L 583, 589 (2018).

44 TALLINN MANUAL 2.0, *supra* note 26, rule 89, at 409.

45 *Id.* at 411, ¶ 10.

46 *Id.* at 410, ¶ 5.

Prima facie, if one considers the tapping of cable infrastructure to be cyber espionage and analogizes it to espionage, it would be permitted in armed conflict (provided, of course, that the intelligence collected is of military value or has a nexus to the military operations). Yet, both IHL and the Tallinn Manual's conception of cyber espionage is limited to situations in which the individual concerned engages in cyber espionage while in "enemy-controlled territory." The Tallinn Manual 2.0 states, "[c]yber espionage that is performed from outside enemy-controlled territory is not subject to this Rule" and "it does not encompass espionage conducted remotely by individuals from beyond enemy territory, even though the exfiltration may take place on enemy-controlled territory."[47] In other words, remotely accessed data from outside enemy-controlled territory would not be considered cyber espionage. Some scholars have suggested interpreting this requirement less restrictively so that an individual "can be considered physically present in the enemy territory since their programs infiltrate systems and networks located in that territory,"[48] although others have countered that the operator's physical presence in enemy-controlled territory is an absolute requirement under IHL, including for contemporary permutations such as cyber espionage.[49] Using cable infrastructure for intelligence collection involves both close access and remote access.[50] If close access operations occur in enemy-controlled territory during armed conflict, it can be argued that it is akin to espionage and governed by the applicable rules. It would not be considered cyber espionage if the close access operation occurs during peacetime and remote access occurs during armed conflict if one takes the position that remotely accessed data does not meet the physical presence requirement.

Moreover, questions also arise on whether the scale of intelligence collection during armed conflict impacts its characterization as cyber espionage (and hence its permissibility). For example, the use of cable infrastructure by the NSA and GCHQ is said to be better described as mass cyber surveillance rather than targeted cyber espionage.[51] Mass cyber surveillance has become a pervasive practice of States ostensibly for national security purposes and has been defined as a "state's indiscriminate monitoring and capture of digital communications, comprising their content and metadata, aimed at identifying future rather than

47 *Id.* at 411, ¶ 8.
48 Longobardo, *supra* note 8, at 823.
49 *Id.* (citing the work of Heather H. Dinniss).
50 BUCHAN, *supra* note 11, at 18–19 n. 29.
51 WATT, *supra* note 10, at 79.

investigating known threats."[52] While contemporary discussions of mass cyber surveillance have subsumed this activity within cyber espionage, Watt has highlighted important differences: targets of cyber espionage often consist of selected government organizations and entities, whereas mass cyber surveillance primarily focuses on the interception of data of entire populations; cyber espionage is sporadic and selective as opposed to the sustained and constant nature of mass cyber surveillance.[53] In principle, any tapping of cable infrastructure would necessarily involve the bulk interception of data which would only be targeted after certain selectors are applied, which would differentiate it from the targeted nature of cyber espionage. In this context some have proposed that a proportionality assessment could control whether particular surveillance operations may be deemed lawful.[54]

If espionage (and cyber espionage) is in principle permitted during armed conflict under IHL, does this extend to surveillance that indiscriminately targets civilian populations, given that mass cyber surveillance is not what was originally contemplated in IHL conceptions of espionage? The majority of the experts of the Tallinn Manual 2.0 opined that the nature of the information gathered has no bearing on the characterization of an activity as cyber espionage, provided it was gathered on behalf of a party to the conflict, while the minority said that the information must be of some military value, which would arguably preclude the type of bulk surveillance conducted by the NSA and GCHQ.[55] This is not an abstract question—the International Committee of the Red Cross (ICRC) has observed in recent conflicts that "[u]nprecedented levels of surveillance of the civilian population have caused anxiety and increasing numbers of arrests, in some instances possibly based on disinformation."[56] International human rights law has developed significant limits on mass surveillance, using the right to privacy as the foundational bulwark against such intrusions, and its applicability in armed conflict

52 *Id*.
53 *Id.* at 29.
54 Asaf Lubin, *The Dragon-Kings' Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 WASHBURN L. J. 17, 58, 73 (2018) (proposing in the context of maritime surveillance, and citing in part Kish, a proportionality assessment that takes into account the "balance of interest" between the parties, that is, whether "the injury suffered by the aggrieved States exceeds the benefit resulting for another State from the enjoyment of its own right." Lubin includes in his assessment such factors as: "the political atmosphere surrounding the operation; the aims that stand at the heart of the decision to launch the surveillance operation; the likelihood of success of the operation; and the potential risks to minimum order goals and to intrusion on coastal States' rights in the exercise of the operation.").
55 TALLINN MANUAL 2.0, *supra* note 26, at 411, ¶ 11; HPCR Manual produced by Harvard University's Humanitarian Policy and Conflict Research, rule 118.
56 ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 21 (Oct. 2019).

will be discussed below. It suffices to note that IHL does not address the bulk interception of data for mass surveillance and the rights to privacy in a meaningful manner.

B LIMITS

If intelligence collection using cable infrastructure is in principle permitted during armed conflict under the rubric of espionage, are there any limits? One may look to the law of neutrality, which does not explicitly address this activity but does have rules on the extent to which belligerents can use neutral cyber infrastructure in armed conflict.[57] Neutrality dictates that neutral territory should not be involved in the conduct of hostilities.[58] Adapting the rules of neutrality to cyber operations, the Tallinn Manual 2.0 adopts the general rule that "the exercise of belligerent rights by cyber means in neutral territory is prohibited."[59] Belligerents cannot use neutral cyber infrastructure located in neutral territory to conduct cyber operations.[60] At the same time, a neutral power is not under any obligation to forbid or restrict the use of neutral cyber infrastructure by belligerent States. If it does restrict belligerents from using such infrastructure, it must do so in a manner that is impartial to all parties to a conflict.[61] Neutral cyber infrastructure means public or private cyber infrastructure located within neutral territory, which includes civilian cyber infrastructure owned by a party to the conflict or nationals of that party, or civilian cyber infrastructure that has the nationality of a neutral State and is located outside of belligerent territory.[62]

However, applying these rules wholesale to prohibit the use of cable infrastructure for intelligence collection is not straightforward. First, the law of neutrality does not explicitly prohibit the use of neutral cyber infrastructure for espionage.[63] The Tallinn Manual 2.0 itself observes

57 For an overview of the law of neutrality, see Michael Bothe, *The Law of Neutrality*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 602 (Dieter Fleck et al. eds., 2021).

58 Hague Convention V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907 (Hague Convention V), art. 1; TALLINN MANUAL 2.0, *supra* note 26, at 553–54.

59 TALLINN MANUAL 2.0, *supra* note 26, rule 151, at 555, based on Hague Convention V, *supra* note 58, art. 3 (a), which states that "belligerents are forbidden to erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces."

60 TALLINN MANUAL 2.0, *supra* note 26, rule 151, at 556.

61 Hague Convention V, *supra* note 58, art. 8; TALLINN MANUAL 2.0, *supra* note 26, rule 151, at 556, ¶ 4.

62 TALLINN MANUAL 2.0, *supra* note 26, at 553, ¶ 2.

63 See KISH, *supra* note 36, at 125, who argues that Hague Convention V allows the belligerent use of neutral communications systems for espionage.

that the law of neutrality as adapted to cyber operations only prohibits the exercise of *belligerent rights* against neutral cyber infrastructure, but belligerent rights do not extend to espionage conducted against neutral States.[64] Second, even if the law of neutrality did apply to prohibit the use of neutral cable infrastructure for intelligence collection, in principle it would apply in the territory of a neutral State or in waters under the territorial sovereignty of a neutral State (internal waters, territorial sea, archipelagic waters).[65] Would it apply to submarine cables laid outside neutral territory (i.e., in the exclusive economic zone and high seas) but owned and operated by corporations from neutral States? The definition of neutral cyber infrastructure adopted by the Tallinn Manual 2.0 includes infrastructure that "has the nationality of a neutral State and is located outside of belligerent territory."[66] The Tallinn Manual 2.0 suggests in the context of *attacks* against neutral cyber infrastructure that neutral cyber infrastructure located on the high seas is protected by virtue of the State of the nationality's sovereignty.[67] There is a lack of clarity on whether submarine cables located in the exclusive economic zone (EEZ) and high seas but owned or operated by nationals from neutral States would be immune to tapping by belligerent States.

Third, as has been pointed out in the context of attacks on cable infrastructure, the law of neutrality is increasingly impractical to apply in today's connected world.[68] The law of neutrality was based on actions in the physical domain and in a time when communications only served the two States that were physically connected by that cable.[69] Because of the complex ownership and control of submarine cables (multiple owners and operators from different States), it would be difficult for belligerents to distinguish between cables which are owned or operated by neutral States or located within neutral territory.[70] There may be cases where such cables are owned and operated by corporations from both neutral and belligerent States. The Oslo Manual on Select Issues on Armed Conflict acknowledges this in the context of attacks against submarine pipelines/power cables and submarine communications cables, which would be equally applicable in the context of the use of cable infrastructure to conduct intelligence collection. The Oslo Manual says submarine

64 TALLINN MANUAL 2.0, *supra* note 26, at 554, ¶ 6.
65 *Id.* at 554, ¶ 5.
66 *Id.* at 553, ¶ 2.
67 *Id.* at 555, ¶ 2.
68 *See* James Kraska, *The Law of Maritime Neutrality and Submarine Cables*, EJIL: TALK!, Jul. 29, 2020, https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/.
69 *Id*.
70 *Id.*

communications cables, whether or not connecting occupied territory with neutral territory, should not be seized or destroyed even if they are serving one or more belligerent States, and belligerent States must take care to avoid damage to such cables, unless they qualify as lawful targets.[71] This is because it will only rarely be possible to determine that submarine communications cables are exclusively serving one or more belligerents, or one or more neutral States, given that today's submarine communications cables are interconnected and data packages travel along unpredictable routes.[72]

The law of neutrality is unhelpful in determining whether there are any limits to the use of cable infrastructure for intelligence collection. Do the limits of distinction, proportionality and precaution recognized by IHL in cases of attacks against cable infrastructure equally apply to utilizing cable infrastructure for intelligence collection? Cyber espionage *per se* does not fall within the concept of a cyber attack, which has been defined by the Tallinn Manual 2.0 as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[73] It has not been settled whether cyber espionage that interferes with the functionality of cable infrastructure constitutes damage or destruction and thereby constitutes an attack.[74] The majority of experts on the Tallinn Manual 2.0 opined that interference with functionality qualifies as damage if restoration requires replacement of physical components, while others took the view that any loss of usability constitutes damage that qualifies it as an attack.[75] In this regard, cable technology allows traffic to be automatically re-routed to other transoceanic cable paths in the event of damage, but that cable may still need to be repaired physically.[76] Moreover, if many cables are damaged during armed conflict, there are significant obstacles to easy restoration of traffic.[77] On this view, intelligence collection that does not affect the functionality of the system or delete the transiting data will not amount to a cyber attack. IHL governing cyber operations not amounting to attacks is less developed than IHL governing cyber operations amounting to attacks.[78] However, there is scope to argue that intelligence collection

71 Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary, rule 69, ¶ 4 (Yoram Dinstein & Arne Willy Dahl eds., 2020).
72 *Id.*
73 Tallinn Manual 2.0, *supra* note 26, rule 92, at 414.
74 *Id.* at 417, ¶ 10.
75 *Id.*
76 Burnett, *supra* note 3, at 1664.
77 *Id.* at 1664–65.
78 Laurent Gisel, Tilman Rodenhauser & Knut Dormann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations During Armed Conflicts*, 102

is a cyber operation that qualifies as a military operation and hence is subject to some limitations, albeit not the full gamut.[79]

First, there is debate on whether the principle of distinction, which stipulates that parties to the conflict should "distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives,"[80] applies to military operations (including cyber operations) not amounting to an attack.[81] As argued by some scholars, however, such an interpretation would appear to be contrary to the plain reading of Article 48 of AP I, which states that parties to a conflict shall "direct their *operations* only against military objectives."[82] Military objectives have been defined as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[83] Cable infrastructure is unlikely to be considered a pure civilian object considering that it is a dual-use object used for military and civilian purposes.[84] Indeed, State practice demonstrates that submarine cables have traditionally been perceived as legitimate military targets in times of armed conflict.[85] The interruption to communications caused by such deliberate damage can make an "effective contribution to military action" and "offer a definite military advantage."[86] There is accordingly a widespread view that *attacks* against cable infrastructure are legally permissible in times of armed conflict, arguably qualified by the law of neutrality that

(913) IRRC 287, 321 (2020).

79 The ICRC Commentary to AP I defines "military operations" as "any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat" or "related hostilities." *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶¶ 2191, 1936, 1875 (Yves Sandoz, Christophe Swinarski & Bruno Zimmerman eds., ICRC 1987).

80 AP I, *supra* note 34, art. 48.

81 The Tallinn Manual 2.0 states that only cyber operations against civilians or civilian objects that rise to a level of an attack are prohibited by the principle of distinction and those rules of the law of armed conflict that derive from the principle. *See* TALLINN MANUAL 2.0, *supra* note 26, rule 93, at 421, ¶ 5; Stefan Oeter, *Methods of Combat*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 237, ¶ 4 (Dieter Fleck et al. eds., 2021).

82 Gisel et al., *supra* note 78, at 324–25.

83 AP I, *supra* note 34, arts. 48, 52 (2).

84 TALLINN MANUAL 2.0 states that cyber infrastructure used for both civilian and military purposes is a military objective, or in other words, all dual-use objects and facilities are military objectives, without qualification. TALLINN MANUAL 2.0, *supra* note 26, rule 101, at 445–47.

85 For example, during the 1898 Spanish-American war, the US cut the Manila-Hong Kong telegraph cable owned by a British company and laid under a Spanish concession. Both Britain and Germany cut each other's telegraph cables in World War I. During World War II, in 1945, British submarines cut Japanese undersea cables between Hong Kong and Saigon and between Hong and Singapore.

86 As required by the definition of "military objective" in AP I, *supra* note 34, art. 52 (2); SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA, Jun. 12, 1994, art. 40.

dictates that attacks against neutral cyber infrastructure are prohibited.[87] This chapter takes the position that the principle of distinction should apply to the use of cable infrastructure for intelligence collection, as it would do to attacks. At the very least, this would require State parties to identify which particular part of the cable infrastructure might have a military objective and whether using that cable infrastructure for intelligence collection would confer a definite military advantage or, in other words, provide information of military value, and whether in the event of possible damage as a result of intelligence collection operations, data can be re-routed.[88]

Second, does the rule of proportionality also apply to cable infrastructure intelligence collection not amounting to an attack? Even though cable infrastructure is a legitimate target in armed conflicts, belligerents must still satisfy the proportionality test. That is, the belligerent should "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[89] Because of this, some scholars have suggested that the combination of the "scale of impact on civilian social and economic infrastructure and the likelihood of this damage spreading beyond the targeted State to neutral third States, can only be excessive in relation to any military advantage."[90] In light of this, it would be impossible for any military advantage to be considered proportional to the "widespread collateral damage that would occur to civilians resulting from the cutting of a submarine data cable."[91] The use of cable infrastructure for intelligence collection would not automatically result in such widespread damage. However, parties to armed conflict cannot completely exclude the possibility of communications being interrupted by their methods of tapping, and the direct tapping of cables on the seabed in particular would appear to pose the highest risk of cables being damaged. Accordingly, it would not make sense if such proportionality calculations were not made by States when deciding whether to conduct intelligence collection via cable infrastructure,

87 Kraska, *supra* note 68; Burnett, *supra* note 3, at 1673–74; Tamsin Phillipa Paige, Douglas Guilfoyle & Rob McLaughlin, *The Final Frontier of Cyberspace: Ensuring that Submarine Data Cables are Able to Live Long and Prosper (Part II)*, OPINIO JURIS, Oct. 16, 2020, http://opiniojuris.org/2020/10/16/the-final-frontier-of-cyberspace-ensuring-that-submarine-data-cables-are-able-to-live-long-and-prosper-part-ii/.
88 Paige et al., *supra* note 87.
89 AP I, *supra* note 34, art. 57 (2) (a) (iii); TALLINN MANUAL 2.0, *supra* note 26, rule 113, at 470.
90 Paige et al., *supra* note 87.
91 *Id*.

especially in view of the critical nature of cable infrastructure and the potential ramifications.

Third, the requirement of precaution applies to military operations and would apply to the use of cable infrastructure for intelligence collection. As recognized by the Tallinn Manual 2.0, constant care shall be taken to spare the civilian population, individual civilians and civilian objects in hostilities involving cyber operations.[92] This requires "all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible and to seek to avoid any unnecessary effects."[93]

There have been efforts to designate the data that travels through such cable infrastructure as a civilian object so that operations against data would be governed by the principles of distinction, proportionality, precaution and the protection they afford to civilian objects.[94] However, while the ICRC has recognized the need to guard civilian data, it acknowledges that an operation designed solely to access data without deleting or manipulating them would not be an attack against a civilian object.[95]

II
LAWS APPLICABLE IN PEACETIME

A LAW OF THE SEA

The law of the sea, as set out in the 1982 UN Convention on the Law of the Sea (LOSC), governs the tapping of one particular type of cable infrastructure, namely, submarine cables laid on the seabed.[96] The law of armed conflict does not automatically displace the law of the sea set out in the LOSC.[97] It will generally apply *mutatis mutandis* during periods of armed conflict, subject to certain rules and prohibitions laid out in the

92 TALLINN MANUAL 2.0, *supra* note 26, rule 114, at 476; AP I, *supra* note 34, art. 57 (1).
93 Gisel et al., *supra* note 78, at 324; TALLINN MANUAL 2.0, *supra* note 26, rule 114, at 476.
94 Gisel et al., *supra* note 78, at 317. The question of whether civilian data enjoys the same protection as civilian objects "has been subject to significant debate and remains unsettled" since objects need to be material, visible and tangible.
95 *Id*.
96 *United Nations Convention on the Law of the Sea*, 1833 UNTS 397 (adopted Dec. 10, 1982, entered into force Nov. 16, 1994) [hereafter LOSC].
97 Jann K. Kleffner, *Scope of Application of International Humanitarian Law*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 50, 79, ¶ 3.48 (Dieter Fleck et al. eds., 2021).

law of naval warfare or law of armed conflict, which may either supplement or supplant the provisions of the LOSC.[98] The LOSC also applies to intelligence collection that occurs before armed conflict but is used during armed conflict.

1 *Legality*

Intelligence collection in the maritime domain is not explicitly mentioned in the LOSC. It occasionally came up during negotiations as part of a larger debate on the permissibility of military activities in the oceans and was never the object of formal negotiations.[99] At the time, that the use of cable infrastructure for intelligence collection was forseen, is evidenced by the use of the Sound Surveillance System (SOSUS) for tracking submarines.[100] What was arguably not foreseen was the use of technology to intercept the data that was being transmitted through submarine cables. As mentioned above, submarines or other underwater vehicles are most likely to be used in such operations, although such operations are undoubtedly technically challenging and cost-intensive, which may reduce the possibility of it occurring. Nonetheless, the rules governing the use of submarines and underwater vehicles for intelligence collection will also determine the legality and limits of the use of cable infrastructure for intelligence collection. These rules, arguably with the exception of the high seas, can be subject to differing interpretations and arguments and do not unequivocally provide answers on the legality of cable tapping on the seabed.

The LOSC *prima facie* prohibits intelligence collection in the 12-nautical-mile territorial sea where the coastal State has sovereignty (subject to the right of innocent passage and other rules of international law not inconsistent with the LOSC).[101] First, intelligence collection in the territorial sea is akin to conducting espionage within the territory of a State, which several scholars have argued is "inconsistent with the essential norm of international law that States respect the sovereignty, territorial integrity and political independence of other States."[102] Second,

98 TALLINN MANUAL 2.0, *supra* note 26, at 233, ¶ 5.

99 Military activities include intelligence gathering, training of forces, testing and use of vessels, equipment and installations, weapons tests, and military engagements either short of or amounting to armed conflict: NATALIE KLEIN, MARITIME SECURITY AND LAW OF THE SEA 43 (2011). *See also* George V. Galdorisi & Alan Kaufman, *Military Activities in the Exclusive Economic Zone: Preventing Uncertainty and Defusing Conflict* 32 CAL. W. INT'L L. J. 253, 271 (2002).

100 *See generally* SAMUEL ROBINSON, OCEAN SCIENCE AND THE BRITISH COLD WAR STATE (2018) 156–57.

101 LOSC, *supra* note 96, art. 2.

102 James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUM. J. TRANSNAT'L L 164, 181 (2015).

while foreign ships, including foreign warships, have the right of innocent passage, certain activities that are considered "prejudicial to the peace, good order or security of the coastal State" will render passage non-innocent, including any act aimed at collecting information to the prejudice of the defense or security of the coastal State, any act aimed at interfering with any systems of communications or any other facilities or installations of the coastal State, and carrying out research or survey activities or any other activity not having a direct bearing on the passage.[103] Third, all submarines and other underwater vehicles are required to navigate on the surface and to show their flag, which obviously limits their ability to conduct underwater activities.[104] These rules would appear to prohibit, at the very least, submarine intelligence activities in the territorial sea and, consequently, the tapping of cable infrastructure directly on the seabed of the territorial sea.[105] The Tallinn Manual 2.0 also considers that the tapping of submarine cables in the territorial sea using submarines or underwater vehicles constitutes a violation of that State's sovereignty (although not the sovereignty of the State that laid or operates the cable).[106]

On the other hand, it has been suggested that while submarines that navigate underwater are not entitled to claim innocent passage, their intelligence activities while submerged may not necessarily be unlawful *per se*.[107] This is also consistent with the position taken by many scholars that intelligence collection in peacetime is not prohibited by general international law.[108] Moreover, questions are raised on whether a foreign submarine that is tapping a submarine cable in a coastal State's territorial sea is collecting information that *prejudices the defense and security of that coastal State*. Only after selectors are applied would it be possible to determine the nature of the information collected. It is also arguable that tapping cables that transit the territorial sea without making landfall in the coastal State may not prejudice the defense and security of that coastal State, for example, because the data is related to other States.[109] On this view, the tapping of cables located in the territorial sea but not making

103 LOSC, *supra* note 96, art. 19 (c), (j) (k) and (l).
104 LOSC, *supra* note 96, art. 20.
105 Kraska, *supra* note 102, at 219.
106 TALLINN MANUAL 2.0, *supra* note 26, at 257, ¶ 17.
107 Kraska, *supra* note 102, at 227–28; Natalie Klein argued that "intelligence gathering activities are not specifically outlawed as a matter of international law but affect the characterization of the passage of foreign vessels." KLEIN, *supra* note 99, at 215.
108 Kraska, *supra* note 102, at 246.
109 *Id.* at 219, 246. A counterargument may be that the tapping alone may be prejudicial, especially if it is bulk surveillance, because the assumption is that all communications that go through the cable—and may include those of the coastal State—are caught in the dragnet.

landfall may also not be considered an interference with the "systems of communications or any other facilities or installations of the coastal state."[110] Similarly, the tapping of submarine cables in the territorial sea for the interception of data running through them would also not constitute "the carrying of research or survey activities," although it may be considered an activity "not having a direct bearing on passage."

In other maritime zones under coastal State sovereignty, that is, archipelagic waters and straits used for international navigation, the legal position is even more ambiguous. For example, the Tallinn Manual 2.0 states that cable tapping that occurs in archipelagic waters would be considered cyber infrastructure subject to the sovereignty of the coastal State.[111] As mentioned above, submarine cables transiting these maritime zones without making landfall in the coastal/archipelagic State may not be considered the coastal State's cyber infrastructure. Moreover, the transit passage and archipelagic sea lane passage regimes permit submarines to traverse in normal mode solely for the purpose of continuous and expeditious transit,[112] which is said to mean that submarines can traverse submerged.[113] On this basis, tapping submarine cables for intelligence collection may be consistent with transit passage, provided it is not tantamount to a threat or use of force against the sovereignty, territorial integrity or political independence of the strait State or archipelagic State.[114]

In the EEZ outside coastal State sovereignty but where the coastal State has sovereign rights over natural resources, all States have the freedom to lay submarine cables and other internationally lawful uses of the sea related to those freedoms, including those associated with the operation of submarine cables, subject to the obligation to have due regard to the rights and duties of the coastal State.[115] This *sui generis* zone is arguably the stage for the most contentious debates on the permissibility of

110 Although note that it is said that States enjoy sovereign authority over cyber infrastructure physically located within their territory regardless of whether that infrastructure belongs to or is operated by government institutions, private companies or private individuals and includes computer networks and systems supported by that cyber infrastructure: TALLINN MANUAL 2.0, *supra* note 26, rule 2, at 13. At the same time, sovereign authority over cable infrastructure could be construed as merely a right to regulate rather than cable infrastructure belonging to or serving the coastal State.

111 TALLINN MANUAL 2.0, *supra* note 26, rule 54, at 257, ¶ 17.

112 LOSC, *supra* note 96, arts. 39(1)(c), 54.

113 Jia Bin Bing, *Article 39: Duties of Ships and Aircraft During Transit Passage*, *in* UNITED NATIONS CONVENTION ON THE LAW OF THE SEA: A COMMENTARY 302, ¶ 5 (Alexander Proelss ed., Hart 2017).

114 LOSC, *supra* note 96, arts. 39(1)(b), 54; Kraska, *supra* note 102, at 222; Klein notes that while transit passage may technically permit intelligence gathering, "a wide variety of intelligence gathering activities during transit passage should not be read into the "normal mode" characterization." KLEIN, *supra* note 99, at 217.

115 LOSC, *supra* note 96, art. 58(1).

military activities, including intelligence collection.[116] These debates play out against the backdrop of the escalating geopolitical rivalry between the US and China with the former arguing that military activities, including intelligence collection, are permissible in another State's EEZ, and China rejecting such arguments on the basis, *inter alia*, that the LOSC does not explicitly mention it and it comes under the regime of marine scientific research requiring the consent of coastal States.[117] For present purposes, this chapter adopts the position that the tapping of cables in the EEZ can be subsumed under military activities (permissible in the EEZ), and there is nothing in the LOSC to suggest that it is prohibited, especially since submarines can travel submerged in the EEZ.[118]

On the high seas, the maritime area in which States have the most latitude, all States have freedoms of the seas, including the freedom of navigation and the freedom to lay submarine cables.[119] While not mentioned, intelligence collection is a military activity that is considered a freedom of the high seas. The Tallinn Manual 2.0 correctly notes that "there is no rationale for excluding cyber activities from the notion of high seas freedoms and other lawful uses of the seas."[120]

2 *Limits*

The above discussion illustrates that arguments can be made for and against the legality of cable tapping in maritime zones under the sovereignty of coastal/archipelagic States; and in areas beyond sovereignty, arguments against the permissibility of this activity become weaker. If the tapping of cables is not explicitly prohibited in any of these zones, there would certainly be limits. Indeed, scholars have suggested limitations on the right to conduct intelligence collection particularly within the EEZ, where it is most contentious.[121] The most salient express limitation is the obligation to exercise *due regard* for the rights and duties of the coastal State in the EEZ and the interests of other States in their

116 For a snapshot of the different views, see Raul (Pete) Pedrozo, *Preserving Navigational Rights and Freedoms: The Right to Conduct Military Activities in China's Exclusive Economic Zone*, 9 CHINESE J. INT'L L 9 (2010); Zhang Haiwen, *Is It Safeguarding the Freedom of Navigation or Maritime Hegemony of the United States? Comments on Raul (Pete) Pedrozo's Article on Military Activities in the EEZ*, 9 CHINESE J. INT'L L 31 (2010).

117 TALLINN MANUAL 2.0, *supra* note 26, at 240, ¶ 4, at 257, ¶ 17.

118 *See also* TALLINN MANUAL 2.0, *supra* note 26, at 257, ¶ 17.

119 LOSC, *supra* note 96, art. 87.

120 TALLINN MANUAL 2.0, *supra* note 26, at 234, ¶ 3, at 257, ¶ 17.

121 Moritaka Hayashi, *Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms*, 29 MAR. POL. 123 (2005); Stuart Kaye, Freedom of Navigation, *Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from Beyond the Littoral* 24 AUST. YB INT'L L 93 (2005); Lubin, *supra* note 54.

exercise of high seas freedoms.[122] The due regard obligation has been interpreted in the *Chagos Marine Protected Area Arbitration* as not imposing any rule governing universal conduct, or a uniform obligation to avoid any impairment of the other State's rights or an entitlement to the other State to proceed as it wishes, merely noting such rights.[123] The extent of the regard required by the LOSC will depend upon the nature of the rights held by the relevant State, their importance, the extent of the anticipated impairment, the nature and importance of the activities contemplated, and the availability of alternative approaches.[124] The majority of cases will require some form of consultation with the State holding the rights.[125] As noted by Lubin, this echoes the necessity and proportionality requirements. Indeed, Lubin has suggested *jus ad bellum* rules such as necessity, immediacy and proportionality as a possible framework to limit intelligence collection in the EEZ.[126] The imposition of these rules for cable tapping on the high seas or in the EEZ matches the intent and reasoning of the *Chagos Marine Protected Arbitration* and would necessitate States to conduct a similar analysis to that described in the section below and to consider, *inter alia*, whether it is necessary to tap cable infrastructure to meet their objectives, whether there are alternative approaches, and what precautions can be taken to prevent unintended consequences. The "due regard" obligation does not expressly apply in areas under coastal State sovereignty. However, it would seem even more pressing that when States are utilizing submarines or underwater vehicles to tap cables in areas under coastal State sovereignty (to the extent that it is considered permissible in the territorial sea), this should be subject to the same limitations that are applicable in areas beyond sovereignty.

B INTERNATIONAL HUMAN RIGHTS LAW

While human rights law has traditionally been perceived as applicable in times of peace, it has now been generally accepted that human rights continue to apply during armed conflict.[127] In most cases, there will be no

122 *Chagos Marine Protected Area Arbitration* (Mauritius v. the United Kingdom), Annex VII Arbitration, Award of Mar. 18, 2015, ¶ 519.
123 *Id*.
124 *Id*.
125 *Id*.
126 *See generally* Lubin, *supra* note 54.
127 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, ICJ Reports, ¶ 25 (July 8); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004, ICJ Reports, ¶¶ 102–42 (July 9); Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, 2005, ICJ Reports, at 168, ¶ 219

conflict between the two regimes and, instead, IHL is most likely silent on the issue, and human rights law will be able to fill the gap.[128] This is particularly so when it comes to the use of cable infrastructure for intelligence collection and the concomitant violations of the right to privacy.

Privacy has been defined as "the presumption that individuals should have an area of autonomous development, interaction and liberty from State intervention and excessive unsolicited intrusion by other uninvited individuals."[129] As put by Watt, "[p]rivacy is also vital to society as a whole, as it permits and facilitates the making of democratic choices; protects against the state's arbitrary interference; and enables the exercise of other rights, including those of free expression and assembly."[130] International human rights law has consistently affirmed the right to privacy in UN documents and international treaties such as the 1948 Universal Declaration of Human Rights (UDHR) ("no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence");[131] the 1950 European Convention on Human Rights (ECHR) ("everyone has the right to respect for his private life, his home and his correspondence");[132] and the 1966 International Covenant on Civil and Political Rights (ICCPR) ("no one shall be subject to arbitrary or unlawful interference with his family, home or correspondence").[133] With the profound transformations caused by the digital revolution, the right to privacy has emerged as a critical human right, particularly after the 2013 Snowden disclosures, with numerous initiatives within and outside the UN recognizing and elaborating on what the right to privacy means in the digital age.[134] It is now recognized "that the same rights that people have offline must also be protected online," and that States must "respect and protect the right to privacy, including in the context of digital communication."[135]

(December 19); Jann Kleffner, *Human Rights in Armed Conflict*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 450, ¶14.01 (Dieter Fleck et al. eds., 2021).

128 Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES 463–92, 482 (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., 2022).

129 U.N. GA, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Ben Emmerson, U.N. Doc A/69/397, ¶ 28 (Sept. 23, 2014).

130 WATT, *supra* note 10, at 93.

131 U.N. GA, Universal Declaration of Human Rights, U.N. GA Res 217 A (III), art. 12 (Dec. 10, 1948).

132 European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5, art 8 (adopted Nov. 4, 1950, entered into force Sept. 3, 1953).

133 U.N. GA, International Covenant on Civil and Political Rights, 999 UNTS, 171, art 17 (adopted Dec. 16, 1966, entered into force Mar. 23, 1976).

134 WATT, *supra* note 10, at 15–20.

135 Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, U.N. Doc A/HRC/20/L.13, (June 29, 2012); U.N. GA, The Right to Privacy in the Digital Age, U.N. Doc A/Res/68/167, ¶ 4 (a) (Dec. 18, 2013).

Bulk interception of data transmitted through civilian cables will inevitably intercept private individuals' communications and hence implicates the right to privacy.[136] The ability of the right to privacy to constrain the use of cable for infrastructure depends on several threshold questions being answered. First, it is not clear whether the right to online privacy has crystallized into customary international law and claims relating to the infringement of the right to privacy are confined to human rights treaties that affirm the right to privacy and to States parties thereto.[137]

Second, the arguments relating to the extraterritoriality of the application of human rights treaties are particularly relevant for intelligence collection by cable infrastructure. This chapter will not revisit the already comprehensive discussion on whether the right to privacy protects persons (citizens and foreigners alike) situated outside the intercepting State.[138] It suffices to note that it has progressively been accepted that States will be held accountable for their human rights violations either where they exercise effective control over an area spatially (i.e., a State will have effective control over individuals who are located outside its territory if it exercises effective control over that territory) or over a person (i.e., when the State exercises authority and control over an individual).[139] The meaning and scope of such effective control remain subject to diverse interpretations. Narrow interpretations require that *physical control* over territory or individuals be met,[140] while more expansive interpretations contend that effective control is met if the State has effective control over the person's rights.[141] Human rights courts have not comprehensively examined the jurisdictional clauses in the specific context of intelligence collection via cable infrastructure.[142] In the most recent decision of the European Court of Human Rights (ECtHR) between Big Brother Watch and the UK (discussed below), the Court did not address extraterritoriality as at least some applicants were clearly within the UK's territorial jurisdiction and the Court proceeded on the assumption that the complaint fell within the jurisdictional competence of the United Kingdom.[143]

The narrow interpretation of "effective control" as confined to physical control will mean that States' obligations on privacy will only be implicated if cable infrastructure is located within their territory and the

136 BUCHAN, *supra* note 11, at 95–96.
137 WATT, *supra* note 10, at 141.
138 BUCHAN, *supra* note 11, at 96–105; WATT, *supra* note 10, at 142–92.
139 WATT, *supra* note 10, at 173–86.
140 TALLINN MANUAL 2.0, *supra* note 26, at 185, ¶ 10; BUCHAN, *supra* note 11, at 100.
141 WATT, *supra* note 10, at 335–36.
142 *Id*.
143 BBW v. UK, *supra* note 25.

individuals affected are within their control. However, bulk interception of data encompasses all communications transmitted on a particular cable and, consequently, involves the interception of information on entire populations outside the intercepting States' territories.[144] The narrow test would not cover the scenarios where the interception takes place remotely wholly outside the territory and territorial sea of a State (e.g., through the backdoor installation of equipment or the tapping of cables on the seabed of a coastal State's EEZ and the high seas). The narrow interpretation would cover the interception of data at cable landing stations (which was directly in question in the Big Brother Watch case) but would be limited to the data of individuals within the surveilling State's jurisdiction, which would result in differentiation in treatment between nationals and aliens, raising issues of discrimination and equality of treatment.[145] The more expansive interpretation of *effective control*, which focuses on a State's control over individuals whose rights it has effective control and power over or has a detrimental impact on the human rights of persons outside its borders, would better cover the use of cable infrastructure for the interception of data because the way in which communications travel makes it difficult or impossible in practice to distinguish between communications along nationality/location lines.[146]

The next question is whether the use of cable infrastructure for intelligence collection is an infringement of the right to privacy. Relevant human rights bodies and courts have adopted different approaches on this. UN bodies such as the Human Rights Council and the Office of the High Commissioner for Human Rights as well as UN Special Rapporteurs on Human Rights and Fundamental Freedoms have consistently found that mass surveillance programs constitute an interference with the right to privacy of communications protected by Article 17 of the ICCPR.[147] These UN bodies have found, *inter alia*, that mass surveillance interferes with the right to privacy when the data is collected, irrespective of whether the data is analyzed. They have circumscribed the legitimate aims for which mass surveillance can be carried out and have recognized that mass or bulk surveillance programs may be deemed arbitrary for being neither necessary nor proportionate because of the amount of data collected, and hence do not meet the requirement that measures should be the least intrusive on human rights.[148]

144 WATT, *supra* note 10, at 161, 173.
145 *See generally* WATT, *supra* note 10, at 142–92.
146 *Id.* at 334.
147 *Id.* at 217.
148 Office of the UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age.

The European human rights system, on the other hand, has adopted a different approach. The ECtHR has considered the bulk interception of data post the Snowden disclosures in *Big Brother Watch and Others v. United Kingdom* and *Centrum for Rättvisa v. Sweden* brought by NGOs to challenge the bulk surveillance regimes of these States.[149] The complaints centered on (1) the bulk interception of communications (i.e., the tapping into and storage of volumes of data drawn from fiber optic cables); (2) the obtaining of communications data from communication service providers; and (3) receipt of intercepted material from foreign governments. The ECtHR found that bulk interception regimes did not *per se* fall outside the States' margin of appreciation, given the "proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection."[150] Notably, the Court found that at the first stage of interception, the interception and retention of communications data was not a particularly significant interference with an individual's right to privacy, and that the degree of interference with individuals' rights will increase as the bulk interception processes progress.[151] Nonetheless, bulk interception had to be subject to certain end-to-end safeguards, and at the domestic level, an assessment of proportionality should be made at each of the four stages of the process of the necessity and proportionality of the measures being taken.[152] These include the requirement that bulk interception "should be subject to independent authorization at the outset, when the object and scope of the operation are defined; and that the operation should be subject to supervision and independent ex post facto review."[153]

From the above discussion, it appears that human rights bodies and courts have differing views on whether the actual collection of data via tapping into cable infrastructure constitutes an infringement of the right to privacy. Nonetheless, even the ECtHR found that an assessment of proportionality must be made at the stage of collection, which would appear to be the minimum safeguard required to be met by States and, again,

Report of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, ¶ 20 (Jun. 30, 2014).

149 BBW v. UK, *supra* note 25; Centrum för Rättvisa v. Sweden, Grand Chamber of the European Court of Human rights, Judgment, 2021 (May 25).

150 BBW v. UK, *supra* note 25, ¶ 340.

151 *Id.* ¶ 330.

152 The Court in *BBW v. UK* described the stage of bulk interception as follows: (a) the interception and initial retention of communications and related communications data; (b) the application of specific selectors to the retained communications; (c) the examination of selected communications data by analysts; and (d) the subsequent retention of data and use of the final product, including sharing the data with third parties. *See* BBW v. UK, *supra* note 25, ¶ 325.

153 *Id.* ¶ 350.

echoes the limits discussed above in relation to the laws applicable in armed conflict and the law of the sea. Therefore, while the right to privacy may not prohibit the use of cable infrastructure for intelligence collection, it at the very least imposes some important limits which become even more stringent as the collected data is analyzed and shared.[154]

CONCLUSION

The use of cable infrastructure for intelligence collection, like most intelligence-related activities, occurs in the "parallel track of State conduct" that flies below the radar, which often means that unless this activity causes significant collateral harm, there will not be an obvious response.[155] This chapter is an attempt to determine how selected fields of international law may be interpreted to apply to intelligence collection via cable infrastructure in armed conflict. Several tentative conclusions can be made. First, determining the permissibility of intelligence collection via cable infrastructure in each separate field of international law under discussion is not clear-cut. There is some uncertainty about the wholesale applicability of IHL and the law of the sea governing intelligence collection via cable infrastructure. Second, and notwithstanding the first point, it would seem that this activity is not expressly prohibited by any of the fields of law under discussion, and this is consistent with the general position in international law that intelligence collection is permitted in armed conflict. Third, the law applicable to armed conflict, the law of the sea and human rights law can be used to extrapolate general limitations on this activity, including the principles of distinction, proportionality and precaution, all of which would apply to States when making the decision to tap cable infrastructure. This calculation is essential when considering the importance of cable infrastructure to States and individuals alike, particularly in times of armed conflict.

154 For a discussion on this, see BUCHAN, *supra* note 11, at 109–21; Lubin, *supra* note 128, at 467–76.
155 Efrony & Shany, *supra* note 43, at 596, 691.

Digital Rights and the Obligations of Militaries and Humanitarian Organizations

Chapter 10

Military Subject Access Rights: A Comparative and International Perspective

Tim Cochrane[1]

INTRODUCTION

Imagine that a villager paralyzed during a special forces combat raid requests access to body camera data to support their claim that the attack was unlawful.[2] Suppose a retired citizen needs data from a local administrative agency under the authority of an occupying power to prove their entitlement to emergency pension payments.[3] Consider a serving member of a nation's armed forces, recently returned from an armed

1 The author would like to thank Dr. Russell Buchan and Dr. Asaf Lubin for their detailed comments throughout, as well as the participants of the conference for their feedback on an earlier draft. The usual disclaimers apply.

2 Mark Willacy, *Video Shows Australian SAS Soldier Shooting and Killing Unarmed Man at Close Range in Afghanistan*, ABC NEWS, (Mar. 16, 2020, at 10:12 AM, updated Mar. 20, 2020, at 4:01 AM), https://www.abc.net.au/news/2020-03-16/video-shows-afghan-man-shot-at-close-range-by-australian-sas/12028512.

3 JAMES DOBBINS ET AL., OCCUPYING IRAQ: A HISTORY OF THE COALITION PROVISIONAL AUTHORITY 199–200 (2009).

conflict, who seeks their military health records to track the progression of a newly diagnosed respiratory illness.[4] These varied scenarios have a unifying theme: all involve individuals seeking their personal data from armed forces in the context of (what are assumed to be) armed conflicts. This theme is the focus of this chapter, which explores "subject access rights" in armed conflicts through the lenses of comparative and international law.

"A review of the roles that the rights to privacy and data protection play in regulating [wartime military behavior] is long overdue," Asaf Lubin recently remarked.[5] This chapter responds to Lubin's call, focusing on the potential of subject access rights to obtain personal data from military agencies during armed conflicts—referred to throughout as military subject access rights (or MSARs). It assumes that individual rights, including privacy and data protection, should be prioritized by States. From that rights-based perspective, it examines MSARs in four dualist common law jurisdictions—Australia, Canada, New Zealand, and the United Kingdom—under data protection, as well as applicable international human rights law (IHRL) and international humanitarian law (IHL) obligations. This chapter has two aims. First, and primarily, it offers a roadmap for individuals seeking to make MSARs in the four comparator States. Secondly, and more generally, it hopes to inform States and others working on data protection frameworks applicable to military agencies—both within the comparator jurisdictions and elsewhere—about how to reform or implement MSARs in a rights-protective manner.

Part I provides background information, contextualizing subject access rights, outlining their significance during armed conflicts, and explaining this chapter's choice of comparator jurisdictions. Focusing on domestic data protection law, Part II outlines MSARs, including redress mechanisms, in these four jurisdictions. Part III then evaluates the extent to which these MSARs are effective in practice, using the three hypothetical scenarios above as case studies, and considering applicable IHL and IHRL. While Parts II and III largely speak to individuals seeking to make MSARs, this chapter concludes with recommendations for States, international organizations, and others.

4 Michael J. Falvro et al., *Airborne Hazards Exposure and Respiratory Health of Iraq and Afghanistan Veterans*, 37 EPIDEMIOLOGIC REVS. 116 (2015).

5 Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES 491 (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., 2022).

I BACKGROUND

A SUBJECT ACCESS RIGHTS, DATA PROTECTION, AND IHRL

Subject access rights—enforceable legal powers to obtain your own personal data from others—have a long pedigree in data protection law.[6] Data protection generally protects information privacy, meaning the ability to control the "acquisition, disclosure and use" of personal data by mandating "core principles" of data processing.[7] Subject access rights are described as "the most important" of these principles.[8] They are "a necessary first step enabling the exercise of most other data subject rights" and "a strategic tool to assess compliance with data protection law more broadly."[9] They are typically enforceable through domestic data protection statutes, including in the four comparator jurisdictions outlined here.[10] They are also recognized regionally within the General Data Protection Regulation (GDPR) of the European Union (EU),[11] as well as "Convention 108+,"[12] the "only legally binding international instrument on data protection universal in scope."[13]

Data protection overlaps with, but is often seen as materially distinct from, the right to privacy in IHRL.[14] The latter protects individuals

6 *See* Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors—Data Subject Access Rights in Practice*, 8 INT'L DATA PRIV. L. 4, 5–7 (2018).

7 *Report of the International Law Commission on the Work of its Fifty-Eighth Session, Annex IV: Protection of Personal Data in Transborder Flow of Information*, ¶ 23 (2006) UN Doc Supplement No. 10 (A/61/10) (2006) [hereinafter *ILC Report*]; Lubin, *supra* note 5, at 475.

8 *E.g.*, *ILC Report*, *supra* note 7, ¶ 23; Organisation for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Explanatory Memorandum, ¶ 58 (Sept. 23, 1980) C(80)58/FINAL 1980, *revised as* THE OECD PRIVACY FRAMEWORK (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf; *see* Ausloos & Dewitte, *supra* note 6, at 7.

9 Ausloos & Dewitte, *supra* note 6, at 7.

10 *See* sources cited *infra* note 50.

11 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 (General Data Protection Regulation), art. 15 (2016) O.J. (L119) 1 [GDPR].

12 Comm. of Mins., Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (consolidated text), Preamble, art. 9(b), 128th Sess., CM/Inf(2018) 15-final (May 17–18, 2018) (Convention 108+), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168076c65bf; *see* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art. 8(b), *opened for signature* Jan. 28, 1981, E.T.S. No. 108 (entered into force Oct. 1, 1985).

13 Alessandra Pierucci, Chair of the Comm. of Convention 108, & Jean-Phillippe Walter, Data Prot. Comm'r, Council of Eur., Speech at 40th Annual Convention 108 on Data Protection, Jan. 25, 2021, https://rm.coe.int/40th-anniversary-convention108/1680a1307e.

14 *E.g.*, *ILC Report*, *supra* note 7, ¶¶ 13–15; Lubin, *supra* note 5, at 468–76; *see* Juliane Kokott &

"against arbitrary or unlawful interference" with privacy, including in relation to home, correspondence, and similar realms, from (at the very least) public authorities (meaning governments and others exercising public functions).[15] The right to privacy has wide recognition within IHRL, including in Article 8 of the European Convention on Human Rights (ECHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[16] It is also regularly reflected within domestic human rights or constitutional frameworks—including at least partly in three of the comparator jurisdictions,[17] Australia being the exception.[18] Indeed, Lubin suggests that the right to privacy is now "part of customary international law"[19]—in contrast with data protection, which he suggests "awaits further crystallization."[20]

Although subject access rights are more commonly discussed in relation to data protection rather than IHRL[21]—presumably because (only) the former expressly provides for them—IHRL is nonetheless relevant. Most significantly, while the complete gamut of data protection rights is assumedly not (yet) recognized by IHRL[22]—indeed, full respect for such digital rights may require more than merely readapting existing IHRL frameworks[23]—subject access rights *specifically* may be, at least when personal data is sought from public authorities. The European Court of Human Rights (ECtHR) has gone "a long way towards introducing such a general right to access" in its Article 8 ECHR jurisprudence, Orla Lynskey argues.[24] Similar comments have been made regarding ICCPR Article 17.[25] The IHRL right to freedom of expression (FOE) may contain a related right to access government information[26]—often provided in domestic

Christoph Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 Int'l Data Pri. L. 222, 223 (2013).

15 *E.g.*, International Covenant on Civil and Political Rights, art. 17, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

16 *Id.*

17 Canadian Charter of Rights and Freedoms, ss 7–8, Part I of the Constitution Act, 1982 (Can.), *being* Schedule 2 of the Canada Act, 1982, c. 11 (U.K.); New Zealand Bill of Rights Act 1990, ss 21, 28; Human Rights Act 1998, c. 42, sch. 1, art. 8 (U.K.).

18 *See* Thomas v. Mowbray [2007] HCA 33, 233 CLR 307 ¶¶379–380 (Kirby J dissenting on other grounds); Moira Paterson, Freedom of Information & Privacy in Australia: Information Access 2.0 ¶ 1.102 (2nd ed., 2015).

19 Lubin, *supra* note 5, at 472 (*citing* Alexandra Rengel, Privacy in the 21st Century 108 (2013)).

20 *Id.* at 14.

21 *E.g.*, *id.* at 6–15; Kokott & Sobotta, *supra* note 14, at 223.

22 *See* source cited *supra* note 19 and accompanying text.

23 *See generally* Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights—A Proposed Typology*, Eur. J. It'l L. (forthcoming 2021).

24 Orla Lynskey, The Foundations of EU Data Protection Law 128 (2015) (*citing* K.H. v. Slovakia, 2009-II Eur. Ct. H.R. 391).

25 *E.g.*, Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 Int'l J.L. & Inf. Tech. 247, 253–54 (1998) (*citing* United Nations Human Rts. Comm., *General Comment No. 16*, ¶ 10, U.N. Doc. HRI/GEN/1/Rev 9 vol. I (April 8, 1988)).

26 United Nations Human Rts. Comm., *General Comment No. 34*, U.N. Doc. CCPR/C/GC/34, ¶ 18–19

freedom of information (FOI) statutes.[27] However, while FOE will often support privacy and data protection rights, on other occasions the two sets of rights conflict.[28] They have "different policy underpinnings": FOE promotes government transparency, while subject access rights seek to provide individuals control over personal data, which may be sensitive and intended to remain confidential.[29] This chapter therefore grounds MSARs in privacy and data protection rather than FOE.

B MILITARY DATA, IHL, AND THE COMPARATOR JURISDICTIONS

Individuals increasingly need MSARs to obtain their personal data from military agencies in the context of armed conflicts, given the quality and quantity of personal data these agencies routinely collect and retain. The U.S. military obtained vast amounts of data, including sensitive biometric information, on citizens of Afghanistan and Iraq during these armed conflicts.[30] Service members' own data is routinely processed on the battlefield: military personnel, for example, may be expected to use "wearable smart devices" continuously monitoring their health.[31] Artificial Intelligence systems being deployed in armed conflicts require "[l]arge data pools" implicating privacy concerns,[32] leading to predictions that "States will be ever more inclined to obtain a full take of all data relevant to a given theater of combat."[33] The hypothetical scenarios with which this chapter opened—which Part III revisits—provide further examples. As

(Sept. 12, 2011); *see* Maeve McDonagh, *The Right to Information in International Human Rights Law*, 13 HUM. RTS. L. REV. 25, 26 (2013).

27 *E.g.*, Freedom of Information Act 1982 (Cth.) (Austl.) [AUFOI].

28 *See* Gabriela Zanfir-Fortuna, *Article 15 Right of Access by the Data Subject*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 449, 452 (Christopher Kuner, Lee A. Bygrave, Chris Docksey & Laura Drechsler eds., 2020); David Banisar, *The Right to Information and Privacy: Balancing Rights and Managing Conflicts* (World Bank Institute Governance Working Paper Series 80740, 2011).

29 *Id.*

30 Eileen Guo & Kimat Noori, *This is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban*, MIT TECH. REV. (Aug. 30, 2021), https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/; Spencer Ackerman, *U.S. Holds on to Biometrics Database of 3 Million Iraqis*, WIRED (Dec. 21, 2011, 6:30 AM), https://www.wired.com/2011/12/iraq-biometrics-database/.

31 Caitlin Doornbos, *Navy Pilot Program Uses Wearable Smart Devices in Effort to Prevent Sleep Deprivation among Soldiers*, STARS AND STRIPES (Aug. 19, 2021), https://www.stripes.com/branches/navy/2021-08-19/navy-sleep-pilot-program-sailors-fitzgerald-mccain-2607983.html; Kyle Mizokami, *Smart Fibers Could Turn Army Uniforms into Wearable Computers*, POPULAR MECHS. (June 17, 2021), https://www.popularmechanics.com/military/research/a36732071/army-uniform-fibers-create-wearable-computers/.

32 *See* CONG. RES. SERV., R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 8–9 (v. 10, updated Nov. 10, 2020).

33 Robin Geiss & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INT'L L. STUD. 556, 571–72 (2021).

those indicate, individuals may want to obtain their own data for various reasons, including to enforce other legal rights.[34]

"Despite this evolving reality," explains Lubin, "there is practically no international legal jurisprudence… applying these rights during armed conflict," either in relation to MSARs or privacy and data protection generally.[35] Armed conflicts were traditionally governed by the laws of war, now known as IHL.[36] It is increasingly understood, and assumed here, that IHRL concurrently applies alongside IHL,[37] although IHRL will be "interpreted against the background of" IHL, the latter typically serving as *lex specialis*.[38] Additionally, while IHL regulates armed conflicts at all times, States must respect IHRL only in respect of persons within their "jurisdiction"[39]—a term the ECtHR has interpreted as "primarily territorial," extending extraterritorially "only in exceptional cases."[40] Crucially, States also remain subject to applicable domestic law during armed conflicts.[41] Given the dearth of relevant international jurisprudence, this latter legal framework—domestic law, specifically domestic data protection legislation—is the focus of this chapter's analysis of MSARs.

This chapter assesses the MSARs given by Australia, Canada, New Zealand, and the United Kingdom specifically for several interlinked reasons. First, this focus is practically useful: these jurisdictions all recognize MSARs and have a significant combined military influence worldwide. Even the smallest, New Zealand, has service members deployed within theaters in the Middle East, Africa, Asia, and the Pacific.[42] This chapter's MSAR roadmap is thus potentially broadly applicable. Secondly, as these are similar common law jurisdictions, all taking a dualist approach to public international law,[43] they are readily internally comparable:[44] differences in the scope and operation of MSARs in one country may credibly inform potential reforms in another. This chapter's comparative analysis

34 *See supra* text accompanying note 9.
35 Lubin, *supra* note 5, at 466.
36 DIETER FLECK, THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 20 (4th ed. 2021).
37 *See id.* at 450; Lubin, *supra* note 5, at 481–83.
38 Hassan v. United Kingdom [GC], 2014-VI Eur. Ct. H.R. 1 [102]–[107]; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶ 25 (July 8); *see* FLECK, *supra* note 36, at 453; Lubin, *supra* note 5, at 481.
39 FLECK, *supra* note 36, at 499; Lubin, *supra* note 5, at 471–72.
40 Al-Skeini v. United Kingdom [GC], 2011-IV Eur. Ct. H.R. 99 [130]–[142]; *cf.* Lubin, *supra* note 5, at 471.
41 *See* Marco Sassòli, *International Humanitarian Law and International Human Rights Law*, *in* THE OXFORD GUIDE TO INTERNATIONAL HUMANITARIAN LAW 381, 401–2 (Ben Saul & Dapo Akande eds., 2020); Lubin, *supra* note 5, at 483; ANNE PETERS, BEYOND HUMAN RIGHTS: THE LEGAL STATUS OF THE INDIVIDUAL IN INTERNATIONAL LAW 217–20 (2016).
42 *Our Operations and Engagements*, NEW ZEALAND DEFENCE FORCE (NZDF), https://www.nzdf.mil.nz/nzdf/our-operations-and-engagements/ (last visited Jan. 28, 2022).
43 *See generally* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF INTERNATIONAL LAW 45 (9th ed., 2019).
44 *E.g.*, Sheldrake v. Dir. of Pub. Pros. [2004] UKHL 43 [33] (Lord Bingham), [2005] 1 AC 264.

may also be externally useful outside these jurisdictions: the comparator States' laws, including the specific legal areas canvassed here, are typically considered robust and influential;[45] this analysis may therefore potentially inspire the implementation or reform of MSARs elsewhere. Indeed, most States now have data protection laws.[46] These appear to commonly include MSARs, including in States retaining conscription, such as Austria and Singapore.[47] Many international organizations operating during armed conflicts also have data protection guidelines with quasi-MSARs.[48] Finally, the similarities and differences in MSARs—indeed, subject access rights generally—across these four jurisdictions may contribute to ongoing discussions as to whether such rights now form part of IHRL.[49]

II
COMPARING MILITARY DATA ACCESS RIGHTS (MSARS)

A ARTICULATING THE RIGHT: SCOPE AND EXCEPTIONS

Australia, Canada, New Zealand, and the United Kingdom each provide individuals with a right to obtain their own personal data from government agencies,[50] generally including the armed forces and other military

45 *E.g.*, Claudia Geiringer, *A New Commonwealth Constitutionalism?*, *in* THE CAMBRIDGE COMPANION TO COMPARATIVE CONSTITUTIONAL LAW 554, 570–71 (Roger Masterman & Robert Schütze eds., 2019); Sandesh Sivakumaran, *Asia-Pacific States and the Development of International Humanitarian Law*, *in* ASIA-PACIFIC PERSPECTIVES ON INTERNATIONAL HUMANITARIAN LAW 118 (Suzannah Linton, Tim McCormack & Sandesh Sivakumaran eds., 2019); Graham Greenleaf, *A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108*, *in* EMERGING CHALLENGES TO PRIVACY LAW: COMPARATIVE PERSPECTIVES 92, 119 (Normann Witzleb et al. eds., 2014). *But see* sources cited *supra* note 18 and accompanying text.

46 *Data Protection and Privacy Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE AND DEV. (updated Dec. 14, 2021), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide; *see supra* text accompanying notes 6–13.

47 For Austria, see BUNDESGESETZ ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN (DATENSCHUTZGESETZ – DSG) [FEDERAL ACT CONCERNING THE PROTECTION OF PERSONAL DATA (DSG)] No. 165/1999, as amended, ss 4, 44, https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html (Austria). For Singapore, see Public Sector (Governance) Act 2018, ss 2, 6–8; GOVERNMENT INSTRUCTION MANUAL ON INFOCOMM TECHNOLOGY & SMART SYSTEMS MANAGEMENT (Sing.) (not publicly available); *see* SMART NATION & DIGITAL GOV'T OFF., GOVERNMENT PERSONAL DATA PROTECTION POLICIES 9–10 (2021).

48 *E.g.*, INT. COMM. OF THE RED CROSS, RULES ON PERSONAL DATA PROTECTION 2, 12–13 (2015, updated and adopted 2019); INT. ORG. FOR MIGRATION, DATA PROTECTION MANUAL 66 (2010).

49 *See supra* text accompanying notes 19–25.

50 Privacy Act 2020, s 22, Information Privacy Principle 6 (N.Z.) [NZPA]; *Privacy Act 1988* (Cth.) sch 1 para 12.1 (Austl.) [APA]; Privacy Act, R.S.C. 1985, c. P-21, s 12(1) (Can.) [CPA]. For the UK, see GDPR, art. 15; Data Protection, Privacy and Electronic Communications (Amendments etc) (EU

agencies, such as departments of defense.[51] All include this right within dedicated privacy legislation.[52] For three of the four comparator jurisdictions, this chapter analyses these dedicated privacy statutes. Australia, however, provides a "complementary" and more "comprehensive" procedure for obtaining personal data in its Freedom of Information Act 1982 (AUFOI);[53] thus, this chapter focuses on that instead.

Subject access rights to obtain data from military agencies—MSARs—have an expansive scope in all four jurisdictions. "Personal data" (or "personal information") is defined broadly, capturing both electronic and paper records.[54] MSARs apply to data merely under the control of military agencies,[55] as well as apparently extending extraterritorially to data created and/or stored overseas.[56] In three of these jurisdictions, MSARs are given to all (living) natural persons, regardless of nationality or residence.[57] The one outlier is Canada, which restricts this right to citizens and permanent residents.[58]

Access may nonetheless be refused under "exceptions" or "withholding grounds,"[59] including what may imperfectly be called a "national

Exit) Regulations 2019, SI2019/419, regs. 2–3, sch. 1 (incorporating the GDPR in UK law with amendments) [UKGDPR]; Data Protection Act 2018, c. 12, Pt. 2 (U.K.) [UKDPA].

51 APA, ss 6(1) (definitions of "agency," "APP entity," "Defence Department," "Defence Force," "Department"), (6), s16A(1); CPA, s 8 (definition of "government institution"), sch. (reference to "Department of National Defence (including the Canadian Forces)"); NZPA, s 7 (definition of "public sector agency"); UKGDPR, art. 86A; UKDPA, s 7; Freedom of Information Act 2000, c. 36 (UK), sch. 1, paras. 1, 6 [UKFOI]; *e.g.*, Knowles v. Sec'y, Dep't of Def. [2020] FCA 1328 ¶ 35 (17 September 2020) (Austl.); *e.g.*, Garnhum v. Can. (Deputy Att'y Gen.) (1996), 30 C.H.R.R. 152, para. 7 n. 12 (Fed. Ct.) (Can.); Plumtree v. Att'y-Gen. HRRT 29/01, Oct. 2, 2002 [23] (Hum. Rts. Rev. Trib.) (N.Z.); Crosbie v. Sec'y of State for Def. [2011] EWHC (Admin) 789 [74] (U.K.). Exceptions apply. *See, e.g.*, text accompanying *infra* note 121.

52 *See supra* sources cited note 50.

53 Office of the Aus. Info. Comm'r, FOI Guidelines: Guidelines Issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982 ¶¶ 7.1, 7.5 (June 2020) [hereinafter AUFOI Guidelines]; Office of the Aus. Info. Comm'n Australian Privacy Principles Guidelines: Privacy Act 1988 ¶¶ 12.22, 12.24, 12.30 (July 2019). Analogous APA caselaw is referenced below.

54 APA, s 6 (definition of "personal information"); AUFOI, s 4 (definitions of same and "document"); NZPA, s 4 (definitions of same); CPA, s 8 (definition of "personal information"); UKGDPR, arts. 2(1)–(1A), (5), 4(1); *see* recitals (26), (30); *see also* CPA, ss 18, 36 (permitting exemptions for "information banks" in Canada but providing for review mechanisms).

55 AUFOI, ss 4 (definition of "document of an agency"), 6C; CPA, s 12(b); NZPA, s 10; UKGDPR, art. 4(7); *see* "OV" v Common. Sci. and Indus. Research Org. [2018] AICmr 48 (22 March 2018) ¶¶ 12–32 (Austl.); Can. (Info. Comm'r) v. Can. (Min. of Def.), 2011 SCC 25 paras. 47–63, [2011] 2 S.C.R. 306; Case C-25/17, Procs. brought by Tietosuojavaltuutettu (Jehovan todistajat), ECLI:EU:C:2018:551 [75], [2019] 1 CMLR 5 (CJEU); Williams v. N.Z. Police [2020] NZHRRT 26 [28]–[35].

56 This is explicitly stated in New Zealand and UK law. NZPA, ss 4(1)(a), (2); UKGDPR, art. 3; UKDPA, s 207. A similar interpretation is long-standing in Australia, Re O'Grady v. Austl. Fed. Police [1983] AATA 390, and appears in early Canadian guidance. *See* Can. Post Corp v. Can. (Minister of Public Works), [1995] 2 FC 110 para. 39 (F.C.A.) (Marceau J.A. dissenting).

57 AUFOI, s 11(1); NZPA, s 7 (definition of "individual"); UKDPA, § 3 (definitions of "Identifiable living individual" and "Data subject"); *see* recitals (2), (14); *Re Lordsvale Finance Ltd and Dep't of Treasury* [1985] AATA 174, 3 AAR 301.

58 CPA, s 12(1). Canada and New Zealand take the same restrictive approach to freedom of information. *See* Access to Information Act 1982, R.S.C., 1985, c. A-1, s 4 (Can.); Official Information Act 1982, s 12(1) (N.Z.) [NZOIA]. *Contrast* AUFOI, s 11; UKFOI, § 1.

59 AUFOI, ss 7, 31B, 33–47; CPA, ss 18–28; NZPA, ss 49–53; UKDPA, §§ 24(5), 25–28; UKGDPR, art. 12(5).

security" exception[60]—assumedly the key ground for military agencies. While statutory language differs, this exception generally applies where, to quote the Australian statute, disclosure "would, or could reasonably be expected to cause damage to" security, defense, international affairs, or similar.[61] A relatively high threshold is needed to trigger it. Australia mandates "reasonable grounds [of] at least a real, significant, or material possibility" of damage from disclosure.[62] Canada and New Zealand use broadly similar language.[63] Whether the UK threshold is "reasonably necessary" or a "more exacting test" of "essential" is unclear.[64] Even where the national security exception is available, reliance on it is optional; a military agency could theoretically decide to release the data.[65]

B ENFORCEMENT: COMPLAINT MECHANISMS AND DEROGATIONS

To understand a right, it is important to consider the extent to which it can be meaningfully enforced.[66] While internal reconsideration of an unsuccessful MSAR request may be requested—as Australia and the UK expressly recommend[67]—an individual's first external option will typically be a designated "Privacy" or "Information" Commissioner (Commissioner).[68] The Commissioner is an independent legal officer tasked with (among other roles) investigating data access complaints.[69] Commissioners normally have extensive investigatory powers,[70] including being entitled to compel production of any data withheld on national security grounds for review.[71] These powers by default usually override

60 AUFOI, s 33(a); CPA, s 21; NZPA, s 51(a); UKDPA, § 26; *see, e.g.*, Ruby v. Can. (Sol. Gen.), 2002 SCC 75 para. 5, [2002] 4 S.C.R. 3; *Zhou v. Chief Exec., Dep't of Labour* [2011] NZEMPC 36 [88]; *see also* Orna Ben-Naftali & Roy Peled, *How Much Secrecy Does Warfare Need?*, *in* TRANSPARENCY IN INTERNATIONAL LAW 321, 322, 327–30 (Andrea Bianchi & Anne Peters eds., 2013).

61 AUFOI, s 33a; *see* CPA, s 21; NZPA, s 51(a); UKDPA, § 26(1).

62 AUFOI GUIDELINES, *supra* note 53, ¶¶ 5.15–5.18; *see* Prinn v. Dep't of Def. [2016] AATA 445 ¶¶ 58–96, 152 ALD 162.

63 *See* Ternette v. Can. (Sol.-Gen.), [1992] 2 F.C. 75 para. 34(4); Beattie v. Official Assignee [2021] NZHRRT 21 [78], *appeal denied*, [2021] NZHC 1607.

64 Aven v. Orbis Bus. Intel. Ltd. [2020] EWHC (QB) 1812 [110]–[112], [129].

65 *See* APA, ss 3A, 11A(4), 31A; CPA, ss 8(2), 21; UKDPA, § 21; UKGDPR, art. 23(1)(a); NZPA, ss 24(1)(a), 51(a); *e.g.*, Cemerlic v. Can. (Sol. Gen.), 2003 FCT 133 paras. 8, 24, 228 F.T.R. 1.

66 *See generally* 3 WILLIAM BLACKSTONE, COMMENTARIES 109.

67 AUFOI, s 54, pt. VI; UKGDPR, arts. 57(1)(f), (2); *see* AUFOI GUIDELINES, *supra* note 53, ch 9; ¶¶ 4.59, 9.3–9.5; ROSEMARY JAY, DATA PROTECTION: LAW AND PRACTICE ¶ 13–068 (5th ed. 2020).

68 AUFOI, s 54L(1)–(2)(a), 54N; CPA, ss 29–35; NZPA, ss 69(3)(a), 70–72; UKGDPR, art. 77; UKDPA, § 165.

69 APA; s 54L; CPA, s 29(1)(b); NZPA, s 20; UKGDPR, arts. 57(1)(f), (2)–(3), 77, recitals (20), (122). *See generally Australia Information Commissioner Act 2010* (Cth.) (Aus.); CPA, ss 53–67; NZPA, ss 13, 17–18, 21; UKGDPR, arts. 51–59; UKDPA, pt. 5, sch. 12.

70 AUFOI, ss 55R–X; CPA, s 34; NZPA, ss 85–87; UKGDPR, arts. 31, 39(d), 58(1).

71 AUFOI, ss 55R–U; CPA, ss 34(1)–(2); UKGDPR, arts. 58(a), (e)–(f); UKDPA, §§ 115(7), 142–145, 154, sch. 15; *see* Can. (Royal Can. Mounted Police) v. Can. (Att. Gen.), 2005 FCA 213 paras. 31, 37,

legal privilege and even "public interest immunity"[72]—a common law doctrine discussed below.[73] The UK, however, generally limits its Commissioner's override powers.[74] Indeed, the UK "purport[s] to wholly exclude the powers of the Commissioner to scrutinise" the use of the national security exception.[75] In each country, the Commissioner and their staff must maintain strict confidentiality.[76] A withholding military agency may potentially provide submissions to the Commissioner *ex parte* (without the other side) and *in camera* (in private).[77] Except for the Canadian Commissioner, who may only make non-binding recommendations,[78] a Commissioner may issue an enforceable disclosure order if it concludes that personal data was improperly withheld.[79]

Secondly—usually only if a Commissioner complaint is dismissed[80]—an individual may seek judicial redress: in New Zealand and Australia, these complaints are normally heard by specialist tribunals,[81] while in Canada and the UK, they go to general courts.[82] Special judges may sit where national security concerns are alleged.[83] These judicial bodies have similarly broad investigatory powers.[84] In all jurisdictions, the military agency may be permitted to provide submissions *ex parte* and *in camera*.[85]

68, 2006 1 F.C.R. 53; NZPA, ss 87–88; Dir. of Human Rights Procs. v. Richardson Human Rights Review Tribunal HRRT 36/05, Dec. 21, 2005 [32] (N.Z.); AUFOI GUIDELINES, *supra* note 53, ¶¶ 10.91–10.96; ICO, REGULATORY ACTION POLICY 18–19 (2018).

72 This is made express in Canada and New Zealand. CPA, s 34(2)–(2.2); NZPA, ss 88(1)–(2), 90(2)–(3), (6), 89, 209(1)(a); *see* Jeffries v. Priv. Comm'r [2010] NZSC 99 [10], [2011] 1 NZLR 4. It is implied in Australia under s55X of the AUFOI regarding privilege and recent legislative amendments regarding public interest immunity. *See infra* notes 103–104; *e.g.*, *Xenophon and Dep't of Def.* [2016] AICmr 14 (16 March 2016) ¶¶ 4–5, 8.

73 *See* sources cited *infra* note 94 and accompanying text.

74 On privilege, see UKDPA, §§ 143(2), sch. 15, paras. 11–13; UKGDPR, recital (164); COLIN PASSMORE, PRIVILEGE ¶¶ 1.49–1.51 (4th ed. 2019). On public interest immunity, see by analogy Wallace Smith Trust Co. Ltd (In Liq.) v. Deloitte Haskins & Sells (a firm) [1997] 1 WLR 257 (EWCA).

75 JAY, *supra* note 67, ¶¶ 20-004, 20-038 to 20-039 (*citing* R (Home Sec'y) v. Info. Trib. [2006] EWHC (Admin) 2958, [2008] 1 WLR 58); *see* UKDPA, § 26(2), (g)(i), (h). *But see* UKGDPR, art. 77; R (Open Rights Grp.) v. Sec'y of State for the Home Dep't [2021] EWCA (Civ) 800 [11]–[13], [2021] WLR 3611.

76 AUFOI, ss 55T(5), 55U(4); CPA, ss 62–63, 65; NZPA, ss 81(6), 90(1), 206.

77 *See* AUFOI GUIDELINES, *supra* note 53, ¶ 10.104; CPA, s 33(1)–(2); *e.g.*, "PN" v. Aus. Taxation Off. [2018] AICmr 71 (12 December 2018) ¶¶ 11–17.

78 CPA, s 35; *see* H.J. Heinz Co. of Can. Ltd. v. Can. (Att. Gen.), 2006 SCC 13 paras. 33–39, [2006] 1 S.C.R. 441.

79 AUFOI, s 55K; NZPA, s 92, UKGDPR, art. 58(2)(c); *see* AUFOI, ss 55ZA–D.

80 AUFOI, s 57A(1); CPA, ss 35(5), 41; NZPA, s 98(1); *e.g.*, Mitchell v. Privacy Comm'r [2017] NZHC 569 [31], [36]; *cf.* UK GDPR, art. 79; UKDPA, § 167; *see also* Dotcom v. United States of America [2014] NZHC 2550 [54]–[59], [69]–[72] (citing NZPA, s 31(2)).

81 AUFOI, pt. VIIA; NZPA, ss 96–99, 104–106. *See generally Administrative Appeals Tribunal Act 1975* (Cth.) (Austl.) [*AATA*]; Human Rights Act 1993, pt. 4 (N.Z.) [NZHRA].

82 UKGDPR, art. 79; UKDPA, §§ 167, 180; *see* Scranage v. Info. Comm'r [2020] UKUT 196 (AAC).

83 AUFOI, ss 58B–D; CPA, s 51(1); *see* Sogi v. Can. (Min. of Citizen. and Imm.), 2004 FCA 212 para. 45, [2005] 1 F.C.R. 171.

84 AUFOI, ss 58A, 57AE, 60A; CPA, s 45; NZPA, ss 109(2)(a), (3), 111(2), 209(1)(b); NZHRA, s 106; *Section 167 – Compliance Orders*, [2021] 2 WHITE BOOK ¶ 3G-44 (June 3, 2021) [hereinafter WHITE BOOK]; *see* Ternette v. Can. (Sol. Gen.), [1984] 2 FC 486 [14].

85 *AATA*, s 35; AUFOI, ss 63–64; CPA, ss 51(2)(a), (3); NZPA, s 109(2)(b), (3); WHITE BOOK, *supra* note 84, ¶ 3G-44; *see* Ruby v. Can. (Sol. Gen.), 2002 SCC 75 paras. 53–60, [2002] 4 S.C.R. 3; Beattie v. Official Assignee [2021] NZHRRT 21 [5]–[6]; *e.g.*, Re OJG Engineering Pty Ltd v Comm'r of Taxation [2019] AATA 4293.

While specific rules differ, each court or tribunal will normally conduct a full "merits review" as to whether the military agency was correct to rely on the national security ground.[86] An enforceable disclosure order may ultimately be issued.[87] Beyond this, domestic appeals may be possible.[88] An individual may also separately seek judicial review of the process (rather than merits) of how their MSAR request was handled.[89] Courts may, however, be slow to entertain judicial review where individuals have not exhausted the above redress options.[90] Finally, international remedies may theoretically be available—the most obvious being through an application to the ECtHR from an individual dissatisfied with a UK military agency withholding decision.[91] A withholding decision from one of the other States may potentially be the subject of a complaint to the United Nations Human Rights Committee (UNHRC).[92]

The above domestic mechanisms may, however, be short-circuited through derogations known as "ministerial certificates"—expansive statutory powers allowing a Government Minister to resist disclosure, even in the face of a court order, by signing a certificate claiming that withholding is necessary on national security grounds.[93] These build on the longstanding common law public interest immunity doctrine, giving governments special powers to resist court disclosure by asserting that national security or similar interests were engaged, which courts were traditionally loath to second-guess.[94] While judicial bodies confronted

86 *See* VMQD v Federal Commissioner of Taxation [2018] AATA 4619 [21]–[22]; Leahy v. Can. (Citizen. and Imm.), 2002 FCA 227 paras. 98–99, [2014] 1 F.C.R. 766; Dotcom v. Crown Law Office [2018] NZHRRT 7 [18]–[23], 11 HRNZ 420; Ittihadieh v. 5-11 Cheyne Gardens RTM Co Ltd [2017] EWCA (Civ) 121, [2018] QB 256.

87 AUFOI, s 58(2); CPA, s 49; NZPA, s 102(d); UKDPA, § 167(2); *see* AUFOI, s 60.

88 AUFOI, s 56; *AATA*, pt 6A; Federal Courts Act, R.S.C., 1986, c. F-7, s 27 (Can.) [FCA]; Supreme Court Act, R.S.C., 1985, c. S-26, ss 33, 37.1, 40(1) (Can.); NZPA, s 111(2); NZHRA, ss 123–126; Civil Procedure Rules 1998, SI1998/3132, r. 52 (U.K.).

89 *Administrative Decisions (Judicial Review) Act 1977* (Cth.) (Austl.); FCA, s 18.1; Judicial Review Procedure Act 2016 (N.Z.); Senior Courts Act 1981, c. 54, s 31 (U.K.); *see also* UKDPA, s 166.

90 *E.g.*, Knowles v Sec'y, Dep't of Def. [2021] FCAFC 215 ¶¶ 59, 69, 75; Mitchell v. Privacy Comm'r [2017] NZHC 569 [19], [38]–[43]; R (Hussain) v. Sec'y of State for Justice [2016] EWCA (Civ) 1111 [32], [2017] 1 WLR 761. *But see* Banlgadesh v. Can. (Att'y Gen), 2019 FC 1177 para. 13.

91 ECHR, *supra* note 15, arts. 34–35.

92 Optional Protocol to the ICCPR, *supra* note 15, arts. 1–2, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter Optional Protocol]. All comparator jurisdictions other than the UK have ratified. *See Status of Ratification: Interactive Dashboard*, UNITED NATIONS HUM. RIGHTS OFFICE OF THE HIGH COMM. (last updated Dec. 16, 2021), https://indicators.ohchr.org/ [select "Optional Protocol" from drop-down menu and navigate to individual jurisdictions].

93 CPA, s 70.1(1); Canada Evidence Act 1985, c. c-5, 38.13(1) (Can.) [CEA]; NZPA, s 88(3); Crown Proceedings Act 1950, s 27(3); UKDPA, § 27. Alternative statutory powers allow greater balancing of public interest factors. *E.g.*, *AATA*, s 34; Evidence Act 2006, s 70 (N.Z.); High Court Rules, r 8.26 (N.Z.).

94 Conway v. Rimmer [1968] AC 910 (HL) (appeal taken from Eng.); *see* Sankey v. Whitlam (1978) 142 CLR 1, 38–46 (HCA) (Austl.); Carey v. Ontario, [1986] 2 S.C.R. 637 paras. 79–85 (Can.); Choudry v. Attorney-General [1999] 2 NZLR 582, 593–94 (CA) (N.Z.). *See generally* Kenneth Keith, *Freedom of Information and International Law*, *in* FREEDOM OF EXPRESSION AND FREEDOM OF INFORMATION: ESSAYS IN HONOUR OF SIR DAVID WILLIAMS 349, 351–55 (J. Beatson & Y. Cripps eds., 2000).

with ministerial certificates today normally at least reserve the ability to confidentially review withheld documentation,[95] their ability to set aside such certificates is typically strictly limited, falling far short of a full merits review.[96] For example, the Canadian Supreme Court described the applicable statutory power as a "narrow right of review provid[ing] no effective judicial means or challenging or correcting a debatable decision by the [Minister] in balancing the public interest."[97] In Canada, the potential—now actual[98]—use of ministerial certificates has long been criticized.[99] Similar concerns have been echoed by the New Zealand Law Commission,[100] as well as recently voiced within the UK Parliament[101]—in the UK, ministerial certificates may prospectively exempt entire categories of data altogether.[102] The status quo regarding ministerial certificates in those three jurisdictions contrasts somewhat with Australia, where "conclusive" AUFOI certificate powers were removed in 2009, promoting transparency.[103] While ministerial certificates may still be deployed before the Australian tribunal assessing withholding complaints, these have much less force and do not restrict the tribunal's evaluation.[104]

95 This appears express in Canada and New Zealand. CEA, ss 38.11–12, 38.131(5)–(6); Dotcom v. Attorney-General [2019] NZCA 412 [22], [33]–[36], [2020] 3 NZLR 397, *leave to appeal dismissed*, [2020] NZSC 1. It seems implied in the UK. *See* UKDPA, §§ 27, 201; Tribunal Procedure (First-Tier Tribunal) (General Regulatory Chamber) Rules 2009, SI2009/1976, r 19(1A) (U.K.); Tribunal Procedure (Upper Tribunal) Rules 2008, SI2008/2698, rr. 5(d), 14, 15, 37, sch. 2 (U.K.). By analogy, see also UK Courts and Tribunal Judiciary, Practice Note: Closed Material in Information Rights Cases (2013).

96 For the Canadian approach, see CEA, s 38.131(10). Certain New Zealand and UK certificates may be challenged on "judicial review grounds" only. UKDPA, § 27(3)–(4); *Dotcom* [2019] NZCA 412 [22]; Hitchens v. Sec'y of State for the Home Dep't [2003] UKIT NSA5 [44]. *But see* Baker v. Sec'y of State for the Home Dep't [2011] UKHRR 1275 [63]–[76] (Info. Trib., Nat'l Sec. Appeals).

97 R v. Ahmad, 2011 SCC 6 para. 23, [2011] 1 S.C.R. 110.

98 *See* R v. Huang, 2021 ONSC 221 para. 5; Huang v. Can. (Att'y Gen.), 2019 FC 1122.

99 *E.g.*, Kent Roach, *"Constitutional Chicken": National Security Confidentiality and Terrorism Prosecutions after* R. v. Ahmad, 54 S.C.L.R. (2d) 357, 375 and 375 n. 63 (2011); Craig Forcese, *Clouding Accountability: Canada's Government Secrecy and National Security Law "Complex,"* 34 Ottawa L. Rev. 49, 81–82, 84 (2004); Kathy Grant, *The Unjust Impact of Canada's Anti-Terrorism Act on an Accused's Right to Full Answer and Defence*, 16 Windsor Rev. Legal & Soc. Issues 137, 149–50 (2003).

100 N.Z. Law Comm'n, The Crown in Court: A Review of the Crown Proceedings Act and National Security Information in Proceedings, chs. 5–7 (R135, December 2015) [hereinafter NZLC, Crown in Court].

101 *E.g.*, Data Protection Bill [Lords] Deb (15 Mar. 2018) cols. 111–14.

102 *See* UKDPA, § 27(2); Re Ewing [2002] EWHC (QB) 3160 [53].

103 AUFOI, ss 33(2)–(7), *repealed by Freedom of Information (Removal of Conclusive Certificates and Other Measures)* Act 2009 (Cth.) (Austl.); *see Warren & Chief Exec. Off., Servs. Austl.* [2020] AATA 4557 (9 November 2020) ¶ 82.

104 AATA, s 36; *see* Fewster v. Nat'l Archives of Austl. [2014] AATA 295 ¶ 18, 63 AAR 440; *e.g.*, Fernandes v. National Archives of Australia [2011] AATA 202 (28 March 2011).

III
APPLYING MSARS: CASE STUDIES

A SERVICE MEMBER SEEKING OVERSEAS HEALTH DATA

The service member seeking their own health data generated during an armed conflict overseas is the most straightforward case study. Each jurisdiction extends MSARs to service members[105]—assumedly either citizens or permanent residents. Health data collected and retained by a military would presumably be under its control under each State's law, even if created overseas.[106] While domestic legislation should, where possible, be interpreted consistently with IHL and public international law generally,[107] providing MSARs to service members appears entirely justifiable under IHL, not least because service members remain subject to their own State's law when operating overseas, including during armed conflicts.[108] Each State also has resources specifically confirming service members' MSARs.[109] Indeed, although information is limited—the contents of personal data requests are typically confidential unless litigated—MSAR requests by service members appear common, including for health records.[110]

Service members appear to have credible redress options in practice. Speaking generally, domestic judicial bodies evaluating MSAR complaints by service members and military agency employees scrutinize withholding grounds relatively closely.[111] Outside Australia, the possibility that a ministerial certificate may ultimately be issued to stymie complaints is nonetheless concerning, given the limited scope to challenge these.[112] Further

105 *See* sources cited *supra* notes 57–58 and accompanying text.
106 *See* sources cited *supra* notes 55–56 and accompanying text.
107 Durham Holdings Pty Ltd v. N.S.W. [2001] HCA 7 ¶¶ 29–31, 205 CLR 399; Nevsun Resources Ltd v. Araya, 2020 SCC 5 para. 170, 443 DLR 4th 183; LM v. R [2014] NZSC 110 [52], [2015] 1 NZLR 23; Assange v. Swedish Pros'n Auth. (Nos. 1 and 2), [2012] UKSC 22 [10], [98], [112], [115], [122], [160], [176], [201], [206], [217], [265], [2012] 2 AC 471 (appeal taken from Eng.). *See generally* A. Nolkaemper, National Courts and the International Rule of Law, ch. 7 (2011).
108 *E.g.*, Austl. Def. Force, Law of Armed Conflict, Austl. Def. Doctrine Pub. 06.4, ¶ 1.4 (2006).
109 *E.g.*, *Service Records*, NZDF, https://www.nzdf.mil.nz/nzdf/medal-and-service-records/service-records/ (last visited Dec. 29, 2021); *Requests for Personal Data and Service Records: A Detailed Guide*, UK Min. of Def. (updated Aug. 6, 2021), https://www.gov.uk/government/collections/requests-for-personal-data-and-service-records.
110 *E.g.*, Francis v. Dep't of Def. [2008] AATA 486 (12 June 2008) (Austl.); Re 100002721759, 2018 CanLII 78506 (June 27, 2018) (Can. Veterans Rev. and Appeal. Board); *see also supra* note 51.
111 *E.g.*, "SRTTT" v. Dep't of Def. [2004] AATA 1175 (9 November 2004); Frezza v. Can. (Nat'l Def.), 2014 FC 32, 445 F.T.R. 299; Plumtree v. Att'y-Gen. HRRT 29/01, Oct. 2, 2002 (N.Z.). *But see* Info. Comm'r of Can., Access at Issue: Nine Recommendations Regarding the Processing of Access Requests at National Defence (2020).
112 *See supra* text accompanying notes 93–104.

recourse may be available internationally. Most significantly, assuming subject access rights to data held by public agencies form part of the IHRL right to privacy,[113] UK service members may obtain recourse before the ECtHR: they will likely be "within the jurisdiction" of the UK for ECHR purposes when its armed forces collect and retain their data, whether at home or abroad.[114] Service members of the other three States may possibly bring UNHRC claims.[115] However, as Marko Milanovic explains, while the UNHRC traditionally has a "more generous" attitude towards questions of extraterritoriality, its regime is less robust and non-binding.[116]

B VILLAGER WANTING COMBAT CAMERA DATA

While the first case study outlined above may, at least in some respects, appear simple, the remaining two deal with relatively unchartered territory, and thus analysis must be much more speculative. With that caveat in mind, the villager seeking special forces camera data theoretically appears to be in a similar position as the service member above—other than in Canada, given that its legislation restricts MSARs to citizens and permanent residents.[117] While States' data protection obligations likely apply "more flexibly in the context of a military operation than in situations of relative normalcy,"[118] the UK Commissioner has expressly recognized that camera footage of overseas military engagements may contain personal data triggering UK data protection law.[119] This data would again be under the armed forces' control.[120] Indeed, other than in the UK, which has a carve-out for its special forces,[121] this data would still appear to be under armed forces' control even if only recorded on a soldier's personal electronic device.[122] This extraterritorial application of MSARs similarly appears consistent with IHL: "subject to compliance with minimum standards of humane treatment," IHL "leaves it to states to determine, usually

113 *See supra* text accompanying notes 21–25.
114 *See* ECHR, *supra* note 15, arts. 1, 8, 10; Smith v. Min. of Defence [2013] UKSC 41 [42]–[55], [102], [153], [2014] 1 AC 52 (appeal taken from Eng.).
115 *See* sources cited *supra* note 92.
116 *See* Optional Protocol, *supra* note 92, arts. 4–5; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 111 and 111 n. 122 (2015).
117 *See* sources cited *supra* note 58 and accompanying text.
118 *See* Marko Milanovic, *Intelligence Sharing in Multinational Military Operations and Complicity under International Law*, 97 INT'L L. STUD. 1269, 1397 (2021).
119 Ministry of Defence (Central Government) [2008] UKICO FS50099223 (Jan. 21, 2008).
120 *See supra* sources cited notes 55–56 and accompanying text.
121 UKFOI, sch. 1, para. 6(a); *see* UKDPA, § 7.
122 *See supra* sources cited notes 55–56 and accompanying text; *e.g.*, Peter Boshier, *Request for Footage of Battle of Baghak*, Case No. 411501 (Nov. 1, 2017) (interpreting an analogous NZOIA section).

under domestic law," what further protections may apply.[123] Additionally, to the extent that MSARs enhance transparency,[124] such extraterritorial application may respond to calls for this within IHL.[125]

Whether this villager would have effective scope to enforce MSARs in practice is less clear. There is little evidence that overseas persons have attempted to exercise MSARs, perhaps due to a lack of awareness.[126] They may also face practical and other difficulties in pursuing redress.[127] Conceivably, given the fact-sensitive nature of the national security exception,[128] the mere fact that a person—here, the villager—is overseas may be a relevant factor favoring the application of the exception and may further reduce the (already limited) scope the villager would have to challenge a ministerial certificate.[129] The villager would also have fewer international redress options: while they might have recourse before the UNHRC,[130] they would likely be barred from the ECtHR in relation to a UK military agency withholding decision—ECHR States are apparently not exercising ECHR "jurisdiction" when conducting military operations "during the active phase of hostilities" of international armed conflicts.[131]

C RETIREE WITHIN OCCUPIED TERRITORY REQUESTING PENSION DATA

The case of the retired citizen seeking data from an occupying power held by a local administrative agency raises even more difficult questions. Like the villager, the retiree, at first glance, appears entitled to MSARs in all States other than Canada.[132] A threshold issue is, however, whether the local administrative agency's data is under the control of

123 *See* Al-Waheed v. Min. of Def. [2017] UKSC 2 [276] (Lord Reed dissenting on other grounds), [2017] AC 821 (appeal taken from Eng.); *e.g.*, Geneva Convention (IV) relating to the Protection of Civilian Persons in Time of War, arts. 3, 107, Aug. 12, 1949, 6 U.S.T. 3516 [hereinafter Geneva Convention (IV)]; NZDF, MANUAL OF ARMED FORCES LAW, VOL. 4 LAW OF ARMED CONFLICT, DM 69 ¶¶ 11.2.25–11.2.26 (2nd ed. 2019); UK MIN. OF DEF., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT, JOINT SERVICE PUB. 383 ¶ 15.41 n. 96 (2004).

124 *Cf.* text accompanying note 29.

125 *E.g.*, Ben-Naftali & Peled, *supra* note 60; Lesley Wexler, *International Humanitarian Law Transparency*, 23 J. TRANSNAT'L L. & POL'Y 93 (2013–2014); EYAL BENVENISTI, THE INTERNATIONAL LAW OF OCCUPATION 346 (2nd ed. 2012).

126 *Cf.* text accompanying *supra* notes 109–110. *See generally* Ausloos & Dewitte, *supra* note 6, at 7.

127 *See, e.g.*, R. (Begum) v. Special Imm'n Appeals Comm'n [2021] UKSC 7 [85], [2021] AC 765 (appeal taken from Eng.).

128 *See, e.g.*, Arnold v. Queensland (1987) 73 ALR 607 ¶ 19 (FCA); Aven v. Orbis Bus. Intel. Ltd. [2020] EWHC (QB) 1812 [123].

129 *See supra* text accompanying notes 93–104.

130 *See* sources cited *supra* note 92. *But see* text accompanying *supra* note 116.

131 Georgia v. Russia (II) [GC], App. No. 38263/08, App. No. 38263/08, ¶¶ 83, 125–144 (Jan. 21, 2021), https://hudoc.echr.coe.int/eng?i=001-207757; *see* ECHR, *supra* note 15, art. 1.

132 *See supra* text accompanying notes 58, 117.

the occupying power.[133] As both the IHL law of occupation and IHRL, as currently interpreted, are triggered by effective control over territory,[134] this question may initially appear straightforward. MSARs as recognized by the domestic laws of the comparator States may, however, theoretically impose a more demanding test for assessing control.[135] This domestic law MSAR test must be separately considered, albeit while taking into account the particular international law context within which the occupying power is operating.[136] While doing so is ultimately a fact-sensitive exercise, the law of occupation accords an occupying power ample authority over agencies in occupied territory that may well meet domestic law MSAR control requirements—a corollary of the occupying power's duty to "restore and ensure, as far as possible, public order and [civil life]."[137]

As noted, the scope and application of MSARs must, where possible, be interpreted consistently with international law, including IHL and IHRL.[138] This interpretative task raises further difficulties in relation to this final case study. Traditionally, the IHL law of occupation strictly constrained legislative changes in occupied territory.[139] On that basis, assuming no indigenous data protection regime was previously in place, permitting a retiree to rely on an occupier's MSARs may be viewed as introducing *de facto* legislative changes in that territory in breach of IHL.[140] This chapter, however, assumes that IHL must now be applied concurrently with IHRL:[141] consistently with that, there is now "recognition of broader powers" to enact welfare-enhancing laws in occupied territory.[142] Whether such powers would permit the introduction of MSARs—or, indeed, public sector subject access rights generally—nonetheless merits "closer attention."[143]

On the one hand, we may consider the *de facto* introduction of an occupier's MSARs as welfare-enhancing and perhaps even "mandated" by IHRL.[144] But whether public sector subject access rights have now

133 *See* sources cited *supra* notes 55–56 and accompanying text.
134 Regulations Respecting the Laws and Customs of War on Land, art. 42, Annex to Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2297, T.S. No. 539 [hereinafter Hague Regulations]; *see supra* note 40.
135 *See* sources cited *supra* note 55.
136 *See* sources cited *supra* notes 107, 118 and accompanying text.
137 BENVENISTI, *supra* note 125, at 68–84 (*quoting* Hague Regulations, note 134, arts. 42–43); *see* Geneva Convention (IV), *supra* note 123, art. 64.
138 *See* sources cited *supra* note 107 and accompanying text.
139 *See generally* BENVENISTI, *supra* note 125, at ch. 4;; YORAM DINSTEIN, THE INTERNATIONAL LAW OF BELLIGERENT OCCUPATION, ch. 5 (2011).
140 *See* BENVENISTI, *supra* note 125, at 93.
141 *See supra* text accompanying notes 37–38.
142 BENVENISTI, *supra* note 125, at 92; DINSTEIN, *supra* note 139, at 120–23.
143 BENVENISTI, *supra* note 125, at 92–93; DINSTEIN, *supra* note 139, at 120–21.
144 BENVENISTI, *supra* note 125, at 75, 92–93, 102–4; *e.g.*, Lubin, *supra* note 5, at 483–86.

crystallized as part of IHRL is debatable[145]—and ultimately beyond the scope of this chapter to resolve. It is, in any event, conceivable that the introduction of an occupier's own MSARs "might not fit the needs of the occupied peoples."[146] Hypothetically, an occupied population may be entirely unfamiliar with subject access rights. Their culture may view data, even personal data, as strictly confidential and altogether inaccessible once handed over to public agencies.[147] Alternatively, even if IHRL requires an occupier to provide public sector subject access rights in some form,[148] the wholesale introduction of an occupier's own MSARs may be insufficiently tailored to the particular needs of the local population and amount to improper "annexation" of that territory.[149] Given these matters, while we may sympathize with the retiree's desire to use an occupier's MSARs, the consequences that this may bring for that territory may conceivably be unwelcome by the broader occupied population and potentially breach IHL.

The consequences of such a conclusion should be clearly stated. Most obviously, permitting such reliance by the retiree would put the occupying power in breach of IHL, regardless of what the occupying force's domestic law provided.[150] Conversely, however, any expressly extraterritorial MSARs, including those given by New Zealand and the UK,[151] would likely be given effect by that occupying force's domestic courts even if inconsistent with IHL[152]—a consequence of the dualist approach these comparator States take to public international law.[153] With that in mind, the retiree's ability to enforce MSARs in practice appears mixed. That individual's domestic redress options will likely be no better than that of the villager.[154] Both administrative and judicial institutions have traditionally been reluctant to provide effective oversight over their own armed forces when acting as an occupier[155]—Israeli courts being a notable, albeit inconsistent, exception.[156] Assuming that the extension

145 *See supra* text accompanying notes 20, 24–25.
146 BENVENISTI, *supra* note 125, at 93; *see* DINSTEIN, *supra* note 139, at 123–25.
147 *See* Jeanne Saliou, *Data Protection and Privacy Through the Lens of Cultural Relativism*, LE LABORATOIRE D'INNOVATION NUMÉRIQUE DE LA CNIL (Oct. 27, 2021), https://linc.cnil.fr/fr/data-protection-and-privacy-through-lens-cultural-relativism.
148 *See supra* text accompanying notes 142, 144.
149 Geneva Convention (IV), *supra* note 123, art. 64; BENVENISTI, *supra* note 125, at 93; *see* DINSTEIN, *supra* note 139, at 122; *e.g.*, INT. COMM. OF JURISTS, THE ROAD TO ANNEXATION: ISRAEL'S MANEUVERS TO CHANGE THE STATUS OF THE OCCUPIED PALESTINIAN TERRITORY 26 (2019); *see also* BENVENISTI, *supra* note 125, at 228–33, 241.
150 *See* CRAWFORD, *supra* note 43, at 45.
151 *See supra* note 56 and accompanying text.
152 *See* CRAWFORD, *supra* note 43, at 45; sources cited *supra* note 107.
153 *See* source cited *supra* note 43 and accompanying text.
154 *See supra* text accompanying notes 126–129.
155 BENVENISTI, *supra* note 125, at 326.
156 *Id.* at 217–24, 327.

of MSARs within that occupied territory had in fact been consistent with IHL and IHRL, the retiree may, however, fare better internationally: an indigenous population is undoubtedly under the control of an occupier and thus within IHRL jurisdiction.[157]

EVALUATION AND RECOMMENDATIONS

MSARs as implemented by Australia, Canada, New Zealand, and the United Kingdom appear to offer genuine scope to individuals to obtain their personal data from the armed forces and other military agencies. While this scope varies depending on circumstances and jurisdiction, this chapter has set out a practical roadmap for individuals seeking to exercise such rights. This may inform individuals implicated in armed conflicts involving any of these comparator States, as well as other jurisdictions with analogous MSARs.

This chapter closes with recommendations for both these comparator States and others. First, from a rights-based perspective, its analysis reveals gaps in the domestic law scope and application of MSARs in the comparator States. To better protect the privacy and data protection rights that underlie MSARs—indeed, public sector subject access rights generally—these jurisdictions should consider plugging these gaps. Ongoing legislative reforms in each State may provide this opportunity.[158] Most significantly, to ensure effective judicial oversight and thus protection of MSARs, the remaining States may wish to follow Australia's lead by removing or amending ministerial certificate powers.[159] Worryingly, a recently introduced New Zealand Government bill would do the opposite, proposing new conclusive certificate powers restricting judicial oversight.[160] Canada should also contemplate expanding its MSARs to

157 Georgia v. Russia (II) [GC], App. No. 38263/08, App. No. 38263/08, ¶ 196 (Jan. 21, 2021), https://hudoc.echr.coe.int/eng?i=001-207757; *see id.* ¶¶ 83, 161–175; BENVENISTI, *supra* note 125, at 331–32.

158 ATT'Y-GEN.'S DEP'T, AUSTL. GOV'T, PRIVACY ACT REVIEW: DISCUSSION PAPER (2021); UK DEP'T FOR DIGITAL, CULTURE MEDIA & SPORT, DATA: A NEW DIRECTION (2021); *Modernizing Canada's Privacy Act*, GOV'T OF CAN. (updated Sept. 1, 2021), https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html; Kris Faafoi, *Security Information in Proceedings Legislation Bill Passes First Reading*, BEEHIVE.GOVT.NZ (Dec. 15, 2021), https://www.beehive.govt.nz/release/security-information-proceedings-legislation-bill-passes-first-reading.

159 *See supra* sources cited notes 93–104 and accompanying text.

160 Security Information in Proceedings Legislation Bill (97-1), pt 3, sch 2 (N.Z.); *see* (14 Dec. 2021) 756 NZPD (Security Information in Proceedings Legislation Bill – First Reading). *Contra* NZLC, CROWN IN COURT, *supra* note 100, ¶¶ 6.69–6.72.

overseas persons,[161] while the UK should similarly reconsider its purported restrictions on its Commissioner's investigatory powers.[162] While Australia's MSARs appear relatively more robust, this may be because the absence of a federal rights framework has led there to more detailed legislative scrutiny[163]—the absence of such a framework is, however, itself concerning.

This analysis and set of recommendations may also inform additional States with MSARs, as well as international organizations and others interacting with personal data during armed conflicts.[164] This chapter may even inform hold-out States without MSARs.[165] Even if such rights are merely "best practice,"[166] holdouts may wish to implement MSARs to aid their armed forces' "legal interoperability" with others[167] or in response to international pressure.[168] Australia and New Zealand, for example, extended subject access rights to overseas persons at the urging of the EU,[169] and Canada may soon do the same.[170] Finally, holdout States should also consider seriously the possibility that MSARs are required pursuant to IHRL.[171] While it is beyond our scope here to resolve this question, this chapter has offered conflicting evidence intended to inform this debate: while MSARs as implemented by these comparator States have much in common, they retain material differences, and the ability to derogate through ministerial certificates is significant. Regardless, MSARs—again, like government subject data access rights generally—will likely only increase in importance. Robust rights-protective frameworks to give effect to these rights should be prioritized.

161 *Cf.* text accompanying *supra* note 58.
162 *Cf.* text accompanying *supra* note 75.
163 *See* sources cited *supra* note 18.
164 *See supra* text accompanying notes 46–48.
165 *See* Lubin, *supra* note 5, at 483.
166 *Id.*
167 *See* David S. Goddard, *Understanding the Challenge of Legal Interoperability in Coalition Operations*, 9 J. Nat'l Sec'y L. & Pol'y 211, 225–28 (2017).
168 *See* Anu Bradford, Brussels Effect: How the European Union Rules the World 132–36 (2020).
169 Privacy Amendment Act 2004, No. 49, 2004, s 4 (Cth.) (Austl.); Privacy (Cross-border Information) Amendment Act 2010, No 113, s 3(a) (N.Z.); *see* Aust. Law Reform Comm'n, For Your Information: Australian Privacy Law and Practice, vol. 2 ¶¶ 31.21–31.22 (ALRC108, 2008); N.Z. Law Comm'n, Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4 ¶¶ 14.31–14.34 (IP17, March 2010).
170 *See* Dep't of Just. Can., Privacy Principles and Modernized Rules for a Digital Age 19–20 (2019).
171 *See* Lubin, *supra* note 5, at 482–83; *supra* text accompanying notes 20, 24–25.

Chapter 11

Managing Data Privacy Rights in Multilateral Coalition Operations' Information Sharing Platforms: A "Legal Interoperability" Approach

Deborah A. Housen-Couriel[1]

INTRODUCTION

A BACKGROUND: LEGAL INTEROPERABILITY IN MILITARY COALITION OPERATIONS

Military coalitions have always shared large quantities of diverse types of data. Joint operations require the common use of operational specifications, identification details for combatants and other personnel, communications and geolocation data, medical and health records, and other mission-critical details.[2] The exchange of such information requires

1 Faculty of Law, Hebrew University of Jerusalem and Chief Legal Officer and VP Regulation, Konfidas Digital Ltd.

2 Tien Pham & Greg Cirincione, *Sensor, Data and Information Sharing for Coalition Operations*, *in* Proceedings of the Seventh International Conference on Knowledge Systems for Coalition Operations Conference (2012), http://ksco.info/ksco/ksco-2012/papers/KSCO-2012-Pham-Sensor%20-Data-Info-Sharing.pdf.

a high level of confidentiality and trust among the sharing organizations. Examples of military coalitions, both ad hoc and permanent,[3] that have established such information sharing (IS) platforms include the Multi-National Force—Iraq (MNF-I) set up by UN Security Council Resolution 1546;[4] the Multinational Force and Observers under the Egypt-Israel peace treaty;[5] the Multinational Joint Task Force (MNJTF) of Nigeria, Niger, and Chad;[6] the forces envisioned under the Association of Southeast Asian Nations (ASEAN) Treaty of Amity and Cooperation;[7] the EU's Permanent Structured Cooperation (PESCO);[8] and the North Atlantic Treaty Organization (NATO).[9] Figure 1 depicts a simplified scheme of typical information sharing requirements within such multinational coalitions.

Beyond the operational aim of efficiently communicating information to achieve coalition aims, IS also serves to mitigate potential informational asymmetries among members concerning coalition aims, capabilities and performance, ultimately impeding coalition objectives. Crucial issues such as personnel and equipment capacity and availability, communications capabilities, tactical and strategic planning, and operational timelines rely on robust, accurate, and rapid IS. Due to the radical digitization of operations data and the use of "big data" to support military activities overall, such accelerated and deepened data sharing has become increasingly critical for military coalitions' operations over the past few decades.[10] Thus, effective information sharing among coalition members provides a valuable shared asset.[11]

3 Military coalitions (including alliances, joint task forces, and multinational forces) are established on a permanent basis by treaty, or to address a specific strategic objective. *See* U.S. Joint Chiefs of Staff, JP 3-0, Joint Operations (Oct. 22, 2018); U.S. Joint Chiefs of Staff, JP 3-08, Interorganizational Cooperation (Oct. 12, 2016).

4 S.C. Res. 1546 (June 8, 2004). *See also* Maryanne Lawlor, *Iraqi Communications Transition from Tactical to Practical*, Signal, Nov. 2004.

5 Protocol to the Treaty of Peace of Mar. 26, 1979, arts. 29–31, Egypt-Isr., Aug. 3, 1981, https://mfo.org/documents-and-downloads.

6 David Doukhan, *Multinational Joint Task Force (MNJTF) against Boko Haram*, Int'l Inst. for Counter-Terrorism, May 1, 2020, https://www.ict.org.il/Article/2640/Multinational_Joint_Task_Force_against_Boko_Haram_Reflections#gsc.tab=0.

7 *See* Charter of the Association of Southeast Asian Nations, Nov. 20, 2007, https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf.

8 Permanent Structured Coop., https://pesco.europa.eu/ (last visited Jan. 12, 2022) [hereinafter PESCO].

9 *Operations and Missions: Past and Present*, NATO, Sept. 10, 2021, https://www.nato.int/cps/en/natolive/topics_52060.htm.

10 In many other non-military contexts, IS also constitutes a widely recognized measure for inter-organizational, inter-sectoral, and inter-governmental data exchange that is relevant to the resolution of a common challenge. *See* Deborah Housen-Couriel, *Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace*, *in* Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace 39–63 (Scott Shackelford et al. eds, forthcoming 2022).

11 Mario Scerala, John Ahmet Erkoyuncua & Essam Shehaba, *Identifying Information Asymmetry Challenges in the Defence Sector*, 19 Procedia Mfg. 127 (2018); Charles Phillips, T.C. Ting & Steven Demurjian, *Information Sharing and Security in Dynamic Coalitions*, SACMAT '02: Proceedings of the Seventh ACM Symp. on Access Control Models & Tech., June 2002.

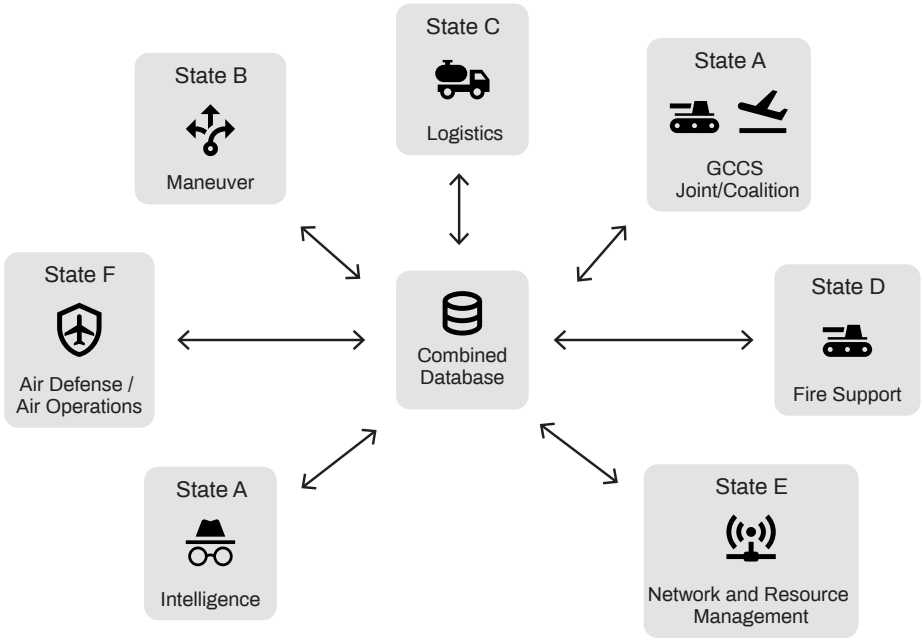

Figure 1. Combined Operations Information Sharing. Based on C. Phillips, T.C. Ting & S. Demurjian, INFORMATION SHARING AND SECURITY IN DYNAMIC COALITIONS (2002) at 89

In parallel with its criticality, digitized data sharing among coalition members presents both operational and legal challenges, and our analysis herein focuses on two of the latter, in particular.[12] The first legal challenge is that of ensuring the "legal interoperability" of coalition members' activities, defined by the International Committee of the Red Cross (ICRC) as "a way of managing legal differences between coalition partners with a view to rendering the conduct of multinational operations as effective as possible, while respecting the applicable domestic law constraints of coalition members."[13] The management of these "legal differences" has until now focused chiefly on issues of international humanitarian law (IHL). We will briefly explore herein some of the ways in which IHL interoperability has been traditionally managed by coalitions, as a basis for the principal analysis of the second legal challenge.

This next challenge focuses on the coordination—and, ultimately, the interoperability—of coalition members' domestic regimes for the

12 The analysis does not address, for example, the important issue of the operative necessity to provide confidentiality of coalition IS as a matter of military field security.

13 INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 32 (2011), www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf [hereinafter ICRC CHALLENGES].

protection of personal data privacy, where such personal data is defined as any identifier "such as a name, an identification number, location data, an online identifier or… one or more factors specific to [an individual's] physical, physiological, genetic, mental, economic, cultural or social identity."[14]

While these two issues both require the coordination of legal and policy constraints among coalition members, the data privacy challenge is a relatively new one in the military context. This is because domestic personal data privacy safeguards have come to the fore in an unprecedented way in recent years, introducing stringent regulatory requirements for the use of data by both private and public organizations in many national and regional jurisdictions. We argue here that data privacy protections can no longer be ignored in military contexts, as military bodies are in fact public organizations that process large quantities of combatants' sensitive personal data; and that information sharing in coalitions thus requires coordination of members' domestic law regimes which currently mandate data privacy protections and safeguards for combatants as data subjects.

B DATA PRIVACY VULNERABILITY ON MILITARY COALITION PLATFORMS: WHAT'S THE PROBLEM?

Vulnerabilities in the use, storage, and transmission ("processing") of combatants' personal data on coalition platforms exist in both the *operational* and *legal* contexts. We address the operational vulnerabilities first, as they highlight the underlying justification and need for addressing the legal vulnerabilities and exposures.

The *operational vulnerabilities* exposed by military coalitions' processing of personal data of military personnel are illustrated by the 2015 Ferizi data breach incident. In March 2015, the Islamic State Hacking Division and Cyber Khalifat hacking group published "kill lists" of U.S. military personnel and their families, based on personal data these groups received

14 This is the definition of "personal data" in Article 4 of European Union Regulation 2016/679 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, 3016 O.J. (L 119) arts. 4, 32 [hereinafter GDPR]. The same definition appears in Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001; Decision No 1247/2002/EC, 2018 O.J. (L 295) [hereinafter Institutional GDPR].

from Ardit Ferizi, a Kosovo-based hacker. Ferizi had hacked into the servers of a civilian company that contained information outsourced by the military, accessing the names, addresses, and photos of approximately 1,300 U.S. soldiers on active duty, as well as personal details about their families. These terrorist groups published the exfiltrated data, calling for attacks on the listed personnel and threats against them and their families, warning:

> [W]e are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the *khilafah*, who soon with the permission of Allah will strike at your necks in your own lands![15]

Other such leaks of personal data of military personnel that have been made public include the exposure of 12,000 U.S. military reservists' data in the New York area in 2010,[16] the publication of thousands of troops' information via the Strava fitness app in 2018,[17] the breach of 200,000 personal data files at the U.S. Defense Department in February 2020,[18] and the June 2021 hack of more than 1,182 UK Special Forces personnel whose personal data was leaked from the WhatsApp commercial platform.[19] It should be noted that not all such data leaks have involved a military "digital adversary": some have been caused by the unprotected sharing of personal data inside military organizations, data breaches of military suppliers' systems, and the unsupervised utilization of non-military, commercial digital platforms by military personnel.[20] Nevertheless, such increasingly frequent leaks underscore the potential operational risks

15 *See ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison*, US DEP'T JUSTICE, Sept. 3, 2016, https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison; and Josh Constine, *ISIS "Cyber Caliphate" Hacks U.S. Military Command Accounts*, TECHCRUNCH, Jan. 12, 2015, https://techcrunch.com/2015/01/12/cyber-caliphate/. Ferditi was convicted to 20 years in prison for providing material support to terrorist groups through unauthorized computer access.

16 Martin Evans, *Army Warns Reservists of Identity Theft Threat*, NEWSDAY, Apr. 22, 2010, https://www.newsday.com/news/new-york/army-warns-reservists-of-identity-theft-threat-1.1876244.

17 Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, GUARDIAN, Jan. 28, 2018.

18 *See* Kevin Collier & Mosheh Gains, *Likely Military Data Breach May Have Compromised Service Members' Personal Information*, NBC NEWS, Feb. 20, 2020, 3:39 PM, https://www.nbcnews.com/tech/security/dod-communications-hub-reports-likely-data-breach-n1140071.

19 The leaked data included details of 1,182 recently promoted troops as well as personnel in sensitive units such as the Special Reconnaissance Regiment. *See* Gareth Corfield, *UK Special Forces Soldiers' Personal Data Was Floating Around WhatsApp in a Leaked Army Spreadsheet*, REGISTER, June 2, 2021, https://www.theregister.com/2021/06/02/uk_special_forces_data_breach_whatsapp/.

20 This is the case with the WhatsApp leak; see *id.* The overlapping of military and civilian digital identities of coalition troops, a key issue for future research, is revisited in the conclusion.

stemming from the unmanaged, unrestricted, and unprotected use of combatants' personal data.[21]

It is admittedly difficult to ascertain whether similar attacks on coalition IS platforms have occurred and compromised combatants' personal data, as such breaches are not likely to be publicized. Yet such cyber attacks, which present an operational threat through the exposure of combatants' personal data, are openly recognized as an ongoing vulnerability in the overall security of coalition operations.[22]

Although coalition cyber security controls and cyber risk-mitigation processes are beyond the present scope of analysis, these measures remain an ever-present background concern when considering mechanisms to protect personal data in coalition operations. This is because the safeguarding of personal data privacy is inherently connected to the cyber security of the computerized systems in which such data is stored, processed, and transmitted. Moreover, domestic and regional data privacy regimes regularly incorporate such controls and processes. For example, the well-known European Union's General Data Protection Regulation (GDPR) and its ancillary regulation applicable to governmental entities (the Institutional GDPR)[23] both require organizations to implement "technical and operational measures." These include widely recognized technological cyber security controls such as encryption; protocols for data confidentiality, integrity, availability, and resilience; system audits; data minimization; and access management as necessary aspects of the safeguarding of data privacy.[24] The GDPR and Institutional GDPR regimes will be further explored herein as leading contemporary examples of the regulatory safeguarding of individuals' data privacy rights.

Thus, it is argued that data privacy vulnerabilities have *operational implications* for coalition activities, chiefly with respect to the sensitivity

21 Moreover, the cyber security vulnerabilities of high-security governmental and military platforms are well-known, and attacks on such targets are no longer rare events. Examples include the 2014 hacks of the U.S. Department of Homeland Security and the U.S. military's Transportation Command, the 2015 hack of Germany's Bundestag, the 2017 exposures of Singapore and South Korea's ministries of defense, the 2019 attacks on Iranian missile launch systems, and the 2021 attack on the Ukrainian naval forces.

22 For example, NATO's June 2021 Brussels Summit Communique states that "Resilience and the ability to detect, prevent, mitigate, and respond to vulnerabilities and intrusions is critical.… NATO as an organisation will therefore continue to adapt and improve its cyber defences." *See* Press Release, NATO, Brussels Summit Communique, June 14, 2021, § 32, https://www.nato.int/cps/en/natohq/news_185000.htm. *See also* Robin Geiss & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INT'L L. STUD. 556, 557–59 (2021); Heather Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISR. L. REV. 39, 41 (2015).

23 GDPR, *supra* note 14; Institutional GDPR, *supra* note 14.

24 GDPR, *supra* note 14, art. 32; Institutional GDPR, *supra* note 14, art. 33. *See also* Protection of Privacy Regulations (Data Security), 5777-2017 (Isr.), https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf; California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.40 (a)(3)(A), (j)(1)(c), (ag)(1)(d) (West 2019).

of external exposure of combatants' personal data. Technical and operational safeguards of data privacy that are, as a rule, required by domestic regimes should be fully synchronized and merged with similar measures that may already be in place on IS platforms.[25]

The legal vulnerabilities and exposures with respect to personal data constitute a new aspect of coalition information sharing. Recent years have seen rapid growth in the regulation of personal data privacy. As stated above, the European Union's GDPR governing private sector entities is a leading example of a regional regime—bolstered by the accompanying Institutional GDPR applicable to governmental entities. All 30 of the EU and European Economic Area member States have incorporated both regulatory measures into national "GDPR laws." In addition, approximately 90 other countries[26] have legislated data privacy regimes, often bolstered by vigorous enforcement mechanisms that include financial and administrative sanctions.[27] Such safeguards are also included in the data privacy policies of several international organizations, including the United Nations and its specialized agencies, the OECD, and the ASEAN.[28] While these regulatory developments have not yet established a binding international standard for data privacy protection,[29] the wide adoption of key provisions makes them relevant to the analysis of coalition IS, and we review them below in Part I.

25 IS for coalition operations is, of course, governed by additional cyber security and military field security requirements beyond those included in data privacy regimes. *See supra* note 12. Further study is needed of the confluence of these requirements with data privacy "technical and organizational measures."

26 *See Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdataprotection.com/ (last visited Jan. 12, 2022).

27 *See International Association of Privacy Professionals (IAPP)*, GLOBAL PRIVACY AND DATA PROTECTION ENFORCEMENT DATABASE, https://iapp.org/resources/global-privacy-and-data-protection-enforcement-database/ (last visited Sept. 24, 2021).

28 Alexander Beck & Christopher Kuner, *Data Protection in International Organizations and the New UNHCR Data Protection Policy: Light at the End of the Tunnel?* EJIL: TALK! Aug. 31, 2015. *See also Privacy Policy*, OECD, https://www.oecd.org/privacy/ (last visited Jan. 12, 2022); *ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows*, PERSONAL DATA PROTECTION COMM., https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows (last visited Jan. 12, 2022). Examples of regional treaties include the Council of Europe's Convention for the Protection of Individuals with Regard to the Processing of Personal Data and the African Union Convention on Cyber Security and Personal Data Protection. *See* Comm. of Ministers, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, 128th Sess., https://edoc.coe.int/en/international-law/7729-convention-108-convention-for-the-protection-of-individuals-with-regard-to-the-processing-of-personal-data.html; African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, 56 I.L.M. 166.

29 For an assessment of the current state of data privacy protections under international law in general, and international human rights law in particular, see Ana Beduschi, *Rethinking Digital Identity for Post-COVID-19 Societies: Data Privacy and Human Rights Considerations*, 3 DATA & POL'Y 15 (2022); and Kirby Abbott, *A Brief Overview of Legal Interoperability Challenges for NATO Arising from the Interrelationship Between IHL and IHRL in Light of the European Convention on Human Rights*, 96 INT'L REV. RED CROSS, no. 893, Mar. 2014, at 107.

Although less immediately obvious than the operational challenges, the legal vulnerabilities caused by insufficient protections for data privacy are also critical for coalitions. Despite the widespread adoption of similar legal safeguards, domestic regimes differ in their substantive definitions of data privacy.[30] Take the example of one member's law forbidding a person with a background of specified illnesses to use certain weapons, and another's forbidding the sharing of such medical information. Another example is the differences in the legality of mapping the geolocation of combatants who are on leave from active service. Such instances are critical to the viability of coalition operations, yet they increasingly reflect differences of approach to privacy issues at the national level.

C STRUCTURE

The structure of the chapter proceeds as follows. Part I briefly reviews the concept of legal interoperability for joint operations, beginning with IHL interoperability and deriving some principles for data privacy using an analysis of the GDPR and Institutional GDPR regimes. Part II provides a case study of NATO's coalition IS, including some current data privacy developments. Finally, in the chapter's conclusion it is proposed that, due to the present state of data privacy regulation at both the domestic and international levels, coalition members should be bound to apply privacy protections in accordance with their respective domestic regimes, as they share combatant information via IS platforms.

30 *See* Mary Sanford & Taha Yasseri, *The Kaleidoscope of Privacy: Differences across French, German, UK and US GDPR Media Discourse* (Working Paper arXiv:2104.04074, 2021), https://arxiv.org/pdf/2104.04074.pdf; Eugenia Ha Rim Rho, Alfred Kobsa & Carolyn Nguyen, *Differences in Online Privacy & Security Attitudes based on Economic Living Standards: A Global Study of 24 Countries* (26th European Conference on Information Systems, Research Paper No. 95, 2018), https://eugeniarho.com/wp-content/uploads/2019/10/ECIS-rho.pdf.

I
APPLICABLE LEGAL REGIMES AND LEGAL INTEROPERABILITY

A THE RATIONALE FOR LEGAL INTEROPERABILITY OF COALITION OPERATIONS

The rationale for ensuring the legal interoperability of military coalitions is based not only on rule-of-law considerations, but also on the practical interests of coalition participants. Goddard succinctly summarizes this confluence:

> [I]ndividual States may be responsible in law for some, though not necessarily all, of the activities conducted under the auspices of a coalition of which they are a part. As a result, each coalition member has a particular interest in satisfying itself, to its own standards, as to the lawfulness of the conduct for which it may be held responsible. Because the legality of conduct attributable to a State must be considered in light of that State's own legal obligations, substantive legal differences can arise between coalition members [and] the members may differ in how they interpret those obligations and how, or even if, they are to be fulfilled. Therefore, while taking account of legal differences is an important component of legal interoperability, **the challenge ultimately concerns the need for States to protect their own legal interests**, while minimizing the impact on the effectiveness of operations.[31]

States' "own legal interests" are, of course, wide-ranging. The analysis in this section focuses on the challenges of legal interoperability in coalitions, beginning with IHL and then deriving some implications for data privacy regimes.[32]

31 David Goddard, *Understanding the Challenge of Legal Interoperability in Coalition Operations*, 9 J. NAT'L SEC. L. & POL'Y 211, 212 (2017) (emphasis added).

32 On this point, see also ICRC CHALLENGES, *supra* note 13; and Marten Zwanenberg, *International Humanitarian Law Interoperability in Multinational Operations*, 95 INT'L REV. RED CROSS, no. 891/892, Dec. 2013, at 681.

B LEGAL INTEROPERABILITY IN COALITION OPERATIONS FOR IHL: TRADITIONAL APPROACHES AND THE CURRENT DEBATE

Military coalitions operate under complex, multilayered legal frameworks. Even where coalition members agree on operational objectives, they may disagree about the legal classification of the conflict—for instance, whether a given conflict should be defined as international or non-international, humanitarian assistance or border security, or one of the "new forms of conflict, for which there may be no ready characterization."[33] In addition to differences in the applicability of specific treaty obligations, States also adopt diverse approaches to their interpretations of IHL, such as the determination of the necessity of joint military actions, the choice of targets, and the classification of certain individuals as combatants. Goddard concludes that:

> even where States' substantive [IHL] obligations are the same, there is still significant latitude for divergence in the positions they adopt. Such differences may not be… known—or even knowable—in advance of a particular operation. However, they ultimately lead to situations where specific conduct may be deemed lawful by some States within a coalition, but unlawful by others.[34]

To address these gaps, mechanisms have evolved for the coordination and management of coalition members' diverse legal positions regarding IHL. For instance, members may specifically agree on applicability and interpretation in the documentation authorizing operations. They may declare national "caveats," which reflect IHL interpretations that restrict one member's troops' actions without constraining other members.[35] In cases where national interpretations of IHL are incompatible, coalition members may "red-flag" operations or their own troops' participation in them.[36] One example of the acuteness and relevance of the academic and practitioner debate around IHL interoperability is the NATO International Security Assistance Force (ISAF) coalition operations

33 Laurie R. Blank, *Complex Legal Frameworks and Complex Operational Challenges: Navigating the Applicable Law Across the Continuum of Military Operations*, 26 EMORY INT'L L. REV. 87, 87 (2012).
34 Goddard, *supra* note 31, at 228. *See also* Zwanenberg, *supra* note 32 (providing several examples).
35 Marius Frost-Nielsen, *Conditional Commitments: Why States Use Caveats to Reserve Their Efforts in Military Coalition Operations*, 38 CONTEMP. SEC. POL'Y 371 (2017).
36 Steven Hill & David Lemetayer, *Legal Issues of Multinational Military Operations: An Alliance Perspective*, 55 MIL. L. & L. WAR REV. 13 (2016).

in Afghanistan. At the height of coalition operations, more than 130,000 troops from 51 countries participated in extended and varied operations on the basis of a number of UN Security Council resolutions.[37] Although some of the previously mentioned interoperability mechanisms were employed, conflicts of IHL interpretation among coalition participants were ongoing and included, *inter alia*, the rules on detention of combatants and non-combatants,[38] targeting,[39] and rules of engagement.[40]

Thus, the current debate around IHL interoperability is by no means settled. Both scholars and practitioners remain concerned about the potential effects of gaps in both the pragmatics and the legitimacy of coalition operations.[41] A central element of the controversy is the applicability of international human rights law during armed conflicts (including the data privacy rights of the adversary's combatants and civilians), either as part of IHL, as *lex specialis*, or in parallel with IHL, in accordance with combatants' domestic law regimes. This important topic is set aside for the purposes of the present analysis. Nevertheless, the mechanisms which have developed for legal interoperability have already become integral to coalition management. We now explore their relevance for managing coalition diversity in the context of data privacy.

C DATA PRIVACY PROTECTIONS APPLICABLE TO COALITION OPERATIONS

The applicability of data privacy safeguards on the part of military organizations in wartime provides a special case of the IHL interoperability issues touched on in the previous section.[42] Data privacy rights under IHL for the adversary's combatants and civilians will be examined briefly. However, current gaps in the interpretation of this issue are complex and preclude IHL's reliable safeguarding of these rights at present. Our core analysis thus focuses on data privacy protections that lie *outside of IHL*: those rights enjoyed by coalition combatants as data subjects of

37 *See ISAF's Mission in Afghanistan (2001–2014)*, NATO, Aug. 19, 2021, 14:41, https://www.nato.int/cps/en/natohq/topics_69366.htm.

38 Marco Sassòli, *The International Legal Framework for Stability Operations: When May International Forces Attack or Detain Someone in Afghanistan*? 39 ISR. Y.B. H. RTS. 177 (2009).

39 Michael N. Schmitt, *Targeting and International Humanitarian Law in Afghanistan*, 39 ISR. Y.B. H. RTS. 99 (2009).

40 Robin Geiss & Michael Siegrist, *Has the Armed Conflict in Afghanistan Affected the Rules on the Conduct of Hostilities?* 93 INT'L REV. RED CROSS, no. 881, March 2011, at 11.

41 Hill & Lemetayer, *supra* note 36; Goddard, *supra* note 31; Zwanenberg, *supra* note 32.

42 *See* Patrick Mello, *National Restrictions in Multinational Military Operations: A Conceptual Framework*, 40 CONTEMP. SEC. POL'Y 38, 49 (2019) (analyzing structural, procedural and operational restrictions on interoperability, he categorizes national legal constraints as "structural").

their respective national data privacy regimes, using the GDPR and the Institutional GDPR as sample regulatory paradigms.

1 *IHL and Data Privacy for Adversary's Combatants and Non-Combatants: Current Gaps*

The current legal guidance on the impact of personal data privacy regulation on the conduct of armed conflict is minimal. Several scholars have recently analyzed aspects of personal data privacy under IHL as it applies to an adversary's combatants and civilians (e.g., combatants' families, civilian casualties, NGO personnel).[43] For instance, in reviewing the ICRC's database of customary IHL, Asaf Lubin has concluded that, at present, this authoritative source "excludes any real mention of privacy within the 161 rules it identifies as constituting the common core of humanitarian law binding on all parties to all armed conflicts today" and that "[s]uch lack of regulation is troubling."[44] He proposes that "the pace of technological innovation is outmatching the intellectual stamina and regulatory capacities of IHL rule-prescribers and rule-appliers" and that a review of the relationship of IHL to data privacy rights "is long overdue."[45] Geiss and Lahmann concur.[46]

Furthermore, data privacy analysis under IHL so far has focused on non-combatants' rights and their potential abuses by belligerents, such as a ransomware attack against a hospital that leaks non-combatants' personal health data; belligerents' surveillance of their adversary's civilian email communications; and the ongoing collection of biometric data at military checkpoints from the civilian population by an occupier.[47] These examples exclusively implicate the privacy rights of the

43 *See, e.g.*, Geiss & Lahmann, *supra* note 22; HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION (Christopher Kuner & Massimo Marelli eds., 2d ed. 2020); Adriana-Maria Sandru & Daniel-Mihail Sandru, *Humanitarian Law and Personal Data Protection*, 18 PANDECTELE ROMANE 58, 58–66 (2018) (Romanian); Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES 464 (Robert Kolb, Gloria Gaggioli & Pavle Kilibarda eds., 2022).

44 Lubin, *id.*, at 464.

45 *Id.*

46 Geiss & Lahmann, *supra* note 22 ("A complete collapse of privacy during armed conflict, as a consequence of adversarial military cyber operations, would be a paradigm shift of how wars are fought and could in principle conceivably lead to a paralysis of the targeted civilian society at large").

47 *See id.*; MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 189–90 (2017); Lubin, *supra* note 43, at 483–86. In a troubling example of a violation of non-combatants' privacy rights, reports indicate that U.S. military officials supplied the Taliban with a list of "American citizens, green card holders and Afghan allies" to expedite the evacuation of those individuals from Afghanistan in the wake of the U.S. withdrawal in autumn 2021. However, this undoubtedly violated the data privacy of civilians in a life-threatening context. *See* Lara Seligman, Alexander Ward & Andrew Desiderio, *U.S. Officials Provided Taliban with Names of Americans, Afghan Allies to Evacuate*, POLITICO, Aug. 26, 2021, https://www.politico.com/news/2021/08/26/us-officials-provided-taliban-with-names-of-americans-afghan-allies-to-evacuate-506957.

adversary's non-combatants under IHL. The privacy protections that might be required for a belligerent's own combatants *in bello*, including coalition operations, have been largely unexplored.

2 *Combatants as Data Subjects under National Data Protection Laws*

Coalition combatants are not only subject to their country's interpretation and application of IHL in the context of their military conduct: they also act under the jurisdiction of their nation's domestic laws, including those relating to personal data privacy. Moreover, examples are emerging of the adoption of formal privacy policies for national armies that sharpen the status of combatants as subjects of such domestic privacy laws.[48]

The GDPR regime that is used as a basis for the present analysis is founded on an understanding of the right of the individual (the "data subject") to personal data protections as a matter of his or her fundamental human rights and dignity.[49] These include consent to the use, storage, and transfer ("processing") of personal data by commercial and governmental entities. Processing must be secure, in accordance with specific technical and organizational measures such as encryption and access management (referred to in the introduction to this chapter). These measures must be transparent to data subjects, who have the right to correct and delete information and to object to certain types of processing.[50] They also enjoy options for remedying any abuse of these rights, including the right to lodge a complaint with supervisory authorities, the right to an effective judicial remedy, and the right to compensation where organizational liability for the breach of privacy rights has been established. These and other data subject rights are all supported by robust enforcement mechanisms, including heavy fines for organizations' violation of mandated safeguards, be they private or governmental entities.[51]

Data subject rights under GDPR-type privacy protection regimes are, of course, not absolute. A full review of the instances where these rights

48 Two instances are the UK's Ministry of Defence Privacy Notice, which applies to all personal data processed by the Army's Personnel Campaign Office for all defense functions and "maintaining and administering Her Majesty's Armed Forces" (https://www.gov.uk/government/publications/ministry-of-defence-privacy-notice/mod-privacy-notice); and the Australian Government's Ministry of Defense Privacy Policy (May 2021), https://www.defence.gov.au/sites/default/files/2021-03/Defence-Privacy-Policy.pdf (Austl.). The U.S. Department of Defense's Data Strategy does not directly mention personal data privacy: it addresses "data interoperability" with coalition members, stating: "Properly exchanging data between systems and maintaining semantic understanding are critical for successful decision-making and joint military operations." U.S. DEP'T OF DEFENSE, EXECUTIVE SUMMARY: DoD DATA STRATEGY 8 (2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

49 GDPR, *id.*, recitals 1, 2, 4.

50 GDPR, *supra* note 14, ch. 3, "Rights of the data subject."

51 For the liability of governmental entities, see Institutional GDPR, *supra* note 14, art. 66.

are limited or superseded is beyond the scope of the present article. However, examples in which processing of personal data by an organization remains lawful without the need for data subject consent include law enforcement (criminal investigations), where required by statute (reporting to tax authorities), and where an overriding public interest exists. Military activities, including coalition tasks, may also permit exemptions from safeguards, but they are by no means completely excluded from the applicability of data privacy rules, as we shall explore in the following section.

3 *The Case of GDPR/Institutional GDPR Applicability to Military Uses of Combatants' Personal Data*

At this juncture, we turn to an analysis of the GDPR and Institutional GDPR applicability to the processing of military coalition combatants' personal data, where coalition member states are also members of the EU and thus bound by these two regulatory measures. The outcome clarifies which military coalition activities fall under their ambit (and, as relevant, the national GDPR laws transposing them) to safeguard combatants' personal data. These include NATO treaty obligations of EU member States (including coalition operations), some additional multilateral coalition operations, European Defense Agency activities, and EU permanent structured military and security cooperation (see examples below). Figure 2 provides a schematic matrix of the textual analysis herein.

At first glance, there is an explicit exemption from GDPR applicability to the processing of personal data by military bodies. Article 2(2), in establishing the material scope of the GDPR, states that the regulation does not apply to processing for "…activities which fall within the scope of Chapter 2 of Title V of the [Treaty of the European Union, or TEU]," the chapter which addresses common EU foreign and security policy.[52] Thus military entities which process combatants' personal information within the framework of this common policy—for example, in UN peacekeeping missions, collective self-defense operations under Article 51 of the UN Charter, and humanitarian and rescue tasks—are ostensibly exempt from GDPR provisions.

Yet, notably, that is not the case. In circumstances in which EU governmental authorities, including military entities, are the data controllers, Article 2(3) of the GDPR explicitly transfers the bulk of its data

52 Consolidated Version of the Treaty on European Union arts. 23–46, Oct. 26, 2012, 2012 O.J. (C 326) 1 [hereinafter TEU].

protection safeguards to the complementary Institutional GDPR regime.[53] The legal effect is to in fact *ensure* privacy protections for data processing by military entities, even under the abovementioned TEU provisions.

Thus, the Institutional GDPR takes up the applicability-to-coalition-combatants issue where the GDPR has left off. It applies data privacy protections to activities listed under TEU Articles 42(2)-(7), 45, and 46,[54] including:

- The framing of a common EU defense policy
- NATO treaty obligations (including coalition operations)
- EU civilian and military capabilities for implementing the common security and defense policy (including some multinational forces)
- European Defense Agency (EDA) operations, and
- EU permanent structured military and security cooperation (PESCO) operations.

Examples of such activities are the EDA development of a human resources management software tool for EU missions and operations,[55] an airborne medical evacuation program;[56] and PESCO projects for a joint mobile military transport coordination hub, a European Medical Command, and military command (operating "either independently or in cooperation with NATO").[57] Further emphasizing the applicability of the Institutional GDPR to the above coalition operations, the EDA's organizational privacy policy specifies that it processes personal data in accordance with the Institutional GDPR, while its privacy statement details GDPR-based data subject rights with respect to the personal data processed by the EDA.[58]

53 "For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 [superseded by the Institutional GDPR] applies." *See* GDPR, *supra* note 14, art. 2(3).

54 The Institutional GDPR excludes some specified types of common EU foreign and security policy missions. The exempted missions under TEU Articles 42(1), 43, and 44 are: Article 42(1), "missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter"; and Articles 43 and 44, "joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, [and] tasks of combat forces in crisis management"; and related joint "tasks."

55 EUR. DEF. AGENCY, FACT SHEET: J1 FUNCTIONAL AREA SERVICE, July 10, 2017, https://eda.europa.eu/docs/default-source/eda-factsheets/2017-07-10-factsheet_j1fas.

56 EUR. DEF. AGENCY, FACT SHEET: AIRMEDEVAC, Feb. 6, 2019, https://eda.europa.eu/docs/default-source/eda-factsheets/2019-02-06-factsheet-airmedevac.

57 PESCO, *supra* note 8. Asked about data protection policies for these programs, a PESCO project official responded that "…the interactions between Member States via email in the project follow normal procedures, where data protection is ensured." Email with PESCO Project Official (Oct. 8, 2021) (on file with author).

58 *See Data Protection*, EUR. DEF. AGENCY, https://eda.europa.eu/who-we-are/how-we-work/data-protection (last visited Sept. 14, 2021).

Applicability Issue for Combatants who are EU Data Subjects	Conclusion/Outcome	GDPR	Institutional GDPR
Definition of "personal data"	Identical GDPR and Institutional GDPR definitions	Art. 4(1)	Art. 3(1)
Applicability in general	The GDPR does not apply when EU "institutions, bodies, offices and agencies," including military entities, process personal data of combatants. The Institutional GDPR applies.	Art. 2(3)	Arts. 2(1) and 3
Institutional GDPR applicability to EU data subjects who are combatants	The Institutional GDPR applies to the framing of a common EU defense policy, NATO treaty obligations (incl. coalition operations), EU civilian and military capabilities (incl. some multinational forces), EDA operations, and PESCO operations.	–	TEU Arts. 42(2)–(7), 45, 46
Exceptions to Institutional GDPR applicability to EU data subjects who are combatants	The exempted missions in Arts. 42(1), 43, and 44 TEU include peacekeeping missions outside the EU; joint disarmament operations; humanitarian, rescue, military advice and assistance tasks; tasks relating to conflict prevention, peacekeeping, crisis management; and additional joint tasks	–	Art. 2

Figure 2. Schematic Analysis of the Interaction between the GDPR and Institutional GDPR with respect to Combatants' Personal Data Protection

This applicability of the Institutional GDPR to some EU combatants thus provides an example of a non-military data privacy regime that specifically extends its safeguards into the context of joint military operations,[59] including NATO coalition operations, which are reviewed as a case study in the following section.

59 The practical application of these safeguards is still developing. *See, e.g.*, Sebastian Cymutta, *Biometric Data Processing by the German Armed Forces during Deployment*, CCDCOE (2021). With respect to future regulatory developments, see TEU, *supra* note 52, art. 39 (establishing that "the [EU] Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data" for security and defense activities which are presently exempted).

II
THE NATO CASE STUDY FOR COALITION INFORMATION SHARING: CURRENT DATA PRIVACY CHALLENGES

A OPERATIONAL INTEROPERABILITY FOR INFORMATION SHARING IN NATO COALITIONS

Information sharing among NATO coalition members constitutes an integral part of the organization's mission.[60] It takes place within the overarching, NATO-wide coordination of members' forces that is implemented on an ongoing basis,[61] through the adoption of a wide variety of technical interoperability standards and other measures to support common missions.[62] NATO coalitions provide an especially interesting challenge to data privacy interoperability, as coalition members are subject to diverse domestic regimes: not only the EU regimes reviewed above but also, *inter alia*, the U.S.'s Health Insurance Portability and Accountability Act of 1996 (HIPAA),[63] Canada's Personal Information and Protection and Electronic Documents Act (PIPEDA),[64] and Turkey's Law on Personal Data Protection of 2016.[65]

Interoperability specifications for information sharing are established via the adoption by all coalition members of NATO Interoperability Standards and Profiles (NISP).[66] Members submit the standards and technical specifications required by each national military force, which are then merged into a common NISP prescribing "the necessary technical standards and profiles to achieve interoperability of Communications and

60 Szilveszter Szeleczki, *Interpreting the Interoperability of NATO's Communication and Information Systems*, 24 SCI. BULL., June 2019, at 95.
61 Hill & Lemetayer, *supra* note 36.
62 Paddy Larkin & Jan Bartels, *A Foreign Perspective on Legal Interoperability*, ARMY LAW., no. 2, 2020, at 40.
63 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1939 (1996) [hereinafter HIPPA].
64 Personal Information and Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.) [hereinafter PIPEDA].
65 Law on Personal Data Protection, Law No. 6698, Official Gazette 29677 (Mar. 24, 2016) (Turk.) [hereinafter TURKEY LPDP].
66 NATO, ADATP-34, 1 NATO INTEROPERABILITY STANDARDS AND PROFILES: INTRODUCTION (M. ed. 2020) [hereinafter NISP 1]; NATO, ADATP-34, 2 NATO INTEROPERABILITY STANDARDS AND PROFILES: AGREED INTEROPERABILITY STANDARDS AND PROFILES (M. ed. 2020) [hereinafter NISP 2]; NATO, ADATP-34, 3 NATO INTEROPERABILITY STANDARDS AND PROFILES: CANDIDATE INTEROPERABILITY STANDARDS AND PROFILES (M. ed. 2020) [hereinafter NISP 3].

Information Systems in support of NATO's missions and operations."[67] This technical coordination is mandatory.[68]

Thus, NATO promotes *operational interoperability* among coalition members, creating and maintaining a collaborative coalition information system.[69] The interoperability is an iterative process: an annual revision is prescribed,[70] and ad hoc Requests for Change can be made by coalition members, should their national requirements change.[71] Hundreds of NISP standards have been instituted through this process: a key example is the Secure Communications Interoperability Protocol.[72]

Several NISP standards also have clear implications for personal data privacy. These include the standards for Biometrics Data Interchange, Watchlisting and Reporting;[73] Captured Persons, Materiel and Documents;[74] Machine Readable Travel Documents;[75] Geolocation API Specification;[76] Authentication Methods and Security Mechanisms;[77] Definition of the inetOrgPerson LDAP Object Class;[78] and User Location.[79] All of these types of IS require the coalition members to process personal data, either of NATO coalition combatants, adversary combatants, or both. However, their *legal interoperability* is not explicitly addressed as part of the NISP process.[80] A turning point is approaching that will require a more transparent NISP or other NATO process for coordination of domestic law privacy mandates, driven partially by the Covid-19 pandemic. Recently, NATO has developed IS capabilities in tracking pandemic breakouts among combatants that may affect coalition capabilities—an example to which we will return below.

67 This takes place in accordance with Alliance C3 Strategy (Ref. C-M(2014)0016) all NATO Enterprise (ref. C-M(2014)0061)).
68 NISP 1, *supra* note 66, at 3, Provision is also made for conflict resolution (at 1).
69 NISP 2, *supra* note 66, at 3.
70 *Id.* at 8.
71 These interoperability standards and profiles must support NATO's Consultation, Command and Control (C3) interoperability and related "common funded Communication and Information Systems… including their development and operations." NISP 1, *supra* note 66, at 8.
72 NATO, Secure Communications Interoperability Protocol, Mar. 3, 2017, https://nisp.nw3.dk/standard/nato-acomp-5068-ed.a-v2.html.
73 NATO, Biometrics Data, Interchange, Watchlisting and Reporting, Oct. 4, 2013, https://nisp.nw3.dk/standard/nato-aedp-15-ed.a-v1.html.
74 NATO, Captured Persons, Materiel and Documents, Aug. 8, 2007, https://nisp.nw3.dk/standard/nato-ajp-2.5-ed.a.html.
75 Machine Readable Passport (2008), ISO/IEC 7501-1:2008, https://www.iso.org/standard/45562.html.
76 *Geolocation API Specification* (W3C Working Draft, 2021), https://www.w3.org/TR/geolocation/.
77 Internet Eng'g Task Force (IETF), Lightweight Directory Access Protocol (2006), RFC 4513:2006, https://www.ietf.org/rfc/rfc4513.txt.
78 Internet Eng'g Task Force (IETF), Definition of inetOrgPerson LDAP Object Class (2000), RFC 2798:2000, https://www.ietf.org/rfc/rfc2798.txt. "LDAP" refers to a Lightweight Directory Access Protocol that enables data location for individuals, groups and other resources on a given network.
79 Joe Hildebrand & Peter Saint-Andre, *XEP-0080: User Location* (v.1.9, 2021), https://xmpp.org/extensions/xep-0080.html.
80 *See id.* at 9, 17 (noting the criterion for approval of non-NATO standards: "Some key criteria for inclusion of non-NATO standards… [are f]reedom from legal issues").

B NATO LEGAL INTEROPERABILITY IN THE IHL CONTEXT: RAMIFICATIONS FOR DATA PRIVACY

Colonel Kirby Abbott, who has served as assistant legal adviser at NATO's military headquarters, writes that "[t]here is no NATO doctrinal definition of 'legal interoperability'" beyond the ability of NATO States to work together in an operation.[81] Abbott argues that while such interoperability has been possible in the past, the present challenges of members' legal diversity with respect to their IHL and international human rights law requirements make such harmonized cooperation unfeasible and "will [eventually] hinder operational interoperability."[82] Other observers concur with Abbot's assessment.[83]

This is a troubling lacuna. The mechanisms for bridging legal gaps among members via caveats and red flags, discussed in Part I above, allow for a certain degree of legal interoperability, but they are unsatisfactory in the long term, as they skew the assumption of operational risk to the detriment of coalition members whose troops are fully engaged with the joint mission. This shortcoming is also indicative of the difficulty facing coalitions for the implementation of the legal interoperability of personal data privacy protections. In fact, as shown above, NATO has not yet incorporated data privacy protections into the NISP database of operational standards at the organizational level. Yet the current diversity of coalition members' legal constraints is wide: the 30 NATO member countries include 21 EU members, three additional countries that implement the GDPR and the Institutional GDPR, and six countries with non-GDPR data privacy laws: Albania,[84] Canada,[85] Montenegro,[86] North Macedonia,[87] Turkey,[88] and the United States.[89] The range of regulatory requirements contained in these national laws, including the scope of any exclusions for military personnel that may be engaged in coalition activities, constitutes a substantive legal challenge for NATO and its members.

81 Abbott, *supra* note 29, at 111.
82 *Id.*
83 *See id.*; Jerrod Fussnecker, *The Effects of International Human Rights Law on the Legal Interoperability of Multinational Military Operations*, ARMY LAW., no. 5, May 2014, at 7; Victor Tunon, *State Responsibility in NATO for the ECHR and Its Effect on Legal Interoperability*, Dec. 31, 2019 (Master's thesis, Uppsala University), https://core.ac.uk/display/328383615.
84 Law No. 9887 on Protection of Personal Data (Mar. 10, 2008) (Alb.).
85 PIPEDA, *supra* note 64.
86 Law on Protection of Personal Data, Official Journal of Montenegro, nos. 79/2008, 70/2009, 44/2012, 22/2017.
87 Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia, no. 42/20.
88 TURKEY LPDP, *supra* note 65.
89 HIPPA, *supra* note 63 (relating to personal health data, as there is no U.S. federal data privacy law).

The time is fast approaching for NATO to address its legal responsibility for mapping and incorporating these variations into its coalition IS platform. This necessity is highlighted by a relevant recent example of NATO coalition members' engagement with a specific data privacy issue—as in so many other contexts, because of the Covid-19 pandemic. In October 2020, the organization adapted its Health Information System at the full scale of coalition operations to promote "medical situational awareness" (e.g., monitoring combatants for Covid-19 infection). Concurrently, the Allied Joint Doctrine for Medical Communications and Information Systems was also adopted by all NATO member States,[90] requiring that personal data use be minimized, based on a risk assessment that explicitly balances "privacy, [UK] Caldicott, GDPR and security considerations."[91] The Doctrine adds that IS "is likely to be constrained by the national medical privacy regulations."[92] Currently, the creation of an all-NATO electronic treatment record for combatants has been delayed, pending the coordination of the privacy requirements of all coalition members.[93]

This recent, Covid-19-related example is cogent. Although it has not prompted formal caveats or red flags, NATO's explicit recognition of GDPR and other national privacy provisions as a constraint on the processing of combatants' personal medical data indicates, at the very least, a growing organizational awareness of the need for legal interoperability for the sharing of such data. This is a key development worth monitoring.

CONCLUDING REMARKS: DATA PRIVACY CHALLENGES POSED BY THE INCREASING DIGITIZATION OF WARFARE

Several points emerge from this analysis of legal interoperability as an inherent aspect of coalition information sharing. For IHL interoperability, necessity has been the mother of invention: coalitions have produced mechanisms such as national caveats that allow, however imperfectly, for a diversity of legal positions on the applicability of IHL while enabling

90 AJMedP-5, Allied Joint Doctrine for Medical Communications and Information Systems (B ed. 2020).
91 *Id.* n. 21.
92 *Id.* ¶ 5.4.b.
93 *Id.* 24.

joint operations. For data privacy safeguards, substantive legal diversity is now presenting a strategic challenge.[94] The NATO case study is indicative, as the sharing of pandemic-related personal health data of combatants becomes a more transparent and critical coalition issue.

We have argued that the present state of personal privacy regulation at both the domestic law and international levels requires coalition members, in sharing combatants' information, to apply personal data protections in accordance with their respective domestic privacy regimes. This imperative is notwithstanding the need to resolve the inherent legal ambiguity at the nexus of IHL, international human rights law, and national data privacy protections for coalition IS platforms. This overarching issue awaits further work.

Moreover, present trends signal the increasing complexity and sensitivity of combatants' digital identities, such as the overlapping of their military and civilian digital personas and the tracking of pandemic-related behavior. Perhaps most daunting are the future types of combatant data that may be shared on coalition IS platforms: deep biometrics (DNA, haptics, and olfactory information); and a synthesis of combatants' military status, tasks, and behavior, including their digital behavior on social media and other non-military platforms (already seen in the Strava hack).[95] Even digital tracking of specific combatants' use of digitized weaponry and the identities of those whom they have targeted may become identifiable and thus shareable.

Beyond the typology of personal data into the future—and its operational and legal vulnerabilities— coalition IS platforms should continue to develop robust technical and operational measures to protect all aspects of information sharing. As the legal accountability and overall effectiveness of such platforms continue to develop and mature, so will the incentives for coalition members' trusted sharing of information, including combatants' personal data, to meet mission tasks and goals.

94 ICRC CHALLENGES, *supra* note 13; and Zwanenberg, *supra* note 32.
95 *See* Hern, *supra* note 17; and Geiss & Lahmann, *supra* note 22.

Chapter 12

Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study

Asaf Lubin[1]

INTRODUCTION

On 16 February 2022, Robert Mardini, the Director-General of the International Committee of the Red Cross (ICRC) issued an open letter in which he apologized for failing to adequately protect the servers that stored the personal data of over 515,000 people worldwide.[2] This cyber attack first began on 9 November 2021 and involved a nation State that exploited a known but unpatched vulnerability in a web-based office communications management program that the Red Cross was internally using for

1 Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law and a Fellow at IU's Center for Applied Cybersecurity Research. He is additionally an Affiliated Fellow at Yale Law School's Information Society Project, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a visiting Scholar at the Hebrew University of Jerusalem Federmann Cyber Security Research Center.

2 *Statement: ICRC cyber-attack: Sharing our analysis*, ICRC (Feb. 16, 2022) https://www.icrc.org/en/document/icrc-cyber-attack-analysis [hereinafter: ICRC Cyberattack Statement]

work purposes.[3] Those impacted by the attack included "missing people and their families, detainees and others receiving services from the Red Cross and Red Crescent Movement as a result of armed conflict, natural disasters, or migration."[4] Once inside the system the hackers installed web shells to carry out "post-exploitation activities," which included among other things "compromising administrator credentials, moving throughout the network, and exfiltrating registry and domain files."[5] Following the incident the ICRC launched a campaign to notify victims of the data breach by the use of "phone calls, hotlines, public announcements, letters and in some cases in-person visits to remote communities."[6]

The cyber attack on the ICRC's servers highlights the importance of implementing and enforcing data protection and cybersecurity standards in the work of international organizations (IOs). These entities engage in a wide variety of data collection and processing work, that is only likely to increase in scope and volume in the years to come, and which includes personally indefinable information and confidential and sensitive materials. As Buchan and Tsagourias noted, "maintaining the confidentiality of this information is critical to enabling the IO to discharge its tasks and achieve its objectives."[7] This is especially true in the context of humanitarian action where "poor information management may spark violence and discrimination… may lead to stigma and ultimately threaten the actors' reputation, putting both employees and beneficiaries at risk."[8]

As this chapter will discuss, while some IOs have developed and put in place data protection frameworks, the practice is far from uniform. Even more troubling, the IOs that have introduced such frameworks have not done so out of a sense of an international legal obligation. Rather, data protection is introduced as a best practice or out of market or reputational demands. This chapter will explain why such a construction is

3 Carly Page, Red Cross says "state-sponsored" hackers exploited unpatched vulnerability, Tech Crunch (Feb. 16, 2022), https://techcrunch.com/2022/02/16/red-cross-links-january-cyberattack-to-state-sponsored-hackers/.

4 *See* ICRC Cyberattack Statement, *supra* note 2.

5 *See* Page, *supra* note 3.

6 *See* ICRC Cyberattack Statement, *supra* note 2. *See also* ICRC RULES ON PERSONAL DATA PROTECTION, Art. 20: Data Breaches (updated and adopted by the ICRC Assembly on Dec. 19, 2019) ("(1) Any breach of security leading to the accidental or unlawful destruction, loss or alteration of — or to the unauthorized disclosure of, or access to — Personal Data transmitted, stored or otherwise processed must always be reported to the ICRC Data Protection Office; (2) The persons affected must be notified of a Data Breach by the Staff in Charge, in close coordination with the Data Protection Office, without undue delay when the Data Breach puts them at particularly serious risk…") [hereinafter: ICRC RPDP].

7 Russell Buchan and Nicholas Tsagourias, *Hacking International Organizations: The Role of Privileges and Immunities*, ARTICLES OF WAR (Dec. 14, 2021), https://lieber.westpoint.edu/hacking-international-organizations-privileges-immunities/.

8 Theodora Gazi, *Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR*, 5 J. INT'L HUMANITARIAN ACTION 1 (2020),

problematic for the further development of international data protection law applicable in both war and peace.

While this chapter focuses on the ICRC as a case study, its arguments extend beyond this important organization. The past two decades have seen a large number of IOs voluntarily adopting data protection regimes, frameworks, and statements, including: The UN International Organization for Migration (IOM),[9] the UN Office of the High Commissioner for Refugees (UNHCR),[10] the UN World Food Programme (WFP),[11] the United Nations Office for the Coordination of Humanitarian Affairs (OCHA),[12] Oxfam,[13] and Médecins Sans Frontières (MSF).[14] While these organizations should be commended for their pioneering data protection work, all of them have failed to explicitly opine on whether international law constrains their data collection and processing practices. As a result, legal ambiguity remains as to the extent to which the practices of these IOs are sufficient, by themselves, to generate customary norms and expectations of behavior that could govern the actions of other IOs and non-State actors.

This brief chapter follows a two-part structure. Part I focuses on the needs for data protection frameworks in the work of humanitarian actors and further highlights the core framework that governs the data processing work of the ICRC. Part II shifts the discussion to the challenge

9 IOM was "one of the first international organizations to develop its own internal guidance concerning data protection, the IOM Data Protection Principles in 2009." *See* Data Protection, IOM, https://www.iom.int/data-protection. In 2010 the IOM released an even broader articulation of its data protection standards as part of the IOM Data Protection Manual (2010). The IOM was further a member of the UN Privacy Policy Group (UN PPG), which released the UN Principles on Personal Data Protection and Privacy. These principles were adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018. The principles bind all members of the UN system and represent a high-level framework for the processing of personal data.

10 *See* UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR (May, 2015), https://www.refworld.org/pdfid/55643c1d4.pdf; See also, UNHCR Guidance on the Protection of Personal Data of Persons of Concern to UNHCR (Aug. 2018), https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=5b360f4d4. Since producing these two overarching documents, the UNHCR has been one of the most prolific in generating specialized data protection principles to address key aspects of its work. For example, consider the UNHCR Procedural Standards for Refugee Status Determination under UNHCR's Mandate (Aug. 2020), https://www.unhcr.org/4317223c9.pdf.

11 *See* WFP Guide to Personal Data Protection and Privacy: Principles and operational standards for the protection of beneficiaries' personal data in WFP's programming (June, 2016), https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

12 *See* OCHA Center for Humanitarian Data, OCHA Data Responsibility Guidelines (Oct. 2021), https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/60050608-0095-4c11-86cd-0a1fc5c29fd9/download/ocha-data-responsibility-guidelines_2021.pdf.

13 *See Responsible Program Data Policy* (Feb. 17, 2015), https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=A1F3301F89806B21BA1F5EB6F708DFAE?sequence=1.

14 *See MSF Privacy and Personal Data Protection policy* (Jan. 22, 2019), https://msfaccess.org/privacy-and-personal-data-protection-policy.

of holding IOs accountable for potential privacy and data protection violations. This part explores both the general challenge of holding non-State actors responsible for protecting and ensuring human rights law, and the more specific concern in applying data protection rules as a matter of a customary international legal obligation applicable to IOs. The chapter concludes by briefly discussing the importance of recognizing data protection as an international legal obligation. This conclusion therefore recommends that all IOs adopt data protection frameworks and that they explicitly state that they have done so out of a sense of a binding international legal rule.

I
DATA PROTECTION IN HUMANITARIAN ACTION AND AT THE ICRC

The International Red Cross and Red Crescent Movement brings together the ICRC and 192 National Red Cross and Red Crescent Societies as well as their International Federation. As the largest humanitarian network in the world, it has a global reach. The ICRC alone has 20,000 staff working in over 100 countries.[15] The organization's work is based on the Geneva Conventions of 1949 and their Additional Protocols of 1977 as well as on the Movement's statutes and the resolutions of the International Conferences of the Red Cross and Red Crescent. Its core mandate is to ensure "humanitarian protection and assistance for victims of armed conflict and other situations of violence" by promoting "respect for international humanitarian law and its implementation in national law."[16]

To achieve this mandate in the digital age the ICRC relies on extensive data collection, processing, storage, and dissemination. As Figure 1 demonstrates, this is prevalent across every aspect of the work undertaken by the ICRC and its sister societies: from the use of data analytics and artificial intelligence to predict emergencies and allocate resources for disaster relief, through the use of cash transfer programs and biometrics collection in the management of facilities for refugees and asylum-seekers, all the way to the use of drones and social media applications in

15 *See* ICRC, *The International Red Cross and Red Crescent Movement*, https://www.icrc.org/en/who-we-are/movement.
16 *See* ICRC, *Mandte and Mission*, https://www.icrc.org/en/who-we-are/mandate.

Figure 1. Use Cases for Humanitarian Data Processing. Source: HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION 16-17 (C. Kuner & M. Marelli eds., 2nd ed., 2020).

the collection of evidence of abuses of rules of international humanitarian law (IHL).

The 37th International Conference of Data Protection and Privacy Commissioners, which convened in Amsterdam in 2015, adopted a resolution on privacy and international humanitarian action. In their Explanatory Statement the Commissioners described the increased need for both data in humanitarian action and rules to protect it:

> Identifying people and personal data processing are an integral part of the performance of the mission of humanitarian actors. The introduction of technology increases the number, nature and flow of data collected. In particular, this data is used to improve knowledge of beneficiaries, strengthen the effectiveness of humanitarian action and be accountable to beneficiaries. This trend may be beneficial if properly framed through privacy and data protection guarantees. However, if not properly framed, it could jeopardize human rights protection…
>
> Specific privacy and security risks are identified, including the potential for development of monitoring systems, which could

> be increased by technologies such as management information systems and electronic transfers; digital identity registration and biometrics, mobile phones but also drones. Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally.

Strong data protection regimes and protocols will thus often complement and reinforce humanitarian action. On occasion, however, there may be "instances of friction" between the two. In such cases IOs will need to rely on "specific working procedures" to "justify derogations from the principles and rights" recognized under personal data processing regimes.[17] In other words, data protection frameworks should be seen as checks on IOs' effective execution of their mandates. When an IO introduces a new data-intensive practice into its sphere of operations, such practice should not result in counterproductive situations or undue risk of digital abuse or physical harm. After all, humanitarian actors are expected to follow the "do no harm" principle and to endeavor not to cause any further damage or suffering as a result of their activities.[18]

Against this backdrop it is perhaps surprising to learn that the ICRC only recently incorporated data protection norms and standards throughout the organization. The ICRC's Rules on Personal Data Protection (hereinafter: RPDP) were adopted in 2015 and, at the time, were one of the first comprehensive sets of data protection rules ever developed by a large humanitarian organization. The framework was meant to enable the ICRC "to remain at the forefront of international humanitarian action."[19]

The framework itself echoes and mirrors parallel regional and international data protection regimes. It generates a set of institutions within the ICRC with authority and capacity to ensure effective implementation

17 *See* HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION 29 (C. Kuner & M. Marelli eds., 2nd ed., 2020) [hereinafter: DATA PROTECTION HANDBOOK].

18 *See generally*, Jean Martial Bonis Charancle & Elena Lucchi, *Incorporating the Principle of "Do No Harm": How to Take Action Without Causing Harm: Reflections on a Review of Humanity & Inclusion's Practices* (Oct. 1, 2018), https://www.alnap.org/system/files/content/resource/files/main/donoharm_pe07_synthesis.pdf.

19 *See* ICRC RPDP, *supra* note 6, at 2.

(including a Data Protection Office and a Data Protection Commission).[20] It further establishes a set of principles to be followed by the ICRC in the conduct of its work:

1. Lawful, Fair, and Transparent Processing.[21]
2. Requirements for Specification and Minimization of Data.[22]
3. Requirements for Adequate and Relevant Data Storage.[23]
4. End-to-End Safeguards around Retention, Deletion, and Archiving.[24]
5. Data Subject Rights to Information, Access, Correction, Objection, Deletion, and in the context of Profiling.[25]
6. Data Protection Impact Assessments and Documentation Requirements.[26]
7. Specialized Rules for Data Breaches, Data Security, and Data Transfers.[27]

Within the limits of this chapter, I am unable provide a detailed account of this framework. Overall, however, the rules are designed "to reduce the risk of unauthorized use or access to personal data" by requiring the ICRC to follow "a 'data protection by design' approach."[28] Such an approach seeks "to minimize the collection of personal data to that which is necessary for the operation and ensure that data subjects' rights are respected."[29]

20 *Id.*, at 25-27 (Articles 26-28).
21 *Id.*, at 5-6 (Articles 1-2).
22 *Id.*, at 6 (Article 3).
23 *Id.*, at 7 (Articles 4-5).
24 *Id.*, at 8 (Article 6).
25 *Id.*, at 11-15 (Articles 7-14).
26 *Id.*, at 18 (Articles 17-18).
27 *Id.*, at 19-23 (Articles 20-25).
28 *Q&A: Humanitarian operations, the spread of harmful information and data protection: In conversation with Delphine van Solinge, the ICRC's Protection Advisor on Digital Risks for Populations in Armed Conflict, and Massimo Marelli, Head of the ICRC's Data Protection Office*, 102 Int'l Rev. Red Cross 27, 34 (2020).
29 *Id.*

II
THE CHALLENGE OF HOLDING IOS ACCOUNTABLE FOR DATA PROTECTION VIOLATIONS

In 2018 the Brussels Privacy Hub and the Data Protection Office of the ICRC joined forces to produce a "Handbook on Data Protection in Humanitarian Action." The handbook, now in its second edition, was produced with the desire to serve as a "useful tool to raise awareness and assist humanitarian organizations in complying with personal data protection standards."[30] The handbook was "inspired by a wide variety of data protection instruments"[31]—including the RPDP—"without being based solely on any single one of them."[32]

The handbook was explicit in suggesting that IOs are shielded from any meaningful domestic obligations concerning data protection. In the view of the editors, IOs "enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence and are not covered by the jurisdiction of the countries in which they work. They can therefore process Personal Data according to their own rules, subject to the internal monitoring and enforcement of their own compliance systems; in this regard they constitute their own 'jurisdiction'."[33]

The ICRC therefore does not consider itself bound by any domestic legal obligation to employ data protection standards. Any norms internalized are voluntary, non-binding, and reflective of "recognized best practices."[34] The ICRC further invites other international humanitarian organizations to follow this interpretive guidance. The ICRC therefore strongly believes that IOs' privileges and immunities should trump any external accountability or legal enforcement. Article 19 of the RPDP is in fact clear about that. While it does not preclude the possibility of cooperation with national or regional data protection authorities (DPAs), the Article simultaneously affirms that the ICRC "cannot be compelled to

30 Data Protection Handbook, *supra* note 17, at 11.
31 Christoper Kuner & Massimo Marelli, *Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian action*, EJIL: Talk! (July 13, 2017), https://www.ejiltalk.org/creating-international-frameworks-for-data-protection-the-icrcbrussels-privacy-hub-handbook-on-data-protection-in-humanitarian-action/.
32 *Id*.
33 Data Protection Handbook, *supra* note 17, at 35.
34 *Id*.

disclose any information acquired while carrying out its work."[35] Instead of relying on external bodies like DPAs or local courts, the ICRC created the Data Protection Commission as the authority responsible to interpret the RPDP and to render decisions about their implementation, in particular in the context of arbitrating complaints by data subjects.[36]

It should be noted that the question of the applicability to IOs of domestic and regional data protection regimes, like the European General Data Protection Regulation (GDPR), is far from settled. "There is little precedent dealing with whether EU data protection law can apply to IOs" as these questions have "not arisen often in practice."[37] At least some scholars take the position that the application of these regimes to IOs "cannot be automatically excluded."[38]

Even assuming *arguendo* that IOs' privileges and immunities supersede any domestic application of data protection rules, such exclusion does not extend to international obligations. This is a crucial point so far ignored in prior discourse. All of the IOs who have produced internal data protection regimes have so far failed to address two crucial questions: (1) To what extent does data protection constitute a human right that is reflective of customary international law; (2) assuming that it is, could the obligations derived from that right extend to non-State actors, such as IOs.

Both of these points are highly controversial. As I have written elsewhere:

> Differences in legal cultures and perceptions mean there is still a lack of international consensus about basic questions of privacy and data protection, and there is still considerable fragmentation concerning core principles that govern this space. As such there is difficulty to verify the existence of any one principle as reflective of custom as a matter of "general practice accepted as law" under Article 38(1)(B) of the ICJ Statute.[39]

In other words, it is at least an ongoing question whether we can even articulate the right to data protection as a customary human right of relevance for our analysis. That said, it is certainly a possibility that over

35 *See* ICRC RPDP, *supra* note 6, at 18 (Article 19).
36 *Id.*, at 27 (Article 28).
37 Christopher Kuner, *International Organizations and the EU General Data Protection Regulation*, 16 Int'l Org. L. Rev. 158, 187 (2019).
38 *Id.*, at 188.
39 Asaf Lubin, *The Rights to Privacy and Data Protection under IHL and HRL*, in Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives 463, 475 (Robert Kolb, Gloria Gaggioli, & Pavle Kilibarda eds., 2022).

time the obligation could crystallize as more and more nations adopt data protection as a mandatory legal framework. Let us therefore proceed for the sake of argument with the assumption that the right to data protection is, or might become in the future, a right of customary character.

Even then, there will be a set of challenges applying the right to the ICRC as an IO. International human rights law (IHRL) generally places primary obligations on States. IOs "are rarely formal parties to human rights treaties, which usually address states and are drafted with the characteristics of states in mind."[40] Surely UN organs, which are bound by the Charter might be required to comply with human rights obligations as they are derived from the Charter.[41] Other human rights obligations might be considered *jus cogens* and therefore binding on all IOs. Data protection as a right, however, does not seem to be a good contender for a *jus cogens* status. Nor can data protection meaningfully be described as an obligation neatly derived from the general and vague commitments to human rights enshrined under the Charter.

More progressive interpretations of the human rights obligations of IOs do exist. These interpretations cite to "evolving practice in the Security Council and in the reports of some special rapporteurs"[42] which "increasingly consider that under certain circumstances non-State actors can also be bound by international human rights law and can assume, voluntarily or not, obligations to respect, protect, and fulfil human rights."[43] In any event, the point of this brief discussion is only to demonstrate the doctrinal complexity of trying to rely on international law, namely on customary rules of IHRL, to further cement the obligations of IOs to proactively produce and effectively enforce data protection standards in both peacetime and in war.

As a matter of future and evolving law there can be no question that a better articulation of IOs customary obligations, particularly in the data protection space, is of increasing importance. IOs now play a core function in our cotemporary world order. These organizations "effectively reflect transnational concerns and in turn strengthen the sense of global, human interdependence… creating an alternative world, one that

40 Gerald L. Neuman, *International Organizations and Human rights – The need for Substance*, Harvard Law School Human Rights Program Research Working Paper Series, (Apr. 2019), http://hrp.law.harvard.edu/wp-content/uploads/2019/04/Gerald-Neuman_HRP-19_001.pdf.

41 The preamble to the UN Charter speaks of "fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small." Article 1(3) similarly speaks of international cooperation "promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion."

42 UN Office of the High Commissioner for Human Rights, International Legal Protection of Human Rights in Armed Conflict 24 (2011).

43 *Id*.

is not identical with the sum of sovereign states and nations."[44] From a normative perspective surely international law should be imbued with the power to prevent gaps in legal coverage generated by the growth in scope and size of IOs. After all, States should not be allowed to create IOs to do their bidding which are then free from customary law or human rights obligations. In this regard there seems to be signs that courts are prepared to apply custom to non-State actors as a *general* international law that is sufficiently comprehensive to bind all actors on the international plane (although they may not be subject to the full gamut of legal rights and duties applicable to States).[45] This trend of expanding the reach of international custom to cover IOs should extend, where possible and relevant, to the areas of digital rights, informational privacy, data protection, and cybersecurity.

CONCLUSION: A CALL TO RECOGNIZE DATA PROTECTION AS AN INTERNATIONAL OBLIGATION ON IOS

At least one commentator has suggested that as IOs' data protection policies "become more widely adopted, they may lead to the gradual crystallization of international law."[46] This position would be true only if IOs adopted these data protection standards out of a sense of an international legal obligation. IOs, however, have so far treated data protection merely as a non-binding best practice.

44 Akira Iriye, Global Community: The Role of International Organizations in the Making of the Contemporary World 7 (2002).

45 *See e.g. Nevsun Resources Ltd v Araya* [2020] Supreme Court of Canada 5, para 107 (noting that "international law has so fully expanded beyond its Grotian origins that there is no longer any tenable basis for restricting the application of customary international law to relations between States."); *Reparations for Injuries in the Service of the United Nations*, Advisory Opinion, ICJ Rep. (1949) 174, 178 (noting that "the subjects of law in any legal system are not necessarily identical in their nature or in the extent of their rights, and their nature depends on the needs of the community."). For a broader reading see Robert McCorquodale, *An Inclusive International Legal System*, 17 Leiden J. Int'l L. 477 (2004).

46 Christopher Kuner, *The Internet and the Global Reach of EU Law*, *in* EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law 112, 131 (Marise Cremona & Joanne Scott eds., 2019) (referring in the immediate footnote that follows specifically to the possibility of crystallization of customary norms).

This book centers around the proposition that countries need to develop more robust international data protection legal regimes for wartime. Yet, if the ICRC—the primary IO whose mandate it is to promote respect for IHL—is unable to publicly declare that data protection is a customary human right of global enforcement, why should we ever expect States to do so?

United Nations organs and the ICRC are role models and are expected to lead by example. They set the tone that could ultimately usher in the progressive development of the law in the direction of enhanced digital rights and humanitarian protection of data. It is simply not enough therefore for the ICRC, and for parallel organizations, to merely "talk the talk" of data protection by adopting internal rules that they fully control and enforce without any sense of an external legal obligation to do so.

The growth of the datasphere generates new opportunities and complex legal and ethical challenges for the management of digital humanitarian spaces. For data protection regimes to offer an effective compass in traversing this new legal terrain, their role as a binding compass must first be recognized. The ICRC and other IOs must play their part in advancing the new agenda for wartime data protection by reaffirming their own legal commitments and obligations to the evolving international rule of law controlling in this area.

Digital Rights in the *Jus Post Bellum*

Chapter 13

The Investigation of Grave Crimes: Digital Evidence, the Right to Privacy, and International Criminal Procedure

Kristina Hellwig[1]

INTRODUCTION

International criminal courts and tribunals (ICTs) have been entrusted with the crucial but demanding task of prosecuting the most serious crimes in the fight against impunity. Technology has the potential to support this endeavor by providing valuable information. Since digital devices and new technologies have become integral parts of military operations and everyday civilian life, there is an ever-growing amount of digital data[2] with evidentiary value.[3] Therefore, digital evidence,[4] such as sat-

1 Lecturer, Hamburg University, Germany.
2 Hereinafter "data."
3 *See, e.g.*, Lindsay Freeman, *Law in Conflict: The Technological Transformation of War and Its Consequences for the International Criminal Court*, 51 N.Y. UNIV. J. INT. LAW POLITICS, 808, 860–61 (May 2019); Sean E. Goodison, Robert C. Davis & Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, http://www.rand.org/pubs/research_reports/RR890.html (last visited Nov. 29, 2021).
4 A commonly used definition is that "[e]lectronic evidence is any data resulting from the output

ellite imagery, communication data, drone footage, and user-generated content (such as videos and photography), is becoming an essential tool in the fact-finding process.[5]

Interestingly, the use of such evidence is not entirely new. For example, at the International Criminal Tribunal for the Former Yugoslavia (ICTY), the Prosecution introduced aerial images provided by the U.S. military as evidence for the Srebrenica massacre.[6] Similarly, the introduction of videos, photographs, and other types of digital evidence is becoming common before the International Criminal Court (ICC) as well.[7] Recently, the ICC's Prosecution presented videos originally shared on social media, allegedly showing executions carried out by Mahmoud al-Werfalli[8] to prove its case. The Special Tribunal for Lebanon's Prosecutor also made use of video footage, special algorithms, and telecommunication data to determine the parameters of an explosion and connected actors in the *Ayyash* case.[9]

With the prevalence of new technologies and current developments in the fact-finding community, this trend will continue, and the role of digital evidence will likely increase. As technology develops, so does the way States and armed groups operate, especially in times of war. They utilize advanced technologies for law enforcement, military, and intelligence purposes,[10] thus producing large amounts of data with evidentiary value.[11] Given recent breakthroughs in robotics, machine learning, AI, and autonomous weapons, this development is unlikely to change.[12] Additionally, as social platforms and the World Wide Web are also utilized

of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using any electronic device. [And] [d]igital evidence is that electronic evidence that is generated or converted to a numerical format." *See, e.g.*, European Commission, *European Evidence Project, European Data Informatics Exchange Framework for Courts and Evidence*, http://www.cordis.europa.eu/project/id/608185/reporting/de (last visited Nov. 29, 2021); Maria A. Biasiotti et al., *Introduction: Opportunities and Challenges for Electronic Evidence, in* HANDLING AND EXCHANGING ELECTRONIC EVIDENCE ACROSS EUROPE, 3, 4 (Maria A. Biasiotti et al. eds., 2018). For a different proposal, see, for example, Burkhard Schafer & Stephen Mason, *The Characteristics of Electronic Evidence, in* ELECTRONIC EVIDENCE, 18, 19 (Daniel Seng & Stephen Mason eds., 4th ed. 2017). For an analysis of the characteristics of digital evidence, see Kristina Hellwig, *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings*, INT. CRIM. L. R. (Advanced Articles 2021).

5 For an analysis of the evolution of digital evidence in ICL, see, for example, Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDH. INT. L. J. 283, 291–307 (2018).

6 Prosecutor v. Krstić, IT-98-33-T, Judgment, ¶¶ 114, 223, 229 et seq., 250 (ICTY Aug. 2, 2001); Prosecutor v. Popović et al., IT-05-88-T, Judgment, ¶¶ 73–75 (ICTY June 10, 2010).

7 *See, e.g.*, Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2842, Judgment pursuant to Article 74 of the Statute, ¶ 93 (Mar. 14, 2012).

8 Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Public Warrant of Arrest, ¶¶ 11–22 (Aug. 15, 2017) [hereinafter Al-Werfalli].

9 Prosecutor v. Ayyash et al, STL-11-01/T/TC, Judgment, at 107–11, 512–86, 605–39 (Aug. 18, 2020).

10 *See generally* Simone M. Friis, *"Beyond Anything We Have Ever Seen": Beheading Videos and the Visibility of Violence in the War against ISIS*, 91 INT. AFF. 725 (July 2015).

11 For more details, see, for example, Freeman, *supra* note 3; Goodison et al., *supra* note 3.

12 *E.g.*, Warren Chin, *Technology, War and the State: Past, Present and Future*, 95 INT. AFF. 765, 772 et seq. (July 2019); Freeman, *supra* note 3, at 813.

by some armed groups and States to spread propaganda, radicalize, or broadcast atrocities,[13] evidence of these actions exists in a digital format. For instance, ISIS uploaded videos showing beheadings,[14] which could serve as evidence in future trials, as is already evident by the social-media-derived evidence that has been introduced in *Al-Werfalli*.[15]

The growing importance of digital evidence is also spurred by civil society and NGOs. The fact-finding community has taken advantage of current technological developments within their documentation efforts,[16] allowing for an increase in third-party involvement[17] and open-source investigation.[18] Various activities, such as collecting, securing, analyzing, cataloging, and publishing large amounts of data on core crimes,[19] are carried out by NGOs, particularly for the purpose of enabling future criminal proceedings.[20]

Given the increase in digital information and its use as evidence, as well as the sheer volume of information being collected by various actors, the question arises as to what role the right to privacy plays in the investigation of core crimes and before ICTs in general. Thus, this chapter will attempt to provide an inventory of the right to privacy in international criminal procedure (ICP) with special regard to digital evidence and will address the role of ICTs in the protection of this right. While this topic is of paramount importance to all criminal tribunals dealing with core crimes, this inquiry will focus primarily on the ICC and use its procedural

13 *See, e.g.*, Freeman, *supra* note 3, at 833–34; *see generally*, Friis, *supra* note 10.
14 *E.g.*, Freeman, *supra* note 3, at 834; Friis, *supra* note 10.
15 Al-Werfalli, *supra* note 8, ¶¶ 11–22.
16 *E.g.*, Susann Aboueldahab & Inês Freixo, *App-Generated Evidence: A Promising Tool for International Criminal Justice*, 21 INT'L CRIM. L.R., 505, 505 et seq. (2021); Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. TRANSNAT'L. L., 1 (2018); Dia Kayyali et al., *Digital Video Evidence, When Collected, Verified, Stored and Deployed Properly, Presents New Opportunities for Justice*, ICC Forum, http://www.iccforum.com/cyber-evidence#Kayyali (last visited Nov. 29, 2021); Brianne M. Leyh, *Changing Landscapes in Documentation Efforts: Civil Society Documentation of Serious Human Rights Violations*, 33(84) UTR. J. INT'L & EUR. L. 44, 49 (2017).
17 In this context, the term "third party" refers to investigations by parties who are not directly involved in the proceedings and have no obligation to investigate, e.g., civil society organizations and NGOs.
18 Human Rights Center, UC Berkeley School of Law & UN Office of the High Commissioner for Human Rights, Berkeley Protocol, HR/PUB/20/2 (Dec. 1, 2020).
19 *See generally* Kayyali et al., *supra* note 16.
20 *See, e.g.*, the projects WITNESS (https://www.witness.org/our-work/, last accessed Jan. 22, 2022: "We coordinate with local citizens and organizations, conduct on-the-ground trainings, and provide free online resources in multiple languages"), Eyewitness (https://www.eyewitness.global/our-work, last accessed Jan. 22, 2022: "EyeWitness develops close partnerships with frontline organisations which document human rights violations that can amount to core international crimes, and with public interest litigators bringing these cases to trial"; "EyeWitness approach is based on three pillars"; "First, the… app allows you to capture photos and video that are embedded with metadata…"; "Second, when you send footage to the eyeWitness server we create a trusted chain of custody"; "Third, eyeWitness ensures the captured information is processed for justice") or Benetech (https://www.benetech.org/lab/ethical-ai-to-promote-justice/, last accessed Jan. 22, 2022: "By applying machine learning and computer vision to these videos, we hope to help them assess human rights violations and promote accountability and the rule of law in Syria and conflict settings worldwide").

rules as a case study having only limited opportunity to address the procedural perspective of the mixed tribunals. This chapter is structured as follows. Part I will focus on potential interference with the right to privacy that may occur during the investigation of core crimes. Part II will address the scope and effect of the right to privacy in ICP in general, while Part III will focus on the application of the right to privacy within the different investigative stages, focusing on the specific ICP rules of the ICC. By way of conclusion, this chapter will examine the future role that privacy rights could and should play before ICTs.

I
COLLECTING DIGITAL EVIDENCE OF GRAVE CRIMES AND POTENTIAL INTERFERENCE WITH THE RIGHT TO PRIVACY

Before analyzing the approach of ICTs regarding the right to privacy, it is necessary to at least briefly visualize how the collection of evidence on grave crimes may interfere with this right. Given how digital evidence is created, collected, and shared, an almost infinite number of scenarios are conceivable that may raise questions of the applicability and interference with the right to privacy. Thus, a complete representation will not be feasible in this chapter. However, this part will attempt to provide a general and manageable structural breakdown of what are arguably the most central groups of interventions.

Generally, privacy issues may arise during the creation or the use and processing of data. For instance, interference may occur when drone footage is recorded, video surveillance takes place, or audiovisual material is created by witnesses. Furthermore, interference may take place during the collection, storage, or transfer and sharing of such data. Gaining access to the content of data does not always require accessing the physical storage medium. It can be obtained by seizing the medium or device it is stored on but also by remote access to the data. Remote access may include sharing it via the internet, viewing the data digitally, or gaining access to the system and copying it (e.g., by interception or malware).[21]

21 *See, e.g.*, Goodison et al., *supra* note 3, at 5–8; Kayyali et al., *supra* note 16.

Additionally, as data is not bound to a single medium, it can be copied and widely disseminated rapidly.[22] In all these steps, multiple actors might take different roles, leading to new types of privacy issues. Overall, the applicable rules and standards may differ depending on the context, e.g., whether the collection was conducted during armed conflict or in peacetime.[23]

From the perspective of ICTs, digital evidence can be created by witnesses, journalists, and victims present on-site (e.g., videos or photographs of attacks or killings, mass graves or destruction of buildings) or gathered by the investigating bodies (e.g., independent investigations by the Prosecution, open-source investigation, etc.). They can also be created, collected, and provided to ICTs by a cooperating entity (e.g., States or NGOs). Which party is carrying out the measures can play a role in the determination of who can and should primarily ensure privacy protection or how far such responsibilities reach.[24] If ICTs wish to access certain data, then from a (criminal) procedural perspective, they can seek to use coercive means, such as interception or search and seizure,[25] but they may also get the data by voluntary transfer, such as by an NGO or a specific individual.[26] In general, coercive investigative measures regularly involve a privacy interference that may or may not be lawful depending on the adherence to the applicable procedural rules and national and international human rights standards. And while the determination of the applicable law can be a source of heated debate even in this more common context, the situation with voluntary disclosures is even more ambiguous. It is submitted here that interference with the right to privacy may also occur in cases where no coercive or covert means are applied and information is provided voluntarily, such as by NGOs or individuals.[27] This follows above all from the fact that the party collecting and providing the data to ICTs and the one whose privacy is affected can be different and can have contrasting standpoints. In this context, it must be asked whether, despite the fact that interference is primarily caused by others, the acceptance and use of third-party generated data by ICTs may nonetheless perpetuate the intrusion upon privacy rights. It is thus worth exploring the extent to which ICTs should take privacy rights into account in the context of such

22 *See, e.g.*, Kayyali et al., *supra* note 16.
23 *See, e.g.*, O'Connell (ch. 1 of this collection).
24 *See* Part III.A.
25 However, for the execution of coercive means, the ICT may have to rely on State cooperation. *See* Part III.A.
26 *See* Part III.
27 *See* Part III.B and the conclusion.

voluntary transfers, and the extent to which they can and should safeguard the protection of privacy rights even outside the scope of their own immediate activities.

II
GENERAL APPLICABILITY OF THE RIGHT TO PRIVACY

The right to privacy is codified in various human rights instruments[28] with broadly analogous scopes of protection, and many national constitutions and criminal codes recognize the importance of this right.[29]

By contrast, there is a lack of general reference to and recognition of this right within the ICTs' legal frameworks. It is explicitly mentioned only in the context of the rights of victims and witnesses and confidential communications.[30] During the drafting process, an interim version of the Rome Statute referred to the right and contained a provision on searches and seizures.[31] Ultimately, however, this provision was not included in the final version.[32]

However, the absence of an explicit reference does not mean that the right to privacy is not applicable before ICTs. For the ICC, this follows from Article 21 of the Rome Statute,[33] according to which internationally recognized human rights are an integral part of the applicable law, including the right to privacy.[34] And while such a rule is missing in the legal frameworks of the ad hoc tribunals, there is a strong rationale for

28 ICCPR, Art. 17; AmCHR, Art. 11; UDHR, Art. 12; ECHR, Art. 8. While the AfCHR does not refer to this right, many African constitutions and statutes do. *See* George Edwards, *International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy*, 26 YALE J. INT'L L. 324, 401–5.

29 For a detailed overview, see, for example, Edwards, *supra* note 28, at 400–5.

30 *See, e.g.*, ICTY, Rules of procedure and evidence, adopted Feb. 11, 1994, last amended July 8, 2015 [hereinafter ICTY RPE], Rule 75(A); ICTR, Rules of procedure and evidence, adopted June 25, 1995, last amended May 13, 2015 [hereinafter ICTR RPE], Rule 75(A); Rome Statute of the International Criminal Court, July 17, 1998, UN Doc. A/CONF.183/9 [hereinafter Rome Statute], Art. 57(3)(c), 68(1).

31 For a detailed illustration of the different versions of this provision, see, for example, Edwards, *supra* note 28, at 350–52.

32 Edwards, *supra* note 28, at 352.

33 Rome Statute, *supra* note 30, art. 21(3).

34 *See, e.g.*, Prosecutor v. Bemba Gombo et al., ICC-01/05-01/13, Judgment on the appeals of Mr. Jean-Pierre Bemba Gombo, Mr. Aimé Kilolo Musamba, Mr. Jean-Jacques Mangenda Kabongo, Mr. Fidèle Babala Wandu, and Mr. Narcisse Arido against the decision of Trial Chamber VII entitled "Judgment pursuant to Article 74 of the Statute," ¶ 284 (Mar. 8, 2018) [hereinafter Bemba II].

its applicability.[35] Accordingly, the ad hoc tribunals stressed that the lack of an explicit reference did not limit the need to act in conformity with recognized human rights,[36] including the right to privacy.[37] To interpret the scope of human rights, ICTs have relied on human rights jurisprudence in the past.[38] At the same time, they emphasized that this jurisprudence is not binding and that the context of international criminal law (ICL) may call for an adaptation of that scope.[39] It has been argued that some departures from domestic standards can be justified, given the *sui generis* goals of ICTs, the complexity and atrocity of the crimes they process, and the innate weaknesses of these tribunals[40] and also that, as ICL deals with crimes often committed in armed conflicts, insisting on peacetime due process standards would be unrealistic.[41]

Accordingly, due to this at least partial divergence from international human rights jurisprudence,[42] it is necessary to further analyze the different areas in which the right to privacy can be of relevance before ICTs and how the courts and tribunals apply this right in practice.

35 Arguments brought forward were, e.g., the applicability of the rules on international organizations, including human rights, references to human rights by the UN SC in their context, and the rule of law. For further details, see, for example, Lorenzo Gradoni, *The Human Rights Dimension of International Criminal Procedure, in* INTERNATIONAL CRIMINAL PROCEDURE, 74, 81 (Göran Sluiter ed., 2013); Yvonne McDermott, *The Influence of International Human Rights Law on International Criminal Procedure, in* INTERNATIONAL CRIMINAL LAW IN CONTEXT, 281 (Philipp Kastner ed., 2018).

36 *See, e.g.*, Barayagwiza v. Prosecutor, ICTR-97-19-AR72, Decision, ¶ 40 (Nov. 3, 1999).

37 *See, e.g.*, Prosecutor v. Brdjanin, IT-99-36-T, Decision on the Defence "Objection to Intercept Evidence," ¶¶ 28–29 (ICTY Oct. 3, 2003) [hereinafter Brdjanin].

38 *See, e.g.*, Situation in the Democratic Republic of the Congo, ICC-01/04-135-tEN, Decision on the Prosecution's Application for Leave to Appeal the Chamber's Decision of 17 January 2006 on the Applications for Participation in the Proceedings of VPRS 1, VPRS 2, VPRS 3, VPRS 4, VPRS 5 and VPRS 6, ¶ 34–40 (Mar. 21, 2006).

39 *See, e.g.*, Prosecutor v. Tadić, IT-94-1, Decision on the Prosecutor's Motion Requesting Protective Measures for Victims and Witnesses, ¶¶ 27–31 (ICTY Aug. 10, 1995) [hereinafter Tadić].

40 Mirjan Damaška, *The Competing Visions of Fairness: The Basic Choice for International Criminal Tribunals*, 36 2 N.C. J. INT'L L. 365, 380 (2010); Brdjanin, *supra* note 37, ¶ 63(7)–(9).

41 *Cf.* DAVID LUBAN, *Human Rights Thinking and the Laws of War, in* JENS D. OHLIN (ED.), THEORETICAL BOUNDARIES OF ARMED CONFLICT AND HUMAN RIGHTS, 45, 68 (2016).

42 For an in-depth analysis, see Amal Alamunddin, *Collection of Evidence, in* PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL JUSTICE, 231, 286 et seq., 301 et seq. (Karim A. Khan et al. eds., 2010); KRIT ZEEGERS, INTERNATIONAL CRIMINAL TRIBUNALS AND HUMAN RIGHTS LAW, 180 et seq. (2016).

III
THE PROTECTION OF THE RIGHT TO PRIVACY DURING THE INVESTIGATION

To carry out this analysis on the privacy rights approach before ICTs, this part will primarily focus on the procedural rules of the ICC, with some references to and examples from the ad hoc tribunals. The idea here is that the principles embodied in these procedural rules and the resulting problems are transferable, at least in their broad outlines, to other tribunals.

A THE PROTECTION OF THE RIGHT TO PRIVACY DURING STATE COOPERATION

Within the model of ICP, most investigative activities that go beyond voluntary cooperation with ICTs are intended to be conducted by the States obligated to cooperate.[43] In principle, this means that the collection of (digital) evidence, to the extent that disclosure is not voluntary, should be carried out by the cooperating States after a request by the ICT. For the ICC, Article 93 of the Rome Statute names various investigative measures that can be requested of Member States, including the execution of search and seizures (Article 93(1)(h)) and any other type of assistance, such as modern investigative techniques (Article 93(1)(l)).[44]

This naturally raises the question of the extent to which ICTs can influence the way the measures are carried out and thus have an impact on the observance of the right to privacy in this process. Following the general approach within ICP, as States conduct the requested measures according to their national procedure,[45] they should be mainly responsible for the protection of human rights during the execution of these

43 Rome Statute, *supra* note 30, Art. 86; S.C. Res. 827, ¶ 4 U.N. Doc. S/RES/827 (May 25, 1993); Statute of the International Criminal Tribunal for the Former Yugoslavia, S.C. Res. 827 (May 25, 1993) [hereinafter ICTY Statute], art. 29(1); S.C. Res. 955, ¶ 2, U.N. Doc. S/RES/955 (Nov. 8, 1994); Statute of the International Tribunal for Rwanda, S.C. Res. 955 (Nov. 8, 1994) [hereinafter ICTR Statute], art. 28(1).

44 ZEEGERS, *supra* note 42, at 166–67; Claus Kress & Kimberly Prost, *Article 93: Other Forms of Cooperation*, *in* ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT, 2078, 2086 (Otto Triffterer & Kai Ambos eds., 3rd ed. 2016). *See also* Rule 39(iii) of ICTY RPE, *supra* note 30, and of ICTR RPE, *supra* note 30.

45 *E.g.*, Rome Statute, *supra* note 30, art. 96 (3), 99(1).

measures, including the right to privacy.[46] However, this approach has clear shortcomings and leads to gaps in protection.[47] These gaps will be summarized here in a cursory manner. Furthermore, while ICTs are not mainly responsible for the conduct of the measures, it is possible to identify some instances where, at a minimum, it would be possible for the ICC (and the ad hoc tribunals) to consider and review the adherence to the right to privacy.

1 *Request for Cooperation*

An initial review of the measure's potential interference and compatibility with privacy rights by ICTs and their bodies could take place during the request for cooperation. However, this is not explicitly provided for in the ICT's legal framework, and some safeguards envisaged in the international human rights law (IHRL) jurisprudence are not fully applied.

In general, the ICC's Code of Conduct for the Office of the Prosecutor states that the Prosecution should respect the human rights and fundamental freedoms recognized by international law in conformity with the Statute.[48] However, as there are no public records of the requests for assistance and this rule is of a rather general nature, it is unclear which considerations are to be made before the request and how extensive any written reasoning should be.[49]

Additionally, while some authors have argued in favor of the need for a judicial warrant,[50] the ICC has not applied this approach until now.[51] Rather, the ICC emphasized that the Prosecution has independent authority to make cooperation requests under Article 93(1) Rome Statute.[52] This issue was also discussed before the ad hoc tribunals, where the tribunals have generally rejected the need for a judicial warrant approach.[53]

In addition, while the procedure regarding the formulation of the request envisaged in Article 96(2) of the Rome Statute could be utilized to weigh the conflicting interests against each other, including the rights

46 *Cf.*, Edwards, *supra* note 28, at 352 et seq.
47 For a detailed analysis, see ZEEGERS, *supra* note 42, at 113–86; Edwards, *supra* note 28, at 357.
48 ICC, Code of Conduct for the Office of the Prosecutor, Chapter 1, ¶ 8(1) (Sep. 5, 2013).
49 *See also* ZEEGERS, *supra* note 42, at 169.
50 *See, e.g.*, KAREL DE MEESTER, THE INVESTIGATION PHASE IN INTERNATIONAL CRIMINAL PROCEDURE: IN SEARCH OF COMMON RULES, 518 et seq. (2014); GÖRAN K. SLUITER, INTERNATIONAL CRIMINAL ADJUDICATION AND THE COLLECTION OF EVIDENCE, 125–28 (2002).
51 *See, e.g.*, Prosecutor v. Kenyatta, ICC-01/09-02/11, Decision on Prosecution's applications for a finding of non-compliance pursuant to Article 87(7) and for an adjournment of the provisional trial date, ¶¶ 28, 33 (Mar. 31, 2014) [hereinafter Kenyatta]; ROBERT CRYER ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE, 533 (2014); ZEEGERS, *supra* note 42, at 167.
52 Kenyatta, *supra* note 51, ¶ 33.
53 *See in detail, e.g.*, MARK KLAMBERG, EVIDENCE IN INTERNATIONAL CRIMINAL TRIALS: CONFRONTING LEGAL GAPS AND THE RECONSTRUCTION OF DISPUTED EVENTS, 252 (2013); ZEEGERS, *supra* note 42, at 153 et seq.

of those affected, there is no guarantee that such a process will take place in every case. The primary purpose of the obligation to provide certain information and reasoning is to enable the State to act under its national procedure,[54] and the rights of individuals are not explicitly mentioned.[55] And while Articles 96(2)(d) and 99(1) of the Rome Statute would allow the Court to proscribe procedural requirements, this possibility is rarely used.[56] Therefore, some authors have rightly argued that the request for State cooperation lacks sufficient and effective safeguards for the right to privacy.[57]

2 *The Execution of the Request*

There is reason to doubt the assumption that all national procedures applicable during the execution of cooperation requests uphold human rights standards and thus provide sufficient protection.[58] Even those States whose procedural rules comply with human rights in general might diverge from them in the context of State cooperation in a manner incompatible with privacy rights.

According to Article 96 of the Rome Statute, the Court must provide information on the case and the reasons for the request, such as the legal grounds and the circumstances of the case. Hence, in a best-case scenario, the State would have sufficient information to assess the request's conformity with human rights.[59] In case of non-conformity, the State could reject the request, as Part 9 of the Rome Statute gives grounds for refusal such as conflicting treaty obligations[60] or incompatibility with existing fundamental legal principles of general application.[61] Both grounds could be used to refuse investigative means contrary to human rights standards.[62]

In many cases, however, the procedure for State cooperation with the ICC, which is often conducted in a manner similar to inter-State cooperation, does not provide sufficient safeguards that at the end of the process, one of the parties, either the requestion or the executing party, will verify that the measures are compatible with human rights.[63]

54 ZEEGERS, *supra* note 42, at 169 et seq.
55 *See also id.* at 169–70.
56 *Id.* at 170–71.
57 *Id.* at 171.
58 *Id.*
59 *Id.* at 173.
60 Rome Statute, *supra* note 30, art. 97(c).
61 *Id.* art. 93(3).
62 *See, e.g.*, Kenyatta, *supra* note 51, ¶ 37; Claus Kress & Bruce Broomhall, *Implementing Cooperation Duties under the Rome Statute: A Comparative Synthesis*, *in* THE ROME STATUTE AND DOMESTIC LEGAL ORDERS, VOL. II, 515, 531 (Claus Kress et al. eds., 2005); ZEEGERS, *supra* note 42, at 172.
63 ZEEGERS, *supra* note 42, at 174; CRYER ET AL., *supra* note 51, at 534.

As some authors rightly argue, without specific legislation, there is an increased risk that cooperative States trying to support ICTs will fail to sufficiently protect human rights.[64] If requested, they might be unwilling to perform a genuine test for political reasons or due to the strength of mutual trust.[65] As a result, some States are implementing the requests without any review or special procedure.[66] Hence, even though the Rome Statute provides grounds for refusal, States may not use these means in order to attend to their duty to cooperate.[67] In addition, the human rights situation in some cooperating States makes it inappropriate to rely on them to protect human rights.[68]

3 *Ex Post Review during the Evaluation of Evidence*

One remaining option is the *ex post* review of the compatibility of measures with human rights. The procedural rules on the admissibility of evidence require such an analysis to some extent, as evidence obtained by means violating internationally recognized human rights is inadmissible if the violation casts substantial doubt on its reliability or if the admission would be antithetical to and seriously damage the integrity of the proceedings.[69] This assessment requires a determination of first, whether the evidence was obtained illegally, and second, whether this violation is sufficient to render it inadmissible.[70]

An analysis of the jurisprudence shows a positive trend, especially in the context of the ICC, towards the increasing review of alleged violations of privacy rights within the investigative stage of proceedings. For instance, when confronted with allegations that evidence was obtained illegally and in violation of the right to privacy, the ICTY often reviewed the legality in only a limited manner.[71] A frequently chosen approach was to focus on the good faith of the investigators.[72] By contrast, the ICC has developed a more detailed review. While the ICC does not elaborate on the process's compatibility with national procedure,[73] it has reviewed compliance with the internationally recognized standard of protection

64 *E.g.*, ZEEGERS, *supra* note 42, at 173–74.
65 *Id.* at 173; Kress & Broomhall, *supra* note 62, at 526 et seq.
66 ZEEGERS, *supra* note 42, at 173; Kress & Broomhall, *supra* note 62, at 526 et seq.
67 ZEEGERS, *supra* note 42, at 172.
68 *See also id.* at 173–74.
69 *See, e.g.*, ICTY RPE, *supra* note 30, Rule 95; ICTR RPE, *supra* note 30, Rule 95; Rome Statute, *supra* note 30, art. 69(7).
70 *See, e.g.*, Bemba II, *supra* note 34, ¶ 280; Brdjanin, *supra* note 37, ¶¶ 57–68.
71 *See, e.g.*, Brdjanin, *supra* note 37, ¶¶ 57–60; Prosecutor v. Haraqija et al., IT-04-84-R77.4, Decision on Morina and Haraqija Second Request for a Declaration of Inadmissibility and Exclusion of Evidence, ¶ 19 et seq (Nov. 27, 2008) [hereinafter Haraqija].
72 *E.g.*, Brdjanin, *supra* note 37, ¶ 63(1); Haraqija, *supra* note 71, ¶ 19 et seq.
73 Rome Statute, *supra* note 30, art. 69(8).

for the right to privacy and in some cases decided that there was indeed a violation of these standards.[74] However, in *Mbarushimana*, the Chamber argued that the defense had failed to provide sufficient information on the illegality of the collection of evidence and that therefore there was no burden on the Prosecution to show that the evidence was not obtained in violation of the Statute or internationally recognized human rights.[75] The Chamber also noted that there is a presumption that the investigative activities were carried out in accordance with the provisions applicable in that State. This approach of shifting the burden of proof regarding the measures' incompatibility with the applicable law is problematic. It limits the scope and extent to which the ICC assesses and takes responsibility for the way investigative measures are conducted. Furthermore, this limiting interpretation of Article 69(7) of the Rome Statute and the divergence from IHRL (according to which the defense must merely prove the occurrence of an interference and not that this interference was unlawful, which from an IHRL perspective must be proven by the State) was made without providing sufficient rationale.[76] A preferable approach was taken later on by the Appeals Chamber in *Bemba II*, where the Chamber emphasized the need to determine whether an action was in accordance with internationally recognized human rights, including whether the interference was proportionate to legitimate investigative needs.[77] The proportionality determination must take the nature of the information and the sensitivity of such data into account, and these interests must be weighed against the pursued investigative need warranting the access.[78]

The extent to which illegally obtained evidence is admitted is also pertinent because declaring such evidence inadmissible could indirectly reinforce the right to privacy for future proceedings. ICTs have brought forward different lines of argumentation for the admissibility of evidence in privacy violation circumstances.[79] For instance, the ICTY has argued that neither international law nor (a relevant number of) national legal systems prescribe the automatic exclusion of illegally obtained evidence.[80] Furthermore, a Chamber has noted that, particularly in the context of

74 *E.g.*, Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06-803-tEN, Decision on the confirmation of charges, ¶ 81 (Jan. 29, 2007) [hereinafter Lubanga]. For instance, in *Lubanga*, the Chamber found that the search and seizure of hundreds of documents and items, including correspondences, photographs, diaries, and many more, was disproportionate.
75 Prosecutor v. Mbarushimana, ICC-01/04-01/10, Decision on the confirmation of charges, ¶ 60 (Dec. 16, 2011).
76 *See also* ZEEGERS, *supra* note 42, at 178.
77 Bemba II, *supra* note 34, ¶ 330 et seq.
78 *Id.* ¶ 333.
79 *See in detail, e.g.*, Alamunddin, *supra* note 42, at 296; Damaška, *supra* note 40, at 365–88.
80 Brdjanin, *supra* note 37, ¶ 31 et seq.

armed conflicts, intelligence can be essential in uncovering the truth.[81] It is also argued that, in light of the gravity and seriousness of the charges and the jurisdiction and purpose of the tribunals, even illegally intercepted evidence obtained in a pre-armed conflict period must be regarded as admissible.[82] The ICC has regularly come to the same conclusion and has not excluded evidence obtained in violation of privacy rights.[83] For instance, the ICC has argued that even though there is no consensus in international law, the majority is of the view that only serious human rights violations can lead to the exclusion of evidence.[84] Accordingly, since evidence is rarely excluded based on violations of the right to privacy, such an indirect influence is questionable.

B THE PROTECTION DURING INVESTIGATIONS BY THE ICT'S PROSECUTORS

Another area of importance is whether there are sufficient safeguards for the protection of privacy rights in the context of investigative activities by the Prosecution and the overall activities of ICTs.

1 *General*

It should first be emphasized that ICTs, and the ICC in particular, have very limited authority to implement coercive measures outside the context of State cooperation. Rather, search and seizures and interceptions are regarded as on-site investigative activities that depend on the cooperation of States or their approval.[85] While the ad hoc tribunals had limited independent investigative means,[86] the Rome Statute provides this possibility only in a very restricted manner.[87] The Prosecution can only conduct such independent on-site investigations in the context of Article 54, 57(3)(d) of the Rome Statute, that is, when a State is unable to execute a request for cooperation due to the unavailability of any authority or any component of its judicial system.

81 *Id.* ¶ 61.
82 *Id.* ¶ 63(8).
83 Bemba II, *supra* note 34, ¶ 44; Lubanga, *supra* note 74, ¶¶ 83–90.
84 Lubanga, *supra* note 74, ¶ 86.
85 *See, e.g.*, Alamunddin, *supra* note 42, at 258.
86 The ad hoc tribunals were provided with more extensive direct investigative rights. *See, e.g.*, ICTY Statute, *supra* note 43, art. 18(2); ICTR Statute, *supra* note 43, art. 17(2); Prosecutor v. Blaškić, IT-95-14-AR108 bis, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, ¶ 53 (Oct. 29, 1997); RICHARD MAY & MARIEKE WIERDA, INTERNATIONAL CRIMINAL EVIDENCE, 62, 67 (2002).
87 *See, e.g.*, MEESTER, *supra* note 50, at 516; ZEEGERS, *supra* note 42, at 147.

However, even aside from this area, it is relevant to consider what role the right to privacy may play in the Prosecutor's investigations. This is especially true given the increase in open-source investigation and data sharing by a wide variety of actors, even without what are known as coercive measures. Moreover, it should be noted that the voluntary disclosure of data to the Court does not necessarily mean that the data has been obtained in a way consistent with the right to privacy or that there has been no interference with it.[88] In addition, data protection and protection from third-party interference is especially important in the context of sensitive data that may be in the possession of ICTs.

To date, there has been only a very limited general policy in place that could sufficiently protect the right to privacy. While the ICC has developed an E-court Protocol[89] on digital evidence, this protocol does not refer to privacy rights but rather aims at standardizing technical-data-type-related questions. The ICC's Code of Conduct for the Office of the Prosecutor does state that the Office of Prosecution should respect the human rights and fundamental freedoms recognized by international law in conformity with the Statute.[90] Similarly, the Regulations of the Office of the Prosecution refer to the privacy in relation to confidential correspondence,[91] and Article 21(3) of the Rome Statute provides that the ICC is bound to respect internationally recognized human rights. However, as these provisions are of a very general nature, there is no certainty in how they are applied to privacy issues.

Therefore, it would be desirable for ICTs to develop specific standards for investigations performed by the ICTs bodies, especially in relation to the right to privacy.[92] These standards should find a balance between the investigative interests and the rights of those affected. They could address issues such as the protection of victims or potential witnesses visible in digital materials, or the outstanding issue of the types of data to be collected or the means of data collection, storage, and processing. While it would be desirable to include such standards in the Rules of Procedure and Evidence (RPE) of ICTs, as these new types of investigative methods will only increase in the future, this option could be difficult to achieve in practice. Nevertheless, official statements and policies could

88 *See also* Kayyali et al., *supra* note 16.
89 Unified Technical protocol for the provision of evidence, witness and victims' information in electronic form, ICC-01/14-01/18-64-Anx (Jan. 23, 2019).
90 Chapter 1, ¶ 8(1).
91 Reg. 21; Reg. 28(2).
92 *See also, e.g.*, Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives, 490–91 (Robert Kolb et al. eds., 2022).

provide some clarity on ICTs' approach regarding the right to privacy in the digital domain.

2 *The Special Protection of Victims and Witnesses*

As noted, the only explicit reference to the right to privacy within ICP can be found in the context of victims and witness protection and confidential correspondences. In the context of ICL, the protection and the privacy of victims and witnesses has a particularly important role. The dangers for them are not only of a theoretical nature and were already evident in the first years of the ad hoc tribunals. For instance, in the first years of the tribunal, some witnesses who testified before the International Criminal Tribunal for Rwanda (ICTR) were killed upon arriving back home.[93] Hence, the ad hoc tribunals attached particular importance to the protection of witnesses and victims.[94] Similarly, the ICC's legal framework entails rules on the protection of witnesses. According to Article 68(1) of the Rome Statute, the Court shall take appropriate measures to protect the safety and privacy of victims and witnesses. This general provision aims at placing on all organs of the Court the obligation to take appropriate measures.[95] In this regard, the Court must consider all relevant factors, including age, gender, and health, as well as the nature of the crimes.[96] Possible measures may be the prevention of releases to the public or the media on the identity or location of a victim, witness, or other person at risk.[97] Hence, witnesses are, in general, not named publicly and are known by pseudonyms in proceedings.[98]

This raises the question of what protection might look like in the context of modern technologies and digital evidence. So far, there is little experience to go on regarding the impact of the increased prevalence of digital evidence. It is important to bear in mind that audiovisual evidence in particular can show not only the perpetrators but also third parties, victims, and witnesses, and metadata and personal information can be used to identify individuals. Some have argued that the existence of audiovisual evidence could ensure the safety of witnesses and victims, as they are not the only ones providing incriminating proof.[99] However,

93 *See, e.g.*, David Donat-Cattin, *Art. 68*, *in* Rome Statute of the International Criminal Court: A commentary, 1681, 1683 (Otto Triffterer & Kai Ambos eds., 3rd ed. 2016).
94 *Id.*
95 *E.g.*, William Schabas, The International Criminal Court: A Commentary on the Rome Statute, 1058 (2016).
96 Schabas, *supra* note 95, at 1058.
97 *Id.*
98 *Id.*; *cf.* Tadić, *supra* note 39, ¶¶ 27–31.
99 *E.g.*, Keith Hiatt, *Open Source Evidence on Trial*, 125 Yale L. J. Forum 323, 325 (2016).

others have rightly expressed concerns regarding identifiability via digital evidence,[100] which could endanger parties not present before the ICTs. Especially in the early stages of investigations, where witnesses are still being sought, the prevalence of digital media could pose a threat to victims and witnesses. Moreover, during ongoing conflicts, the availability of information on informants, witnesses, and victims could be harmful to them. As practice shows, civilian populations are increasingly active in collecting evidence on grave crimes. NGOs and civil society in particular tend to use digital data for the collection.[101] Collections that do not sufficiently protect the privacy of the identifiable individuals could pose immeasurable threats to those on site.

The latter norms could be used to protect those affected. There are still some legal uncertainties, especially concerning whether the standards can be interpreted to apply to victims shown in digital and documentary evidence. While an overly broad interpretation of the above-mentioned provisions may make their fulfillment impossible, an overly narrow interpretation might harm those trying to support investigations. Hence this rule should generally also apply in the context of digital evidence; however, the interpretation and understanding of the appropriate means may vary in this context. Conceivable technical means here could be to make faces unrecognizable if they are not relevant for the proceedings and establish data collection in a manner that protects personal information that could be used to identify specific individuals. An additional safeguard would be to not share potential evidence publicly.

Overall, States and ICTs should seek to adopt approaches that do not pose additional harm to victims and witnesses, regardless of whether they testify in person or by providing documentary proof.

3 *Protection during Cooperation with NGOs and Civil Society*

As elaborated above, NGOs are engaging more and more in fact-finding or quasi-investigative functions, especially by using digital data. They collect information shared on social media or provided to them by individuals and create large data collections with considerable potential to support ICP. However, there are also risks involved, especially in relation to the protection of human rights. This follows above all from the fact that the party collecting and providing the data to ICTs and the one

100 *See, e.g.*, Beth van Schaack, *Fourth Industrial Revolution Comes to the Hague*, http://www.iccforum.com/cyber-evidence#Van-Schaack (last visited Nov. 29, 2021); Kayyali et al., *supra* note 16; Hiatt, *supra* note 99, at 324; Hamilton, *supra* note 16, at 60; Aboueldahab & Freixo, *supra* note 16, at 523.

101 *E.g.*, Hellwig, *supra* note 4.

whose privacy is affected can differ and that both can have contrasting standpoints. For example, while a portion of data is shared with ICTs by individuals willing to take the risks involved, other information is collected or shared without consent and, in some cases, by the perpetrators. Furthermore, if recordings and large data collections are openly accessible, they could be used to identify not only alleged perpetrators but also collectors, victims, and witnesses. This may significantly affect their right to privacy and sometimes also their safety, especially in ongoing conflicts. Therefore, the protection of potentially affected parties throughout the process is essential.[102]

However, there is a lack of internationally applicable law in this framework. Data collections today are rarely established and overseen by ICT's Prosecutions; instead, this is typically done by various NGOs. Within the current international legal framework, there are no clear internationally binding obligations for NGOs to respect human rights. While attention should be drawn to NGOs' efforts to develop voluntary standards on these issues, such as with the Berkeley Protocol,[103] precisely because of the voluntary nature of these instruments, there is still a pressing need to find additional safeguards. Furthermore, while these entities largely act independently, the acceptance and use of the data by ICTs may perpetuate interference in the affected individuals' right to privacy.

As a number of collections are aimed specifically at enabling criminal proceedings, ICTs are in a unique position to influence this sector towards a more privacy-conscious approach. Thus, while it may be difficult to argue that ICTs and other fact-finding bodies have an obligation to regulate this sector, they could take a more active role in safeguarding the protection of such rights even outside the scope of their own activities.

Therefore, the question arises of how to achieve higher standards in this area. As ICTs rarely exclude evidence based on privacy violations, it is unlikely that the threat of exclusion of the collected evidence alone could lead everyone to adhere to privacy regulations. Possible solutions include the implementation of additional (binding) guidelines[104] or contract relations with the ICT's Prosecutions[105] or other fact-finding bodies. The latter possibility in particular could help to realize the potential

102 *See also, e.g.*, Aboueldahab & Freixo, *supra* note 16, at 507, 521.
103 Berkeley Protocol, *supra* note 18.
104 *E.g.*, Elena A. Baylis, *Outsourcing Investigations*, 14 UCLA J. INT'L L. FOREIGN AFF. 121, 146 (2009); International Bar Association, *Evidence Matters in ICC Trials*, 26 (Aug. 2016); Alexander Heinze, *Private International Criminal Investigations*, Z. INT. STR. DOGM. 169, 181 (Feb. 2019).
105 Hamilton, *supra* note 16, at 53–61.

offered by these activities without excessive strain on the rights of the persons concerned if contracts would contain provisions on the respective rights to be protected.

CONCLUSION: WHAT IS THE ROLE OF ICTS IN THE PROTECTION OF THE RIGHT TO PRIVACY?

This chapter has provided an overview of the areas in which the right to privacy could be of relevance in ICP and where future issues may occur. It is not yet apparent if ICTs have sufficiently adapted to the increasing relevance of digital evidence. Overall, while the right to privacy is recognized in ICL, better approaches to enforcing this right are desirable. Two main areas for action can be identified.

First, standards and policies should be established for ICTs' own activities.[106] This would be beneficial in light of transparency concerns, existing responsibilities to witnesses and victims, and the commitment to human rights. In this context, there is a need to develop sufficient standards to protect victims and witnesses but also find a sufficient procedure for open-source investigation. It should be borne in mind that open-source investigations and voluntary disclosures of data are not completely free of potential interference with the rights of data subjects.[107]

Second, the role of the right to privacy in the context of cooperation must be reevaluated. In many ways, ICTs must deal with rather limited availability of evidence, and the crimes they deal with are of such seriousness that violations of the "mere" right to privacy do not take a prominent role. Therefore, some have argued that this right must yield second place to the interests of the victims seeking justice and the interests of the international community.[108] However, this line of argument is not fully convincing. While it is correct that ICTs do not have the function of disciplining national armies or authorities,[109] ICTs and national authorities are bound to respect international human rights. If commonly applied investigative procedures are incompatible with such rights, they must be

106 *See also, e.g.*, Lubin, *supra* note 92, at 490.
107 Kayyali et al., *supra* note 16.
108 Brdjanin, *supra* note 37, ¶ 63(7); Lubanga, *supra* note 74, ¶ 86.
109 Brdjanin, *supra* note 37, ¶ 63(9).

adjusted. In many cases, the issue is not so much whether the measures should be implemented at all but rather that procedural standards and safeguards must be complied with, or in some cases, developed in the first place. There needs to be a structural adjustment within the investigative process to ensure the predictability and monitorability of measures. For this reason, authors have rightly called for *ex ante* checks on the ordering of coercive measures ensuring compliance with the right to privacy.[110] *Ex post* checks are also crucial.[111]

Given the increasing relevance of the digital domain, limiting the scope of the right to privacy and the acceptance of an approach to ICP in which the imperative for human rights protection is outweighed by the need for evidence[112] is concerning. Upholding human rights standards, and not only to a minimum, conveys respect for human rights by demonstrating fairness and adherence to legal rules even in the context of prosecuting mass atrocities.[113] Omitting privacy rights could have an overall derogatory effect on the rights in question, as well as on the approval of ICTs by the international community and the acceptance of their rulings by local communities. This holds at least the risk that some entities question their legitimacy. In addition, privacy protection can also safeguard other human rights (e.g., the right to life and the right to freedom from arbitrary detention), especially in the context of ICP. Therefore, ICTs should take a more prominent role in promoting these rights and upholding human rights standards.

110 Zeegers, *supra* note 42, at 186.
111 *Id.*
112 Damaška, *supra* note 40, at 386.
113 *See generally* Yvonne McDermott, Fairness in International Criminal Trials (2013); Salvatore Zappalà, Human Rights in International Criminal Proceedings (2005).

Chapter 14

The "Right to be Forgotten" and International Crimes

Yaël Ronen[1]

INTRODUCTION

The ubiquity of information in cyberspace has brought new challenges to the concept of privacy and has led to the development of new forms of protection of the right to privacy. Among those is the notion of a right to be "forgotten" or "erased."[2] These terms cover a variety of measures aimed at removing personal information from the public sphere or making it less accessible, through, among other things, the deletion of news articles, the de-linking of web pages in search results on search engines, and the redaction of personal information on existing web pages.[3]

1 Professor of Law at the Academic Center for Science and Law at Hod Hasharon, and a Research Fellow at the Minerva Center for Human Rights at the Hebrew University in Jerusalem.

2 KIERON O'HARA ET AL., A PRAGMATIC APPROACH TO THE RIGHT TO BE FORGOTTEN 2–3 (Centre for International Governance Innovation and Chatham House, 2016), https://www.cigionline.org/publications/pragmatic-approach-right-be-forgotten. For a critique of the term "forgetting," see Ignacio Cofone, *Google v. Spain: A Right to Be Forgotten*, 15 CHI.-LENT J. INT'L & COMP. L. 1, 8–9 (2015).

3 Under European law, the term refers specifically to a qualified right of individuals to have their

"Forgetting" and "erasing" are largely misnomers, as information is not fully removed from cyberspace. First, the removal of news items and page links does not affect the availability of the information on legal databases and archives. What is removed is only the likelihood that the information be found by someone who is not deliberately seeking it. Moreover, there are ways to circumvent the "loss." For example, de-linking on Google has, in some cases, prompted the original website to publish articles about the de-linking itself, including details about the content of the original story. Secondly, despite apparent erasure and deletion, the information may still be available in a cache.[4] This chapter will nonetheless employ the phrase "the right to be forgotten," which has taken root in both legal and technological discourse.[5]

The chapter concerns the right to be forgotten for individuals who have been convicted of, and punished for, the commission of international crimes. It may well be asked whether the suppression of information would have any effect when international crimes are at issue. However, not all convictions for such crimes necessarily have a high public profile or a long-lasting effect. Are Paul Slough, Janis Karpinski, Calvin Gibbs, Yuri Budanov, Fadil Covic, Donald Payne, Dragan Kolundzija, or Ahmad al-Mahdi household names?[6]

Part I of this chapter considers the value of forgiving and forgetting and the need to replicate the fading of memory with technical means when human memory is replaced by the technological storage of information. Part II frames the individual and public interests involved in the removal of information relating to the criminal past of identified individuals as an exercise in balancing competing human rights and interests. Part III examines how the balance is affected when the crimes in question are international crimes. It first analyzes the implications of two characteristics of international crimes that distinguish them from ordinary crimes: the fact that they are committed in the course of a

personal data erased from filing systems, primarily when the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed. Council Regulation 2016/679, 2016 O.J. (L 119) 1, art. 17(1)(a) [hereinafter GDPR]; or, in the words of the CJEU, when the data becomes inadequate, irrelevant, or excessive for the purposes of its processing. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 92–94 (May 13, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [hereinafter Google Spain].

4 Eduard Fosch Villaronga et al., *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, 34 COMP. LAW & SEC. REV., 304 (2018). Google refused to de-list these articles on the grounds that the search links were relevant and in the public interest. For the decision of the Information Commissioner's Office, see Data Protection Act 1998 Supervisory Powers of the Information Commissioner, Enforcement Notice, INFO. COMM'R'S OFFICE, Aug. 18, 2015, https://www.pdpjournals.com/docs/88469.pdf.

5 GDPR, *supra* note 3, art. 17, entitled "Right to erasure ('right to be forgotten')."

6 All these persons have been convicted of war crimes or offences that amount to war crimes.

communal conflict and their status as violations of peremptory norms of international law. It then analyzes how the general considerations regarding the removal from cyberspace of personal information relating to crime apply when international crimes are at issue.

I
THE IMPORTANCE OF FORGETTING

Forgiveness encapsulated the idea that former criminal offenders need not be defined exclusively by their criminal past. Forgiveness is intended not to erase the criminal acts themselves but to demarcate the context in which they are to be regarded as relevant, thereby limiting their place in historical consciousness and the weight of the guilt associated with them.[7]

The notion of forgiveness is assisted, to some extent, by the natural process of human forgetfulness. While written documentation has reduced the dependence of society on human memory, digitization has all but eliminated the notion of information loss. The use of cyberspace, on which this chapter focuses, has eliminated the geographical and temporal containment of information. Information of all types, including on individuals' involvement in the commission of a crime and specifically international crimes, is available from a variety of sources: formal records, judicial archives, news archives, and private sources. Hyper-connectivity through search engines allows retrieval of those sources. Personal information linked to the commission of international crimes is now accessible to information consumers everywhere and virtually forever, even when they do not actively seek it.[8]

In a rational society, abundance and availability of information may appear to be an optimal situation, as more information enables the making of better informed—and therefore better—decisions. But the unlimited availability of information exacts a price when it hinders individuals from turning a new page. For this reason (as well as other reasons, some not so virtuous), there is nothing novel or surprising about the wish of

7 Ugo Pagallo & Massimo Durante, *Legal Memories and the Right to Be Forgotten*, *in* PROTECTION OF INFORMATION AND THE RIGHT TO PRIVACY: A NEW EQUILIBRIUM? 17, 26 (Luciano Floridi ed., 2014).

8 Cécile de Terwangne, *The Right to be Forgotten and Informational Autonomy in the Digital Environment*, *in* THE ETHICS OF MEMORY IN A DIGITAL AGE 82–89, 85 (Alessia Ghezzi, Ângela Guimarães Pereira & Lucia Vesnić-Alujević eds., 2014).

individuals to remove unflattering information about themselves from the public sphere, especially information on criminal activity.[9]

Since nothing is ever naturally forgotten, the obstacle to forgiveness has to be removed through active measures. This is a costly, resource-consuming process.[10] Yet legal regulation of information management has been limited and partial.[11] The rise of bureaucracy generated legislation on the erasure of spent convictions.[12] In the EU, the retention of information on databases became regulated in the 1990s and is now governed by the GDPR, whose impact goes far beyond EU borders.[13] Elsewhere, the removal of information from databases and archives, as well as the de-linking of web pages on search engines, have been sought through private tort actions.[14] There is a whole spectrum of means for dealing with lingering personal online information that causes individuals significant harm,[15] from erasure of the information itself to the addition of contextualizing information.[16] In between are measures such as limiting access to the information, redacting it, and anonymizing it. A separate type of measure concerns search engines, where individuals' names can be de-linked from web pages.[17]

Different jurisdictions adopt different balances between conflicting rights and interests relating to personal information on criminal

9 Theo Bertram et al., *Five Years of the Right to Be Forgotten*, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (ACM, 2019), https://dl.acm.org/doi/10.1145/3319535.3354208.

10 *Id.*

11 O'Hara et al., *supra* note 2, at 1.

12 Human rights: Comparative table of legislation on spent convictions, Australian Human Rights Commission (2004), https://humanrights.gov.au/our-work/human-rights-comparative-table-legislation-spent-convictions (last visited Nov. 20, 2021); T.J. McIntyre & Ian O'Donnell, *Criminals, Data Protection and the Right to a Second Chance*, 58 Irish Jurist 27, 34–35 (2017); Dominic McGoldrick, *Developments in the Right to Be Forgotten*, 13 Hum. Rts. L. Rev. 761, 763 (2013) (mentioning the French "voluntary Charter of Good Practices on the right to be forgotten on social networks and search engines"); W. Gregory Voss & Céline Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms*, 14 Colo. Tech. L.J. 281, 310–13 (2015) (discussing American privacy regulation).

13 For practice in Europe relating to newspaper archives and search engines based on the GDPR, see Dawn C. Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten*, 39 U. Pa. J. Int'l L. 1 (2018).

14 Franz Werro, The Right to Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia (2020); Jasmine E. McNealy, *The Emerging Conflict Between Newsworthiness and the Right to Be Forgotten*, 39 N. Ky. L. Rev. 119 (2012); Ashley Messenger, *What Would a "Right to Be Forgotten" Mean for Media in the United States?* 29 Comm. L. 29, 29–30, 35 (2012). In France this was known as "le droit á l'oubli," a predecessor in both name and form to the modern digital counterpart. Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88, 88 (2012). For Japanese law, see Frederike Zufall, *Challenging the EU's Right to Be Forgotten: Society's Right to Know in Japan*, 5 Eur. Data Prot. L. Rev. 17 (2019).

15 Meg Leta Jones, *Ctrl + Z in Legal Cultures, in* CTRL + Z: The Right to Be Forgotten 147–49 (2016).

16 Jones, *supra* note 15, at 147–49; McGoldrick, *supra* note 12, at 775.

17 O'Hara et al., *supra* note 2, at 8–9; Andrew Neville, *Is it a Human Right to Be Forgotten? Conceptualizing the World View*, 15 Santa Clara J. Int'l L. 157 (2017); Ivan Szekely, *The Right to be Forgotten and the New Archival Paradigm, in* The Ethics of Memory in a Digital Age: Interrogating the Right to Be Forgotten 33–34 (Pereira Ângela Guimarães, Alessia Ghezzi & Vesnić-Alujević Lucia eds., 2014).

activities.[18] This chapter does not second-guess these choices; nor does it focus on what specific technical means should be used for erasure or de-listing. Rather, it examines whether and how the balancing should be modified when what is at issue is information revealing a particular aspect of an individual's involvement in the commission of international crimes. Such information may encompass a whole variety of matters: allegations, indictments, convictions, acquittals, civil proceedings against a person convicted of such a crime, a person's family relationship with an individual who has been the victim of international crimes, and much more. However, the chapter is limited to information on persons who have been convicted and punished.[19] One reason for this is that the chapter concerns the notion of forgiveness and considers the erasure or de-linking of information specifically on the grounds that the passage of time has rendered the information inaccurate or excessively harmful, rather than on the grounds that the information should not have been made public to begin with or that it provides an incomplete and therefore misleading account. A separate discussion should be dedicated to issues relating to information on allegations and indictments that have come to naught, as well as to issue relating to persons other than the former offenders themselves. These issues are informed less by considerations of forgiveness and more by questions such as the relationship between the legal truth and factual truth, and between the presumption of innocence and freedom of information. The chapter follows existing practice, whereby requests for the removal or de-linking of information are considered only when made by the subjects of the information themselves.[20]

18 For comparative studies, see Franz Werro, *The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash, in* LIABILITY IN THE THIRD MILLENNIUM (Aurelia Colombi Ciacchi, Christine Godt, Peter Rott & Leslie Jane Smith, eds., 2009). WERRO, *supra* note 14. In the US recently, see *G.W. v. Gannett Co.*, Inc., No. 2082CV0629, 2020 WL 9076502, at *1 (Mass. Super. Dec. 29, 2020).

19 Under European law, such information is regarded as personal data, namely information relating to the social identity of a natural person. GDPR, *supra* note 3, art. 4(1).

20 The GDPR explicitly states that erasure will be considered only when requested by the data subject.

II
COMPETING RIGHTS AND INTERESTS

A PRIVACY AND REPUTATION

The right to be forgotten in the sense of removal of information from the public sphere or de-linking of information stems from individuals' interest to protect their reputation. Under the universal human rights system, the right to protection from unlawful interference with one's reputation and honor is an independent right.[21] The European human rights system formally recognizes reputation and honor not as independent rights, but as legitimate grounds for restricting other rights.[22] Nonetheless, over the years the European Court of Human Rights has expanded the right to privacy to encompass what the domestic law of many European States recognizes as "personality rights," namely individuals' interest in representing themselves in a public context and developing their identity and personality.[23]

Privacy as personality is underpinned by the notion of human dignity, from which derives the perception of individuals as autonomous agents, able to determine freely the development of their life.[24] This autonomy justifies holding individuals accountable for their bad choices. But by the same token, human dignity requires that individuals not be reduced to their bad choices and not be forever burdened and stigmatized by them.[25] Instead, they should be allowed to differentiate themselves from their past selves.[26] In the context of criminal activity, what is at issue is the (re-)integration of former offenders into law-abiding society. This involves

21 International Covenant on Civil and Political Rights art. 17(1), Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

22 Bart van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data,"* 31 UTRECHT J. OF INT'L AND EUR. L. 25, 31–32 (2015).

23 *Id.*

24 Voss & Castets-Renard, *supra* note 12, at 291, citing Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten,"* 29 COMP. L. & SEC. REV. 229, 229 n. 1 (2013).

25 Norberto Nuno Gomes de Andrade, *Oblivion: The Right to be Different... from Oneself: Re-Proposing the Right to be Forgotten, in* THE ETHICS OF MEMORY IN A DIGITAL AGE (Alessia Ghezzi, Ângela Guimarães Pereira & Lucia Vesnić-Alujević eds., 2014); Luciano Floridi, *"The Right to Be Forgotten": A Philosophical View,* 23 JAHRBUCH FÜR RECHT UND ETHIK/ANN. REV. L. & ETHICS, 163, 155 (2015); Christiana Markou, *The "Right to Be Forgotten": Ten Reasons Why It Should Be Forgotten, in* REFORMING EUROPEAN DATA PROTECTION LAW, vol. 20 (S. Gutwirth, R. Leenes & P. de Hert eds., 2015); McGoldrick, *supra* note 12, at 764–65.

26 De Andrade, *supra* note 25, at 73–74; Terwangne, *supra* note 8, at 90–91. For a critique that the right to reinvent oneself is tantamount to a right to misrepresent, see John W. Dowdell, *An American Right to Be Forgotten,* 52 TULSA L. REV. 311, § V (2016).

developing new personal connections and distancing oneself from old ones, finding new income sources, and numerous other aspects of social life. Moreover, (re-)integration is in the interest not only of the former offenders themselves but also of society at large, since the successful adjustment and civic engagement of former offenders reduces financial and social burdens.[27] Without opportunities for social re-integration, the risk increases that a criminal underclass will emerge, endangering public safety. In addition, exclusion creates marginalized populations that are burdened with multiple layers of disadvantage, thereby depriving society of skills and talents while imposing on it the costs of unproductivity.[28]

The availability of information in cyberspace presents a serious challenge to the reconstruction of personal identity, especially when it does not contextualize the information. Perhaps least problematic are judicial records, which are usually not generally accessible and which, like institutional databases and archives, by nature delineate the context of the information very strictly.[29] They could be regarded as a repository where information is left to sediment. In contrast, news articles offer the reader a social interpretation of the information, which remains fixed and eternally available, despite changes that may have taken place over time. If those changes are not taken into account, the original context may become misleading as to the relevance of the information. Finally, hyperconnectivity makes information available entirely out of context and to audiences that did not seek it.[30] News websites and search engines are therefore the platforms that present the greatest difficulty for individuals seeking to reform and develop a new personality. They are the focus of this chapter.

B FREEDOM OF EXPRESSION AND INFORMATION

The right of news organizations to impart information as part of their freedom of expression[31] needs no elaboration. Concerning search engines, the matter is more complicated. One question is whether the results

27 Jones, *supra* note 15, at 141–43.
28 McIntyre & O'Donnell, *supra* note 12.
29 They are also likely to provide the most accurate information. However, this chapter does not address problems arising from inaccurate or fake information as such.
30 Google Spain, *supra* note 3, ¶ 80.
31 ICCPR art. 19, European Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, as amended by Protocols Nos. 11 and 14, 4 November 1950, E.T.S. No. 5 [hereinafter ECHR]; American Convention on Human Rights art. 13, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 143 [hereinafter ACHR].

of a search constitute "expressions" protected under the freedom of expression. Given the broad interpretation of the term "expression" as inclusive of every communicable form of subjective ideas and opinions, value-neutral news and information, and more,[32] there is no reason to exclude search results from the scope of the term. Not only do such results indicate a substantive link between a person's name and certain conduct, but often the titles of websites and snippets of content contain enough information for the user to understand the underlying facts.[33] The 2014 Court of Justice of the European Union (CJEU) *Google* case—a landmark for holding that the activity of a search engine constitutes the "processing of personal data" for the purpose of EU law and that a search engine may be regarded as the "controller" in respect of that processing[34]—did not address the matter in terms of freedom of expression or of information. When the Court mentioned the considerations to be weighed against the individual's right to private life and to protection of personal data, it mentioned access to information only as "the legitimate interest of internet users."[35] It did not mention freedom of expression as a right of the data controller.[36] In other courts, search results have at times been held to be "expression"[37] and thereby protected by the right. A separate question is whether search engines, as nonhuman entities, possess and may invoke human rights. This question, too, may be answered differently depending on the jurisdiction.[38]

Freedom of expression protects internet users' right to seek and receive all generally accessible information and ideas.[39] Clearly, a news organization is not obligated to make its archives (digital or other) available to the public; nor are search engines obligated to provide search opportunities.[40] Users cannot claim a *right* to such information. Nevertheless, as the CJEU noted, there does exist a public *interest* in having the information available. While mere curiosity may not be sufficient to justify interference with individuals' right to privacy,[41] criminal activity

32 Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary 443–44 (N.P. Engel, 2005).
33 Zufall, *supra* note 14, at 19.
34 Google Spain, *supra* note 3, ¶ 41.
35 Both quotes from *Google Spain*, *Id.* ¶ 81.
36 Nor, for that matter, did it consider the availability of the information as reflective of the right to freedom of expression of the publisher of the information.
37 For a judicial articulation of this view, see Zufall, *supra* note 14, on the Japanese case law of 2017.
38 For example, under Japanese law, Google benefits from the right to freedom of expression, Zufall, *supra* note 14, at 22.
39 ICCPR art. 19, ECHR art. 10, ACHR art. 13. ECHR Art. 10 does not provide the right to actively seek information explicitly, but this is inferred from the case law. Nowak, *supra* note 32, at 446.
40 If a substantive right exists that is within the power of a non-State actor to "respect," the government is obligated to ensure that the non-State actors supply the information.
41 Google Spain, *supra* note 3, ¶ 81.

is usually regarded as a matter of public relevance, and information about it is pertinent to various legitimate public interests that may at times override the right to privacy, such as concerns that the transgression will be repeated. In addition, the formal, State-imposed punishment does not dispense with social censure.[42] Thus moral judgment has been recognized as a legitimate concern with regard to public figures of persons seeking to hold public positions.[43]

The public may also have interests that are not related directly to specific former offenders but for which the personal information of former offenders may be pertinent. For example, the demographics of offenders, at least in aggregated form, are important in developing a rational policy to reduce crime.[44]

III
IMPLICATIONS OF INTERNATIONAL CRIMES FOR THE BALANCING OF RIGHTS

Numerous factors have been cited in international case law and scholarship as pertinent for balancing the right to privacy against the public interest when online information on criminal activity is at issue. These include the nature and content of the information, including the severity of the offense; the concrete harm caused to the individual by the availability of the information; the social position and influence of the individual; the platform on which the information is presented; the purpose and meaning of the article containing the information; the social situation when the information was posted and subsequent changes; the need to reveal particular facts; and, of course, the passage of time.[45]

42 For a judicial articulation of this in Japanese law, see Zufall, *supra* note 14, at 22. Zufall criticizes the granting to Google, a private corporation, the power to determine public interest beyond the legal limitation periods, *id.* at 24.

43 Google Spain, *supra* note 3, ¶ 81.

44 The name of specific offenders may not be required for this purpose. Whether the name can be separated from the information depends on the information source. Furthermore, at times individuals may be identifiable even without the explicit mention of their name.

45 Google Spain, *supra* note 3, ¶ 81; Supreme Court of Japan, Decision of Feb. 8, 1994 (Minshū 48, No. 2) 149 (nonfiction "gyaku-ten" jiken) ¶ 7; Information Commissioner's Office, *supra* note 4, ¶¶ 23–29; Róisin A. Costello, *The Right to Be Forgotten in Cases Involving Criminal Convictions: Nt1 & Nt2 V Google and the Information Commissioner*, 3 EUR. HUM. RTS L. REV. 268 (2018).

In what follows, I consider various factors that may be relevant to the balancing process when the information concerns convictions specifically for international crimes. Some of these factors are unique to international crimes. Other factors apply also with regard to ordinary crimes but may have specific angles when considered in relation to international crimes.

A THE RIGHT TO TRUTH WITH REGARD TO INTERNATIONAL CRIMES

International human rights law requires that crimes be investigated, that they be prosecuted where appropriate, and, when convictions are secured, that perpetrators be punished. With respect to some serious crimes, State obligations have been expanded to the provision of victims' families with information about the crimes that have been committed and the circumstances that have led to that commission.

Transitional justice scholarship suggests that the requirements of accountability for international crimes may go further. A successful process of social reconstruction cannot be limited to criminal tools and requires genuine self-reckoning by the communities involved. Recent years have seen the emergence of new expectations and principles that suggest that, beyond the rights of direct victims of crimes to have their individual cause vindicated through courts of law, the public at large is entitled to know the truth about past events concerning heinous crimes and the circumstances and reasons that led to those crimes.[46] Truth seeking, also outside the courtroom, is therefore an essential aspect of a society's efforts to address a past that involves international crimes.[47] It is too early to declare a legal right to truth, since this public entitlement has yet to be formally accepted by States as legally binding, and its content has yet to be elucidated. But the underlying rationale of the "right" to truth (the term henceforth being used loosely) may inform the balancing of conflicting rights and interests with regard to accessibility

46 Principles 2 and 4 of the Report of the independent expert to update the Set of principles to combat impunity, Diane Orentlicher, Updated Set of principles for the protection and promotion of human rights through action to combat impunity, E/CN.4/2005/102/Add.1 (2005), http://daccessdds.un.org/doc/UNDOC/GEN/G05/109/00/PDF/G0510900.pdf?OpenElement; El-Masri v. the former Yugoslav Republic of Macedonia, App. No. 39630/09, Grand Chamber Judgment, Eur. Ct. H.R. (2012) ¶ 191; Al-Nashiri v. Poland, App. No. 28761/11, Judgment, Eur. Ct. H.R. (2014) ¶ 495; Abu Zubaydah v. Poland App. No. 7511/13, Judgment, Eur. Ct. H.R. (2014) ¶ 489; Association "21 December 1989" and others v. Romania App. No. 33810/07, Judgment, Eur. Ct. H.R. (2011) ¶ 144.

47 Eva Brems, *Transitional Justice in the Case Law of the European Court of Human Rights*, 5 Int'l J. Transitional Just. 282, n. 25 (2011), and cases cited there.

online to personal information about convictions of international crimes. Opposite the notion of a right to be forgotten, there is an obligation to prevent oblivion.

Two issues that merit consideration are the identity of the duty holder, namely the relationship between States and private actors, and the type of "truth" to which the public has a right.[48] To be sure, the right to truth is addressed to States and not to private actors. At present, the requirement from States is to preserve and enable access to public records and archives but not to regulate the management of information held by private parties. In other words, it is hard to argue *categorically* that information about international crimes, even once published online, must remain accessible and that States must therefore force news organizations to provide online access to their archives or prohibit search engines from removing links to such archives. On the other hand, when a person seeks to have information about a conviction for an international crime removed, perhaps States must ensure that the decision-making body gives the right to truth, expressed in the availability of information, especially weighty consideration. This, too, would be a far-reaching requirement.

A separate question is whether the "truth" to which there is a right necessarily includes the naming of individuals. Some guidance may be found in the International Convention for the Protection of All Persons from Enforced Disappearance,[49] probably the most detailed and concrete legal expression of a right to truth. The Convention cites the right to truth as inclusive of the right to know the progress and/or results of any and all official investigations of the crime.[50] Even this wording does not, in itself, imply that the names of perpetrators must be available without restriction. The ECtHR, for its part, has held that freedom of expression and the right to know require States to allow debate on the rights-violating past itself, as well as on the approach taken toward the legacy of that past. But it does not require them to interfere with the privacy of individuals involved in the rights-violating past.[51]

Another consideration regarding the relationship between the right to truth and the right of individuals to privacy is that since international crimes are often a matter of mass perpetration and few persons are brought to legal account, it is all too easy for others, individually and

48 Grażyna Baranowska & Aleksandra Gliszczyńska-Grabias, *"Right to Truth" and Memory Laws*, 47 POLISH POL. SCI. Y.B. 97, 98–99 (2018).

49 International Convention for the Protection of All Persons from Enforced Disappearance, art. 24.2, Dec. 20, 2006, 2716 UNTS3 (entered into force Dec. 23, 2010).

50 *Id.*; Baranowska & Gliszczyńska-Grabias, *supra* note 48, at 97.

51 Brems, *supra* note 47, at 287–88, n. 31; Antoon De Baets, *A Historian's View on the Right to Be Forgotten*, 30 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 57, 61 (2016).

collectively, to distance themselves from their own moral responsibility by holding that the particular individuals who had been prosecuted are the only ones responsible for the crimes. This results in the apparent scapegoating of certain individuals. In the criminal process, the inability to hold everyone accountable is not a justification for impunity. But in the context of accessibility of information online, there is valence to the argument that the availability of information on specifically named individuals may give the false impression that moral and social responsibility, too, lies exclusively with them, and easily absolve the community at large from engaging with its past and present. It should nonetheless be noted that while the availability of personal information on specific perpetrators may indeed enable a particular society to disregard its past and avoid engagement with its collective responsibility, the removal of that personal information would obviously not have the opposite effect, namely to force a society to contend with its collective responsibility. If anything, it may simplify that disregard even further. Thus any scapegoating of individuals should be prevented by other means.

Arguably, an analogy could be made from the often-cited statement of the international military tribunal in Nuremberg (IMT) that "[c]rimes against international law are committed by men, not by abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced."[52] Like legal accountability, communal self-reckoning requires that the crimes be concretized for there to be genuine engagement. The mention of names may be a powerful reminder to members of the general public of their own potential proximity to the act. It may force a discussion of "crimes we (as a society) have committed" as opposed to "crimes that have been committed."

B THE PEREMPTORY CHARACTER OF INTERNATIONAL CRIMES

It is generally recognized that the prohibitions on the commission of international crimes are peremptory norms,[53] which, by their nature, prevail over other norms of international law. The question arises as to how

52 France et al. v. Goering et al., 22 IMT 411, 466 (Int'l Mil. Trib. 1946).

53 ILC, Peremptory Norms of General International Law (Jus Cogens), Text of the Draft Conclusions and Draft Annex Provisionally Adopted by the Drafting Committee on First Reading, annex, 23, U.N. Doc. A/CN.4/L.936 (May 29, 2019); Alexander Orakhelashvili, *State Immunity and Hierarchy of Norms: Why the House of Lords Got It Wrong*, 18 European Journal of International Law 955, 963 (2007).

far the character of peremptory norms extends and, specifically, whether it has consequences in the public sphere after punishment has been served.

There is a strong, albeit controversial, view that the obligation of States to prosecute and punish the perpetrators of international crimes is also a peremptory norm.[54] This view is reflected in international practice with respect to norms related to the prescription of prosecutions and the granting of amnesty. The first matter is addressed in the 1968 Convention, which requires States parties to ensure that statutory or other limitations shall not apply to the prosecution and punishment of international crimes.[55] There is also a view that amnesties for perpetrators of international crimes are impermissible, although practice varies.[56]

By contrast, international tribunals have consistently ruled that the fact that the subject matter of criminal or civil proceedings in a domestic court is the commission of an international crime does not create an exception to the rules on State immunity and immunity of officials. This position has been grounded primarily in the reasoning that immunity creates a procedural obstacle that does not conflict directly with the substantive prohibition, and therefore no conflict arises between a peremptory norm and an ordinary one.[57] This analysis has been strongly criticized (as has been the practice of granting amnesties) on the grounds that if the remedies for the violations of a peremptory norm are considered derogable, then effectively the peremptory norm itself becomes derogable.[58] But even if one adopts the stricter view—that the peremptory character of the norm dictates that there must not be procedural or other obstacles to the provision of remedies for international crimes—it should be stressed that the remedies at issue are those offered by the criminal process. Thus if a crime has been committed, it must be investigated and prosecuted; and if a conviction is secured, punishment must be served. But when the criminal process ends, the peremptory character of the norm ceases to have consequences.

54 *Id.* at 304–7.

55 Convention on the Non-Applicability of Statutory Limitations to War Crimes and Crimes Against Humanity, art. 4, 26 November 1968, 754 UNTS 73 (entered into force Nov. 11, 1970). While a few States have ratified the Convention, the travaux préparatoires suggest that many States regarded the prohibition on prescription for international crimes as already constituting a customary norm that the convention merely codified. William Schabas, *Time, Justice and Human Rights: Statutory Limitation on the Right to Truth? in* UNDERSTANDING THE AGE OF TRANSITIONAL JUSTICE: CRIMES, COURTS, COMMISSIONS, AND CHRONICLING 37–55 (Nanci Adler ed., 2018).

56 The Prosecutor v. Furundzija, Judgment of Dec. 10, 1998, IT-95-17/I-T, at ¶ 155; Prosecutor v. Morris Kallon & Brimma Bazzy Kamara, SCSL-2004-15-AR72(E) & SCSL-2004-16-AR72(E), Decision of Mar. 13; Orakhelashvili, *supra* note 53.

57 Al-Adsani v. the United Kingdom, App. No. 35763/97, Eur. Ct. H.R. (Nov. 21, 2001); Jurisdictional Immunities of the State (Ger. v. It.: Greece Intervening) (Germany v. Italy), Judgment (Feb. 3, 2012), http://www.icj-cij.org/docket/files/143/16883.pdf.

58 Orakhelashvili, *supra* note 53, at 243, expanded in ch. 10 and on pages 226–50, 304–7.

The normative hierarchy analysis takes an interesting turn even if one accepts the view expressed by international tribunals that procedural norms resulting in impunity do not defer to substantive peremptory norms. Unlike statutes of limitation, amnesties, and immunities, which are procedural mechanisms that *undermine* legal accountability, the (procedural) right to truth *strengthens* this accountability. Where the tension lies is between the peremptory prohibition and the right to privacy, which is a substantive norm. In this tension, the peremptory character of the norm dictates its superiority. However, this superiority does not mean that the right to privacy may be entirely obviated. What the right to truth entails, and how far the right to privacy should be curtailed, are questions that still require consideration.

C GRAVITY

In considering how long personal information relating to criminal conduct should legitimately be retained in the public sphere, the criterion most often used is the gravity of the criminal act. The graver the crime, the longer the public interest should be considered a legitimate factor.[59] In what follows, I consider how the factor of gravity operates when the crime at issue is an international one.

One line of examination is whether keeping information available online should be subject to the same standards that apply to preserving criminal records. Just as international crimes are not subject to statutes of limitation, should online information related to their perpetrators likewise not have an expiration date? Statutory limitations, by which ordinary crimes are limited, have various justifications. One argument, developed with regard to minor offenses, is that alleged offenders can and, at times, do mend their ways. If the alleged offenders were not promptly punished, and over time the crimes have all but been forgotten, and the offenders have mended their ways and become better members of society, then legal impunity is no longer a strong concern.[60] Statutes

59 Joran Spauwen & Jens van den Brink, *Dutch Google Spain Ruling: More Freedom of Speech, Less Right to be Forgotten For Criminals*, INFORRM'S BLOG, Sept. 27, 2014, https://inforrm.org/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/.

60 CESARE BECCARIA, AN ESSAY ON CRIMES AND PUNISHMENTS 112 (2nd ed., 1872), cited by Comm'n on Human Rights, Twenty-second Session, "Question of Punishment of War Criminals and of Persons Who Have Committed Crimes against Humanity, Question of the Non-Applicability of Statutory Limitation to War Crimes and Crimes against Humanity," Study Submitted by the Secretary-General, ¶ 104 C/CN.4/906 (1966), https://www.un.org/ga/search/view_doc.asp?symbol=E/CN.4/906.

of limitation also developed as a matter of expediency, driven by considerations such as the reduced reliability of witnesses and other types of evidence when the crimes in question were committed a long time ago. These make prosecution for long-gone crimes excessively burdensome on governmental resources and increase the risk of false convictions.

These two sets of considerations were discussed in the negotiations on the 1968 Convention on the Non-Applicability of Statutory Limitations to War Crimes and Crimes against Humanity. With respect to the former, several States argued that it was unrealistic to believe or hope that Nazi criminals would repent and become decent members of any civilized community.[61] In addition, it was argued that atrocious crimes in general are long-remembered[62] and that, with respect to Nazi atrocities in particular, world opinion would never forgive them or become indifferent to them.[63] In other words, legal impunity would forever remain the overriding concern.

With respect to resources, throughout the negotiations there was controversy over whether gravity (of the acts or of crimes[64]) should be a limiting factor for the non-applicability of statutory limitations.[65] Ultimately, the Convention rejected the distinction,[66] thus conveying the message that no international crime is light enough to enjoy impunity, even on practical grounds.

How do these considerations operate when applied not to statutory limitations on prosecution but to the balancing of conflicting interests after a sentence has been served? The development of IHRL appears to be crucial in this respect, since the argument that perpetrators of

61 Comm'n on Human Rights, Report on the Twenty-First Session, 39 U.N. ESCOR, Supp. (No. 8) 87, ¶ 544 UN Doc E/4024, E/CN.4/891 (1965).

62 BECCARIA, *supra* note 60.

63 Comm'n on Human Rights, *supra* note 61.

64 Comm'n on Human Rights, Twenty-third Session, Preliminary draft convention, prepared by the Secretary-General, on the non-applicability of statutory limitation to war crimes and crimes against humanity E/CN.4/928 (1967); Comm'n on Human Rights, Report on the Twenty-third Session, 49 U.N. ESCOR, Supp. (No. 6), ¶¶ 142, 146–48, 155, UN Doc E/4322, E/CN.4/940 (1967); U.N. General Assembly, Question of punishment of war criminals and of persons who have committed crimes against humanity: Report of the Secretary-General UN Doc A/7174 (1968); U.N. General Assembly, Third Committee, Summary records of meetings nos. 1564 to 1568, UN Doc A/C.3/SR.1564–68 (1968).

65 Comm'n on Human Rights, Question of the punishment of war criminals and of persons who have committed crimes against humanity: United Kingdom: amendment to the draft convention (A/7174, annex) A/C.3/L.1564/Rev.1 (1968).

66 *E.g.*, US proposed amendment in Comm'n on Human Rights, *supra* note 61, ¶ 520: "Deeply concerned that those guilty of the gravest war crimes of the Nazi period shall not escape the bar of justice," https://www.un.org/ga/search/view_doc.asp?symbol=E/4024(SUPP), rejected in favor of Commission Res 3(XX)) Question of Punishment of War Criminals and of Persons Who Have Committed Crimes Against Humanity, adopted 9 April 1965, available in Comm'n on Human Rights, *supra* note 61, ¶ 567: "Deeply concerned that no one guilty of war crimes or of crimes against humanity of the Nazi period shall escape the bar of justice…," https://www.un.org/ga/search/view_doc.asp?symbol=E/4024(SUPP); Vote rejecting to amendments to draft article I on this matter, Id. A/C.3/SR.1568, ¶ 37, rejecting UK and 4-power amendments.

international crimes cannot be reasonably expected to repent directly contradicts the notion of privacy as personality rights. It is one thing to gauge that perpetrators of international crimes are beyond reform as a matter of fact;[67] but it is another to categorically deny them the opportunity for reform. If the right to personal identity is an element in the human right to privacy, no one may be altogether deprived of it, not even a perpetrator of international crimes. Persons who have been held to criminal account should be protected from being forever reduced to nothing but former offenders. Accordingly, international crimes do not merit a categorical bar to removal or de-linking of personal information relating to their commission.

That said, the gravity of international crimes as categories of crime, irrespective of the gravity of a particular act that formally falls within these categories, may justify attaching weight to them when determining the proper balance between conflicting rights and interests relating to online availability of the information. The categorical gravity of international crimes lies in the fact that, in addition to the harm to life, limb, and property that they cause to direct victims, these crimes offend the tenets of global society as envisaged by international law, one in which all persons are equally valued and deserving, individually and in groups. Each of the categories of international crimes addresses a different aspect of this humanness. The category of war crimes indicates that humanness is innate and inalienable and therefore may not be denied even to the enemy with whom one is locked in armed conflict. Crimes against humanity represent the failure of political organization, which is a necessity for individual security and well-being.[68] The crime of genocide concerns an attack on the human need for collective identity.[69]

Case law and policy on the erasure and de-linking of online information take into account the gravity of the acts when determining the balance between the perpetrator's right to personal identity and countervailing interests. This gravity is usually reflected in (and gauged by) the punishment actually meted out. Social censure thus operates as an extension of the formal censure and on the basis of the same standard:

67 For discussion of the genuineness of repentance among defendants in international courts, see Frédéric Mégret, *The Repentant Defendant and the Potential of International Criminal Justice*, 21 CONTEMPORARY JUSTICE REVIEW 432 (2018).

68 David Luban, *A Theory of Crimes against Humanity*, 29 YALE J. OF INT'L L. 85, 109–10, 117, 119–20 (2004). Darryl Robinson attributes to Kress and Schabas, Darryl Robinson, *Essence of Crimes Against Humanity Raised By Challenges at ICC,* EJIL: TALK! (2011), https://www.ejiltalk.org/essence-of-crimes-against-humanity-raised-by-challenges-at-icc.

69 Michael Ignatieff, *Lemkin's Word*, NEW REPUBLIC, Feb. 26, 2001, at 27–28, *cited in* Luban, *supra* note 68, n. 102.

the graver the act, the longer it can legitimately be held against the individual even beyond the serving of their sentence. This means longer retention of the information. At first glance, it may seem that applying the criterion of gravity to requests for the removal and de-listing of information requires no particular modification for international crimes, since punishments for acts constituting international crimes are severe enough already. Ratko Mladić and Jean-Paul Akayesu, for example, have been sentenced to life imprisonment by the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR), respectively. The repercussions of their criminal conduct will never be in their past. Similarly, the criminal conduct of Bosco Ntaganda, who in 2043 will be released at the age of 70 after serving 30 years in prison following his conviction by the International Criminal Court,[70] will remain a legitimate matter of public interest for the rest of his life, justifying retention of his personal information online under the existing standard based on the severity of the punishment. Even if that conduct were not considered under the rubric of "international crimes," a request for the removal or de-linking of information relating to Ntaganda would probably be rejected. However, not all convictions for international crimes lead to life sentences or decades-long imprisonment. In the ICTY, some individuals have been sentenced to imprisonment for periods ranging between two and six years.[71] The ICTR, too, sentenced some individuals to less than 10 years' imprisonment.[72] Domestic courts have convicted individuals for "minor" acts that constituted international crimes and have imposed much lighter sentences.[73] The persons mentioned in the introduction to this chapter have been sentenced to short periods of imprisonment. Their past might not haunt them forever if online information linking them to it is not easily available.

At the time of the negotiations over the 1968 Convention, the drafters must have been aware that criminal proceedings against perpetrators of

70 Prosecutor v. Bahar Idriss Abu Garda, ICC-02/05-02/09-243-Red, Decision on the Confirmation of Charges, Public Redacted Version, PTC I, ¶ 233 (Feb. 8, 2010), https://www.icccpi.int/CourtRecords/CR2010_00753.pdf [hereinafter Prosecutor v. Bahar Idriss Abu Garda].

71 *E.g.*, Amir Kubura—two years (Apr. 22, 2008); Rasim Delić—three years (Sept. 15, 2008; appeal terminated on death, June 29, 2010); Enver Hadžihasanović—3.5 years (Apr. 22, 2008); Dragoljub Prcać—five years (Feb. 28, 2005); Veselin Šljivančanin—five years (Sept. 27, 2007); Milan Gvero—five years (appeal terminated on death, March 7, 2013); Milojica Kos— six years (Feb. 28, 2005); Simo Zarić—six years (Nov. 28, 2006); and Lahim Brahimaj—six years (Apr. 3, 2008), https://www.icty.org/en/cases.

72 For aggregated data on sentencing by crime category, hierarchy, and more, see Barbora Holá, Alette Smeulers & Catrien Bijleveld, *International Sentencing Facts and Figures: Sentencing Practice at the ICTY and ICTR*, 9 J. INT'L CRIM. JUST. 411 (2011).

73 For example, in 2007 Corporal Donald Payne was sentenced by a UK court to 12 months' imprisonment for the offense of inhuman treatment of persons protected under the Geneva Conventions.

international crimes might not always culminate in lengthy sentences, as even in the IMT, there have been some relatively short sentences.[74] The fact that ultimately the Convention does not distinguish between acts that constitute international crimes by their gravity indicates that the drafters attached categorical significance to such acts. In the same vein, it could be argued that when considering the public's interest in knowing against the individual's right to privacy, the classification of the act as an international crime, while by itself not tipping the balance in favor of freedom of expression and the right to know, should add weight to that consideration, irrespective of the specific punishment that was meted out to the individual.

D PUBLIC SAFETY

Public interest in a crime is greater, and justifies retention of information for longer, when there is a risk of the former offender repeating the crime.[75] When assessing the legitimacy of interfering in a person's privacy in order to avoid a speculative risk, the relevant factors include not only the gravity of the act but also the given offender's propensity to repeat the transgression. This propensity depends on the traits of the individual, as well as on their social circumstances.

There is reason to assume that perpetrators of international crimes are not particularly prone to relapse into criminal conduct. International crimes are, for the most part, committed in the context of communal strife or conflict (though not necessarily armed conflict). Perpetrators of international crimes are not typically the victims of adverse circumstances or bearers of any personal traits that are regarded as the "common" breeding grounds of criminality. In fact, perpetrators of international crimes often act not in a personal capacity but as organs (even if low-ranking ones) of a public authority engaged in the conflict.[76] Outside the context of communal conflict, and stripped of their apparent authority, they might well be ordinary, law-abiding individuals. This does not detract from their responsibility for their past conduct, but there is no reason to assume that

74 For example, Josef Alstötter, Chief of the civil law and procedure division of the German Ministry of Justice, was sentenced to five years; Curt Rothenberger, President of the Court of Appeals in Hamburg and later State Secretary in the German Ministry of Justice, was sentenced to seven years' imprisonment.

75 Jones, *supra* note 15, at 141.

76 J.Y. Dautricourt, *L'orientation moderne des notions d'auteur de l'infraction et de participation à l'infraction en droit international pénal*, 27 Revue Internationale de Droit Public 90, 106–7 (1957). The public authority may be self-styled rather than a recognized government.

absent the enabling environment, they would be more prone to repeat the act than anyone else would be. Thus public safety does not seem to carry particular weight in terms of the online preservation of the personal information of perpetrators of international crimes.

CONCLUSION

The removal and de-linking of personal information available online is an imitation of human memory loss. These measures are grounded in the view that the fading of memory can be a useful feature of the human character.[77] Yet, unlike natural memory loss, removal of information from the visible public sphere requires active choices as to which information should be removed and when. These decisions, regardless of the particular institutional form in which they take place, involve the balancing of competing rights and interests. This chapter considers these rights and interests as they pertain to information about individuals who have been convicted and punished for committing international crimes. It concludes that no special rules need to be applied to international crimes. However, international crimes do have certain characteristics that should shift the balance away from the right to privacy and towards freedom of expression. These are the importance of public access to information on international crimes in the context of transitional justice processes, and the gravity of the category of crimes to which these acts belong.

77 Liam J. Bannon, *Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing*, 2(1) Int'l J. CoCreation Design & Arts 3–15 (2006).

Chapter 15

The Right Not to Forget: Cloud-Based Service Moratoriums in War Zones and Data Portability Rights

Amir Cahane[1]

INTRODUCTION

Long gone are the days when individuals relied exclusively on tangible media as memory extensions. Little black telephone books, daybooks, photo albums, filing cabinets, and (actual) folders are mostly relics of the past. Everyday to-do lists, addresses, personal documents, and photographs are more likely to be preserved in digital forms. Increasingly, these personal digital archives are stored online, in "the cloud."[2]

1 Researcher, Israel Democracy Institute; Research Fellow, Federmann Cyber Security Research Center in the Law Faculty of the Hebrew University.

2 See, for example, Cisco's estimate (in 2016) that by 2020, the majority of residential internet users would be using cloud storage. Thomas Barnett, Jr., Shruti Jain, Arielle Sumits, Usha Andra & Taru Khurana, *Cisco Global Cloud Index 2015–2020*, CISCO PUBLIC 39 (2016), https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco. A recent survey by Statistics Finland indicates that 45 percent of respondents use personal online storage services. However, within the 16-to-54 age group, personal online storage users form a majority. *Share of People Who Used the Internet for Personal Online Storage Services in Finland from 2018 to 2020, by Age Group*, STATISTA (2020), https://www.statista.com/statistics/558062/ (last visited Sept. 15, 2021).

If a large-scale humanitarian disaster occurs, such as a massive missile strike in the heart of a major metropolitan area, many individuals are likely to focus their efforts on survival. In the aftermath, those dislocated individuals may find themselves without stable electricity and communications infrastructure for weeks and months, and the financial institutions they depend on may be paralyzed. Those individuals may be more preoccupied with their basic physical needs than with their internet access and even less so with their online cloud-based accounts. Will those accounts survive this prolonged period of forced inactivity?

This chapter aims to introduce a new digital right—the right not to forget. The right not to forget recognizes the value of one's personal data stored on the cloud and ensures its protection from arbitrary deletion or purging. Part I of this chapter addresses the growing reliance of individuals on cloud-based storage services and social media and outlines three paradigms under which these personal storage spaces can be conceptualized: as a proprietary personal document archive, as an extension of the self, or as social data. Part II outlines the terms and conditions pursuant to which cloud-based service providers may terminate, purge, or delete accounts and personal data on the cloud due to prolonged inactivity periods or the user's default on payments. Part III focuses on the consequences of applying these terms and conditions within the context of humanitarian disasters by noting the importance of cloud-based personal data storage to survivors of such events. Part IV outlines a proposed moratorium mechanism under which personal data storage service providers shall retain all accounts related to a qualifying humanitarian disaster. Part V explores possible legal venues to ground this mechanism.

I
SOCIAL MEDIA AND CLOUD STORAGE AS EXTENSION OF THE SELF

Cloud computing is an IT architecture that provides for on-demand network access to a shared array of configurable computer resources, such as online processing or storage.[3] Although the "cloud" metaphor for online

3 Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, NATIONAL INSTITUTE

distributed computing services, including online data storage, was coined in the late 1990s,[4] it was only after the rise of Web 2.0 in the decade of the 2000s and the emergence of smart mobile devices in the early 2010s that personal cloud computing services became ubiquitous.[5]

A large share of personal cloud storage services, such as Google One, Google Drive, Microsoft One Drive, and iCloud,[6] are integrated by their providers into other products and services. Dropbox, a personal storage service that is not operated by such tech giants, offers a user interface that emulates local on-device storage.

Some of these cloud storage services are mediated to their users via different platforms—email services, messaging apps, smartphone cameras, social networking platforms, and other applications whose secondary function may be any of the above. Even before the smartphone era, scholarly studies noted people's dependence on their mobile devices.[7] As mobile devices became a gateway to a myriad of cloud-based internet services, users' dependence on them has increased:[8] smartphones have become an extended memory artifact,[9] which facilitates a variety of short-term mnemonic techniques for personal memory[10] and supports the development of new objects of memories[11] but also serves as an extended long-term, autobiographical memory cache.

Delegating personal memory to the scaffolding of memory technologies, from books to Google searches, has been criticized as potentially undermining both personal identity and collective cultural practices.[12]

of Standards and Technology (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last visited Sept. 15, 2021).

4 The earliest reference to "data clouds" is attributed to Andy Hertzfeld. *See* Steven Levy, *Bill and Andy's Excellent Adventure II*, Wired (Sept. 4, 1994), https://www.wired.com/1994/04/general-magic/ (last visited Sept. 15, 2021).

5 See early predictions by Forrester Research, *Personal Cloud Services Emerge to Orchestrate Our Mobile Computing Lives* (2012).

6 *See* Statista, *Tech Giants in the U.S. 2019 Report* 19 (2019).

7 *See, e.g.*, James B. Rule, *From Mass Society to Perpetual Contact: Models of Communication Technologies in Social Context*, *in* Perpetual Contact: Mobile Communication, Private Talk, Public Performance 242–54 (James E. Katz & Mark A. Aakhus eds. 2004); Jon Agar, Constant Touch: The Global History of the Mobile Phone (2003).

8 Astrid Carolus, Jens F. Binder, Ricardo Muench, Catharina Schmidt, Florian Schneider & Sarah L. Buglass, *Smartphones as Digital Companions: Characterizing the Relationship between Users and Their Phones*, 21 New Media & Soc. 914–38 (2018).

9 Natalia Juchniewicz, *Extended Memory: On Delegation of Memory to Smartphones*, 25 Techné: Research in Phil. & Tech. 308–31 (2021).

10 Arlene R. Lundquist, Emily J. Lefebvre & Sara J. Garramone, *Smartphones: Fulfilling the Need for Immediacy in Everyday Life, but at What Cost?*, 4 Int'l. J. Humanities & Soc. Sci 80–89 (2014); Amanda J. Barnier, *Memories, Memory Studies and My iPhone: Editorial*, 3 Memory Studies 293–97 (2010).

11 For example, the constant record-keeping of instant messaging conversations influences the construction of memories. *See* Chris Drain & Charles Strong, *Situated Mediation and Technological Reflexivity: Smartphones, Extended Memory, and Limits of Cognitive Enhancement*, *in* Social Epistemology and Technology: Toward Public Self-Awareness Regarding Technological Mediation, 187–96, 190 (Frank Scalambrino ed. 2016).

12 *See, e.g.*, Nicholas Carr, The Shallows: What the Internet Is Doing to Our Brains (2011);

However, these arguments were mostly raised within the context of technologies by which individual knowledge of common facts is eroded by delegation to computer systems, where one allegedly does not need to memorize sections from the classics, as they are available from a simple Google search. Heersmink argues that delegating one's private, autobiographical memory to external storage technologies is widening the constitutive base form of one's identity rather than outsourcing it,[13] while Mayer-Schönberger expresses concerns that digital archives serve only as a veneer of memory while decontextualizing it.[14]

Regardless of the theoretical debate over its potential risks or harms to personal identity, reliance on cloud technologies for the backup of personal, private, long-term autobiographical memories and documents is prevalent. Cloud storage is used—via devices—for active self-documentation that later will be used for personal evocation of significant biographical events.[15]

Alongside storing data that serves as an extension of the autobiographical memory of individuals, and thereby of their selves, cloud services also function as a personal backup archive of miscellaneous files,[16] such as medical, financial, or identification documents. These two aforementioned categories of memory—autobiographical and archival—correspond with notions of narrative memory and database memory. Within the context of personal data, autobiographical memory tends to be retained within a personal narrative that charges it with emotive power and serves as an extension of the self. Personal digital archives are organized mostly as database memory, of decontextualized items to be retrieved when needed, such as financial documents, academic or professional certificates, and medical history. The database paradigm alludes to a proprietary relation to one's personal data and accordingly may invoke property rights.

The effective management of personal digital archives is a complex task.[17] Indeed, many individual digital personal archives are amalgams

Nicholas Carr, Is Google Making Us Stupid? 302 Atlantic Monthly 56–62 (2008); Susan Greenfield, Mind Change: How Digital Technologies Are Leaving Their Mark on Our Brains (2015).

13 Richard Heersmink, *Distributed Selves: Personal Identity and Extended Memory Systems*, 194 Synthese 3135–51 (2017); Richard Heersmink & J. Adam Carter, *The Philosophy of Memory Technologies: Metaphysics, Knowledge, and Values* 13 Memory Studies 416–33 (2017).

14 Viktor Mayar-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (2019).

15 Juchniewicz, *supra* note 9, at 318; Heersmink & Carter, *supra* note 13, at 419.

16 See, for example, the study by Finley, Nazz, and Goh, in which 35 percent of respondents declared that they use cloud services for backup. Jason R. Finley, Farah Naaz & Francine W. Goh, Memory and Technology: How We Use Information in the Brain and the World 40 (2018).

17 *See, e.g.*, Catherine C. Marshall, *Rethinking Personal Digital Archiving, Part 1: Four Challenges from the Field*, 14 D-Lib Magazine (2008). For general criticism of the delegation of intimate activities,

of data stored in various databases and online storage services offered by a range of platforms and apps, in a manner that makes their retrieval challenging.[18] Nevertheless, even such mismanaged personal repositories, rather than being carefully curated by their owners, are accumulating personal data that is of immense value to their owners. This is unique data, of a very personal nature, which may be very hard to retrieve or recreate if lost.[19] This indicates that, despite the theoretical differentiation between database and narrative memories,[20] in practice, personal data is not stored in a manner that allows this distinction.

A third category of data preserved by cloud services should also be mentioned: social data. A myriad of social contacts, social interactions, and public or semi-public posts that individuals manage via social networking, instant messaging, or email platforms is documented in the cloud. The sum of these interactions becomes an individual digital persona.

The aforementioned categories of personal data stored on the cloud may reflect Dror-Shpoliansky and Shany's account of the three generations of digital rights.[21] While first-generation digital property rights may apply to personal digital archives[22] functioning as databases, second-generation digital rights, such as the German notion of the right to informational self-determination,[23] may serve to further protect personal data stored in the cloud that functions as an extension of the self. The third category of social data may call for further protection within third-generation digital rights for digital personae.[24] However, there may be other digital rights that apply to all categories, such as the second-generation right to data portability.[25]

see Arlie Russell Hochschild, THE OUTSOURCED SELF: WHAT HAPPENS WHEN WE PAY OTHERS TO LIVE OUR LIVES (2013).

18 This is especially the case when an individual personal digital archive is a cumulative cache of short-term memory artifacts, such as digital photos of identification documents a user may send to herself via email or instant messaging apps before traveling abroad. These artifacts may be useful for the long term yet difficult to retrieve in lieu of a personal management system.

19 For example, the possibility of losing one's personal photos (which evokes the "saving the photo albums from a burning house" trope) raises individual anxiety. Some have expressed "intense fear of losing their digital images": Emily Keightley & Michael Pickering, *Technologies of Memory: Practices of Remembering in Analogue and Digital Photography*, 16 NEW MEDIA & SOC. 576–93, 582–83 (2014). In a market research survey cited by Lury, 39 percent of respondents claimed their (tangible) family albums to be their "most treasured possession." CELIA LURY, PROSTHETIC CULTURE: PHOTOGRAPHY, MEMORY AND IDENTITY 82 (1998).

20 LEV MANOVICH, THE LANGUAGE OF NEW MEDIA 194–202 (2002).

21 Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights—A Proposed Typology*, EUR. J. INT'L L. (forthcoming 2022).

22 *See, e.g.*, Dixon v. R. [2015] NZSC 147, [2016] 1 NZLR 678, at 25.

23 65 BVerfGE, 1 (1983); DONALD KOMMERS & RUSSELL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 408–11 (2009).

24 *See, e.g.*, The Internet Rights & Principles Dynamic Coalition (IRPC) and the Internet Governance Forum (IGF), The Charter of Human Rights and Principles for the Internet, Art. 8(d) (2014).

25 The most notable codifications of the right to data portability are in the European Union's General Data Protection Regulation (GDPR) and in the Californian civil code (as part of the California Consumer Privacy Act (CCPA)). *See* Regulation 2016/679 of the European Parliament

II
DEFAULTING ON YOUR MEMORIES

Retail cloud service providers often offer freemium services, where users are first introduced to a rudimentary version of a product or a service and encouraged by their provider to acquire a premium version with additional features or enhanced performance. Dropbox, for example, offers a basic 2GB storage account for free, which may be upgraded to premium subscription plans of up to 2TB for personal users.[26] According to its 2020 annual SEC (Securities and Exchange Commission) filing, Dropbox has more than 700 million registered accounts, of which nearly 15.5 million are paying users.[27]

Personal cloud-based storage services that operate under the freemium paradigm strive to strike a balance between the cost of resources allocated to non-paying users and the revenue generated from premium accounts. While some cost-reduction strategies may aim to optimize performance, other such strategies will seek to identify and purge inactive non-paying accounts, thereby saving resources. Another strategy is to recalibrate the balance between premium and free accounts by changing the terms of use—narrowing the set of free features offered to non-paying users, in the hope of incentivizing them to pay.

Under Dropbox's terms of service, non-paying users who remain inactive on the site for prolonged periods (i.e., exceeding 12 months) may be subject to termination or suspension of their access to their accounts.[28] Similarly, Google states in its Gmail program policies that it may take action on accounts inactive for more than two years, including deleting email messages from the product.[29] Similar provisions stating that inactive accounts may result in the termination and deletion of data can be found in the terms of service of Yahoo online email service,[30] iCloud

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 O.J.L 119/1, Art. 20 [GDPR]; CAL. CIV. CODE § 1798.100(d) [CCPA]. For an overview of contemporary data portability legislation, see Peter Swire, *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations*, GA. TECH. SCHELLER C. OF BUS. RES. PAPER SERIES (Sept. 5, 2020), at 14–21, https://ssrn.com/abstract=3689171.

26 DROPBOX, INC., ANNUAL REPORT (Form 10-K) (Feb. 19, 2021).

27 *Id.*

28 *Dropbox Terms of Service*, DROPBOX (July 6, 2021), https://www.dropbox.com/terms (last visited Sept. 15, 2021).

29 *Gmail Program Policies*, GOOGLE, https://www.google.com/gmail/about/policy/ (last visited Sept. 15, 2021).

30 *Yahoo Terms of Service*, § 13, YAHOO, https://policies.yahoo.com/sg/en/yahoo/terms/utos/index.htm (last visited Sept. 15, 2021).

by Apple,[31] WhatsApp by Facebook,[32] Microsoft OneDrive,[33] and Amazon Cloud services.[34]

These terms of service typically contain provisions that allow their providers to change the terms and conditions applying for unpaid accounts. Recently, Google revised its once-unlimited Google Photos storage policy, declaring that as of June 1, 2021, any new photos backed up on Google Photos will count towards the free 15 GB storage quota generally allocated to the user's Google account.[35]

Data of paying users that is stored in premium cloud accounts may also be deleted when users exceed their allocated quota[36] or when they default on their payments. Under the iCloud terms of service, for example, Apple may terminate its services upon a failure to pay, provided that it has given the user a 30-day notice.[37]

While the above provisions allow providers of cloud-based services to terminate users' access to their personal data (which may be used under the self-extension, personal archive, or social paradigms) or delete such data, these actions are typically subject to prior notification or to a sufficiently long period of inactivity, thereby providing users with time to back up their data, transfer it elsewhere, or cure any breach of contract.

Such backup mechanisms are usually made available by service providers pursuant to data portability rights, such as those under the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).[38] Data portability, as a legal term of art, allows an individual to take his or her data from a service provider and transfer—or "port"—it elsewhere.[39] While the right to data portability is considered a possible antitrust measure, which paves the way for the interoperability of online platforms and services and increasing competition between them,[40] it also allows users to control their own data. Users

31 *Welcome to iCloud*, APPLE, https://www.apple.com/legal/internet-services/icloud/ (last visited Sept. 15, 2021).
32 *Terms of Service*, WHATSAPP (Jan. 4, 2021), https://www.whatsapp.com/legal/updates/terms-of-service/?lang=en (last visited Sept. 15, 2021).
33 *Microsoft Services Agreement*, § 4.a.ii., MICROSOFT (Jun. 15, 2021), https://www.microsoft.com/en/servicesagreement/ (last visited Sept. 15, 2021).
34 *File Retention Policy*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202146630 (last visited Sept. 15, 2021).
35 *Updated Storage Policy for Google Photos*, GOOGLE, https://support.google.com/photos/answer/10100180?hl=en (last visited Sept. 15, 2021).
36 *See, e.g.*, *How Your Google Storage Works*, GOOGLE, https://support.google.com/googleone/answer/9312312?hl=en (last visited Sept. 15, 2021); AMAZON, *supra* note 34; MICROSOFT, *supra* note 33, at § K.i.
37 APPLE, *supra* note 31, § B(g).
38 See *supra* note 25.
39 Gennie Gebhart, Bennett Cyphers & Kurt Opsahl, *What We Mean When We Say "Data Portability,"* ELEC. FRONTIER FOUND. (Sept. 13, 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability (last visited Sept. 15, 2021). *See also* Swire, *supra* note 25, at 8.
40 *See, e.g.*, Swire, *supra* note 25, at 12–13; Maurice E. Stucke & Allen P. Grunges, *No Mistake About*

may autonomously exercise control[41] over their data[42] stored in online platforms by porting between services, as well as by downloading it for backup purposes. However, the temporal reach of the right to data portability appears to be, prima facie, limited to the right of the user to port any applicable data stored at the moment of porting. This is supported by the common understanding of data portability rights as facilitators of competition in the market economy: the exercise of those rights should allow users to switch, in real time, between service providers.

III
THE PRECARIOUSNESS OF THE DISLOCATED AND THE SUPPORT OF THE CLOUD

Barton's two-dimensional typology of collective stress situations encompasses a wide range of disasters in which "many members of a social system fail to receive expected conditions of life from the system."[43] Within Barton's broad definition, disasters differ in their societal scope and duration. Disasters of wide societal scope that are brief, such as large-scale violent conflicts, massive natural disasters, or complex humanitarian emergencies in which violence exacerbates the latter,[44] adversely affect the livelihood of individuals and lead to their mass deprivation of basic necessities and, at times, to mass displacement scenarios. Individuals seeking refuge from such calamitous events are likely to have lost contact with family and friends, some of whom may have perished. These

It: The Important Role of Antitrust in the Era of Big Data, Antitrust Source, April 2015; Inge Graef, *Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets*, *in* Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? 121–51 (Mor Bakhoum, Beatriz Conde-Gallego, Mark-Oliver Mackenrodt & Gintarė Surblytė-Namavičienė eds. 2018).

41 Helena U. Vrabec, Data Subject Rights under the GDPR 181–86 (2021).

42 As to the scope of users' data under the right to data portability, see Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay & Ignacio Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 Comp. L. & Sec. Rev. 193–203 (2018); Vrabec, *supra* note 41, at 167–68.

43 Allen H. Barton, *Disaster and Collective Stress*, *in* What is a Disaster? New Answers to Old Questions 125–52 (Ronald W. Perry & E.L. Quarantelli eds. 2005).

44 On the concept of complex humanitarian emergencies, see Sue Lautze & Angela Raven-Roberts, *Violence and Complex Humanitarian Emergencies: Implications for Livelihoods Models*, 30 Disasters 383–401 (2006); Richard J. Brennan & Robin Nandy, *Complex Humanitarian Emergencies: A Major Global Health Challenge*, 13 Emergency Medicine 147–56 (2001).

individuals may be out of money, displaced, and challenged by a variety of health, psychological, and/or livelihood problems. Such individuals may eventually be recognized as refugees or remain, albeit dislocated from their homes, in their country.

During catastrophes, individuals often strive to hold on to personal memory artifacts—personal documents and photographs.[45] Such artifacts may hold the only record of a loved one lost in the calamities.[46] Personal identities, in a post-traumatic context, may be reaffirmed through the re-creation of personal memory. Such re-creation can be fragmented and dependent on the availability of relevant documents in community archives,[47] or on individual ability to retain possession of tangible memory artifacts during a crisis. A richer path to fuller memory reconstruction and the partial restoration of individual pre-catastrophe identity can be found in their extended memories stored in the cloud.

If national archives are destroyed, academic registers, financial databases, and similar record-keeping institutions during conflicts, personal documents that provide proof of birth, professional qualifications, academic degrees, medical history, or possession of assets cannot be replicated. At times, the only copy of such records is available in personal digital archives. While functioning under the paradigm of personal digital archives, cloud-based storage services are invaluable to survivors of humanitarian catastrophes. The aforementioned documents may, in time, prove crucial to the process of rehabilitating displaced individuals trying to re-establish themselves in a new country, or of redeeming lost property.

Furthermore, proper documentation is an important factor in the status determination of individuals seeking international protection.[48] In many cases, individuals applying for refugee status have few if any documents to support their statement, and their status determination depends on an assessment of applicants' credibility.[49] On the other hand, decision-makers who assess applicants' credibility tend to have unreasonable expectations of human memory, whose accuracy can be limited

45 Hariz Halilovich, *Re-Imaging and Re-Imagining the Past after "Memoricide": Intimate Archives as Inscribed Memories of the Missing*, 16 ARCHIVAL SCI. 77–92, 89 (2016).

46 Hariz Halilovich, *Reclaiming Erased Lives: Archives, Records and Memories in Post-War Bosnia and the Bosnian Diaspora*, 14 ARCHIVAL SCI. 231–47, 234 (2014).

47 Halilovich, *supra* note 46, at 85.

48 *See, e.g.*, Council Directive 2011/95/EU, Art. 4, 2011 O.J. (L 337/9) 9, 14.

49 Michael Kagan, *Is Truth in the Eye of the Beholder? Objective Credibility Assessment in Refugee Status Determination*, 17 GEO. IMMIGR. L.J. 367 (2002–2003); Cécile Rousseau, François Crépeau, Patricia Foxen & France Houle, *The Complexity of Determining Refugeehood: A Multidisciplinary Analysis of the Decision-Making Process of the Canadian Immigration and Refugee Board*, 15 J. REFUGEE STUD. 43–70 (2002); Bruno Magalhães, *The Politics of Credibility: Assembling Decisions on Asylum Applications in Brazil*, 10 INT'L POL. SOCIOLOGY, 133–49 (2016); John R. Campbell, *Examining Procedural Unfairness and Credibility Findings in the UK Asylum System*, 39 REFUGEE SURV. Q. 56–75 (2020).

for certain categories of information.[50] The availability of personal documents retrieved from cloud-based storage services may tip the balance in favor of applicants, who may be able to provide objective evidence supporting their request.

Social data may also be of immense importance to survivors of humanitarian disasters.[51] Survivors may use their pre-catastrophe online contacts to locate missing persons and reunite with relatives and loved ones—a process much more targeted and potentially fast-paced than the search bureaus established following World War II that relied on mass media broadcasts to assist survivors in reuniting with their families.[52] Furthermore, subject to the availability of internet access within the disaster zone, social data can be of use to individuals in areas undergoing crisis to request assistance from contacts abroad, as well as to provide real-time eyewitness reports. Another benefit of stored social data is as a basis to create online communities of survivors—providing a collective space for individuals to process the trauma,[53] preserve their collective identity and heritage,[54] and establish local refugee communities to assist their members in the transition to a new host country. In these digital communities, survivors can network and exchange practical information that allows for a smoother relocation and socialization abroad.

Viewed either as extended memory, as a personal digital archive, or as social data, the information retained in personal accounts of cloud-based platforms and services can vastly improve the living conditions and personal well-being of survivors of humanitarian disasters. However, during such disasters, personal resources are likely to be diverted into long-term real-life self-preservation efforts in an unstable, hostile environment. Individual online self-preservation activities, such as the maintenance of personal online accounts and presence, are most likely to be deprioritized and at times—in cases of the collapse of internet and electricity infrastructure—untenable. While fleeing, refugees may lack devices that allow

50 Hilary Evans Cameron, *Refugee Status Determinations and the Limits of Memory*, 22 INT'L. J. REFUGEE L. 469–511 (2010).

51 *See also* LINDA LEUNG, CATH FINNEY LAMB & LIZ EMRYS, TECHNOLOGY'S REFUGE: THE USE OF TECHNOLOGY BY ASYLUM SEEKERS AND REFUGEES 8–12 (2009).

52 Compare with the relatively successful efforts of the Jewish Agency's Search Bureau for Missing Relatives, which achieved a success rate of 30 percent within less than a decade of operations. Tehila Darmon Malka, *Missing Persons and World War II: Between Personal and National Loss*, WAR IN HISTORY (forthcoming 2022); *Search Bureau for Missing Relatives*, CENTRAL ZIONIST ARCHIVES, http://www.zionistarchives.org.il/en/AttheCZA/AdditionalArticles/Pages/ChipushKrovim.aspx (last visited Sept. 15, 2021).

53 *See, e.g.*, Victoria Bernal, *Nationalist Networks: The Eritrean Diaspora Online*, in THE NEW MEDIA AGE: IDENTITY, POLITICS, AND COMMUNITY 122–35 (ANDONI ALONSO & PEDRO J. OIARZABAL EDS. 2010).

54 Xabier Cid & Iolanda Ogando, *Migrate Like a Galician: The Graphic Identity of the Galician Diaspora on the Internet*, *in* THE NEW MEDIA AGE: IDENTITY, POLITICS, AND COMMUNITY 317–36 (ANDONI ALONSO & PEDRO J. OIARZABAL EDS. 2010).

internet access and may go for long periods of rarely using the internet; moreover, such usage may be limited to information-gathering efforts regarding their destination or planning their escape.[55]

This also applies to the preservation of cloud-based premium accounts, which, as outlined in Part II above, may be terminated or deleted by service providers pursuant to users' default on their payments—either due to the collapse of national financial institutions or the allocation of personal resources for stressing and immediate survival needs.

As not only survivors of humanitarian disasters may default on their payment in installments for premium cloud services, or undergo prolonged online inactivity, it may be argued that the termination policies outlined in Part II above are reasonable when applied to ordinary users. Under the various terms of service and policies, ordinary users, those who are not suffering the consequences of humanitarian events, are typically given sufficient time to either exercise their data portability rights and backup their data locally or transfer their cloud data elsewhere. It may be prudent to consider a solution for individuals undergoing personal crises such as imprisonment or long periods of hospitalization that prevent them from accessing their accounts. However, survivors of collective stress situations are situated in a more precarious situation than those unfortunate individuals, and their personal data stored in cloud-based services—possibly a key factor in their rehabilitation—may be the only surviving copy of documents and photographs that cannot be replicated or recreated elsewhere.

IV
LONG-TERM RETENTION OF CLOUD-BASED ACCOUNTS IN HUMANITARIAN DISASTERS

Given the importance of personal digital storage to its owners—as an extension of the self, a proprietary record-keeping mechanism, or an

55 *See* Martin Emmer, Marlene Kunst & Carola Richter, *Information Seeking and Communication during Forced Migration: An Empirical Analysis of Refugees' Digital Media Use and Its Effects on Their Perceptions of Germany as Their Target Country*, 16 GLOBAL MEDIA AND COMMUNICATION 167–86 (2020). Note that this study is limited to the internet access and usage habits of refugees who managed to reach Germany.

amalgam of social contacts—its preservation in times of crisis is imperative. Commercial practices of purging personal data upon the termination of payment or after a predefined period of inactivity should not be curtailed when users are unable to sustain their online activity due to a large-scale collective stress situation. This part will outline principles for a proposed moratorium mechanism under which, in areas of humanitarian disaster, personal accounts of online services and their respected data will be retained for future use.

Under the proposed moratorium mechanism, once a qualifying humanitarian disaster is identified, cloud-based service providers will refrain from any deletion of data or purging of personal accounts or users that may be affected by the event. Their data will be retained for enough time to allow survivors access to their personal accounts and data. Accordingly, defining the geographical domain of the moratorium could evolve as the event progresses.

A qualifying humanitarian disaster should be defined as any large-scale conflict or natural or manmade disaster that is likely to subject a substantial number of individuals to prolonged periods without online access or, due to the collapse of national infrastructures, to render those individuals unable to keep up payments on their premium accounts. There is room to consider in further detail which events will constitute qualifying humanitarian disasters; however, the definition should capture circumstances in which many individuals are likely to lose access to their cloud-based accounts. It may also be advisable to consider a declaration mechanism by an independent international body. Such a body could be under the auspices of the UN or the World Trade Organization or be entirely independent thereof (such as an association of leading cloud services providers). It is likely that the identity of such a body would be determined by the obligatory force of the moratorium mechanism.

Given that most online service providers allow minimal inactivity periods of a year before taking any action on non-paying users, a declaration of a crisis as a qualifying humanitarian disaster may be made within a reasonable period from the start of the events, when its magnitude can be thoroughly evaluated.

However, during conflicts, accounts of cloud-based services can be weaponized for odious purposes, such as the coordinated online campaign against the Rohingya ethnic group of Myanmar.[56] Implementing

56 *See in re*: Application Pursuant to 28 U.S.C. § 1782 of Republic of the Gambia v. Facebook, Inc. Case 1:20-mc-00036-JEB-ZMF, ¶ 12 (Sept. 11, 2021).

the moratorium mechanism should not preclude the application of content moderation policies—either for hate speech or for illegal content—by cloud-based service providers. Nevertheless, as such accounts may contain evidence to be used later in international criminal proceedings, cloud-based service providers should block access to such accounts while retaining the data for potential evidentiary purposes.

There could be, however, instances in which accounts need to be deleted or blocked in order to protect their users. Databases containing personal data can expose the political affiliation of their data subjects and thereby be weaponized to persecute individuals.[57] Safeguards should be put in place so that data preserved under the proposed moratorium mechanism cannot be accessed for nefarious purposes. First, the purpose of the moratorium is to prevent any arbitrary account deletion or blocking by service providers. Accordingly, it does not preclude users from deleting their accounts or limiting public access to their data if they wish to do so. If these users cannot do so (as their ability to access and control their accounts is assumed to be limited), it may be advisable to lay out procedures for surgically limiting public access to specific jeopardized accounts (and in extreme cases, even temporally limiting private access to these accounts) subject to a request by a trusted flagger.[58]

It should be noted, prior to defining in further detail the various components of the moratorium mechanism proposed above, that these elements should be rigidly designed, rather than leaving their calibration to the discretion of service providers. It may be tempting to allow service providers to use machine learning techniques to determine, for example, how long it took, following a prolonged inactivity period subsequent to a humanitarian disaster, before users regained control and access to their accounts. However, given the diverse online behavior patterns of users with varying cultural backgrounds and different crisis scenarios, the ability to infer from past localized events is questionable. In normal times, the balance between users and service providers may place some burden on users to access their accounts or ensure that regular payments are made. However, in the context of humanitarian disasters, that balance should be revisited in a manner that takes all the burden off the now-displaced users.

57 *See, e.g.*, Frank Bajak, *US-Built Databases a Potential Tool of Taliban Repression*, AP (Associated Press), Sept. 7, 2021.

58 On trusted flaggers, see European Commission, Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act), Art. 19 COM (December 15, 2020), 825 final.

Accordingly, the protected users should be broadly defined—both by actual evidence of their proximity to the disaster event, such as IP (Internet Protocol) addresses, and by presumption of proximity when their accounts are registered in the country in which the qualifying humanitarian disaster took place. Other indicators, such as the use of a unique regional language, may help identify protected users. The retention period should be uniform for all such users, with rigid temporal boundaries of several years.

Generally, the rationale underlying the moratorium mechanism does not preclude the possibility that users may waive their right not to forget, as an exercise of their personal autonomy. However, there may be other considerations that may provide support against allowing individuals to waive this right, or at least to restrict it to an ex-ante waiver only, as the retained data may be used for international criminal investigations or even as a digital time capsule for future historians. Nevertheless, any such waiver should be on an opt-out basis and designed in a neutral manner, avoiding "dark patterns" designed to encourage users to opt out.

While the range of applicable online services may be wide, ranging from emails and virtual storage services to social media and messaging platforms, which cloud-based service providers will fall within the scope of the proposed moratorium mechanism should be considered carefully. By definition, these service providers are likely to be operating outside of the disaster zone and therefore almost certain to be international businesses. Any applicable platform operated by a leading multinational provider (which can be defined by revenue, net worth, or global number of users) should be within the scope of the moratorium mechanism. Supplementary criteria should be in place to identify online services that are in common use in the disaster region, which might be operated by either local or international providers.[59]

Although the costs of retail data storage continue to decrease,[60] and cloud-based services rely on the freemium model, under which a small fraction of their users pay for additional premium services,[61] declaring

59 The now-defunct Orkut SNS is an example of a social media cloud-based service that gained local popularity exceeding that of leading international platforms (with high penetration rates in Brazil during its operation). Other examples of locally popular cloud-based SNS services include the Japanese GREE, the South Korean KakaoTalk, and the Russian Odnoklassniki and VKontakte. Petros Iosifidis & Mark Wheeler, Public Spheres and Mediated Social Networks in the Western Context and Beyond 180, 182, 236–38, 243–44, 248–49 (2016); Javier Bustamante, *Tidelike Diasporas in Brazil: From Slavery to Orkut*, in Diasporas in the New Media Age: Identity, Politics, and Community 170–89, 175–79 (Andoni Alonso & Pedro J. Oiarzabal eds. 2010).

60 See, for example, the historical hard drive prices presented by John C. McCallum, *Price-Performance of Computer Technology*, *in* The Computer Engineering Handbook: Digital Design and Fabrication 4-12–4-13 (Vojin G. Oklobdzija ed., 2nd ed. 2008).

61 Dropbox, *supra* note 26.

long-term data retention applicable for millions of accounts of potential displaced users may prove costly for service providers. When a moratorium mechanism is designed in detail, it should include measures to prevent abuse by qualifying users who are not facing actual harm. However, any limitation on users' access to their online accounts should ensure that they retain complete access to their data, as well as the ability to communicate within the platform with other accounts. Furthermore, the financial loss incurred by the moratorium will likely be mitigated by the lower penetration rates of internet usage and social media in developing countries.[62]

The general framework proposed above for a cloud-services moratorium in disaster events suggests stretching the concept of data portability rights beyond its current temporal boundaries. Over time, users should be given greater autonomy to decide where their personal data is stored. As technology makes it possible to retrieve data, memories, and social contacts that are irreplaceable to dislocated persons, data portability options should include not only transferring the data in its present form from one service provider to the other but also porting it to a better future.

V
LEGAL BASIS OF THE RIGHT NOT TO FORGET?

This section aims to explore the legal basis of the right not to forget and whether the moratorium mechanism similar to the one generally outlined in Part IV can be established thereunder.

It may be tempting to consider shoehorning the right not to forget into existing international human rights frameworks. For example, under the personal digital archive paradigm that conceptualizes personal data stored in the cloud as digital property, the right not to forget can be protected as a first-generation digital right whose offline equivalent is well established as a human right in the Universal Declaration of Human Rights,[63] as well as in various regional legal instruments.[64] When framed

62 *Digital 2021 Global Overview Report*, WE ARE SOCIAL, https://wearesocial.com/digital-2021 (last visited Sept. 15, 2021).
63 G.A. Res. 217 (III) A, Universal Declaration of Human Rights, Art. 17 (Dec. 10, 1948).
64 Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms Art. 1, *opened for signature* Mar. 20, 1952, E.T.S. No. 009; American Convention on Human Rights,

under the paradigm of self-extension as a second-generation digital right, akin to the right to be forgotten or the right to informational self-determination,[65] the right not to forget can be either outlined as a reconfiguration of the latter or independently restated in future legal instruments. It might even be worthwhile to define this new digital right by framing personal digital archives as the extension of the self, thereby giving primacy to core values and fundamental rights of autonomy and self-determination.

Conceptualization of data as private property[66] is required to invoke potential international law protections but is not sufficient. For example, under Article 46 of the Hague Regulations, private property "must be respected [and] cannot be confiscated."[67] However, Article 46 has been applied to acts such as pillage or the manufacturing of weapons that caused substantial collateral damage to private property.[68] The deletion of data in the normal course of business is hardly in the same category.

An effective moratorium mechanism is unlikely to be enforceable under either international humanitarian law (IHL) and international human rights law (IHRL). While IHL lays out the responsibilities of parties to an armed conflict[69] and IHRL generally lays out State obligations,[70] the duty-holding parties under the proposed moratorium are private business entities, which are not expected to be engaging directly in a conflict and whose behavior is barely regulated under these two frameworks. Accordingly, at present such a moratorium mechanism can be firmly established only within a voluntary legal framework.

The UN Guiding Principles on Business and Human Rights (UNGP-BHR) calls for private business entities to "address adverse human rights impacts with which they are involved"[71] and, in particular, to "avoid causing or contributing to adverse human rights impacts through their

Art. 21, Nov. 22, 1969, 1144 U.N.T.S. 123; Organization of African Unity (OAU), African Charter on Human and Peoples' Rights (Banjul Charter) Art. 14, June 27, 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

65 *See, e.g.*, Dror-Shpoliansky & Shany, *supra* note 21, at 33–34.

66 On data as property see Blank & Jensen (ch. 3 of this collection).

67 Convention (IV) Respecting the Laws and Customs of War on Land, Annex: Regulations Concerning the Laws and Customs of War on Land Art. 46, Oct. 18, 1907, 36 Stat. 2277.

68 Jonathan Kolieb, *Don't Forget the Geneva Conventions: Achieving Responsible Business Conduct in Conflict-Affected Areas through Adherence to International Humanitarian Law*, 26 AUSTRALIAN J. HUM. RTS. 142–64 (2020).

69 *See, e.g.*, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, Art. 49.

70 *See, e.g.*, RENÉ PROVOST, INTERNATIONAL HUMAN RIGHTS AND HUMANITARIAN LAW 57–75 (2004).

71 *UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights* (E/CN.4/Sub.2/2003/12/Rev.2, 26.8.2003) and the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (by John Ruggie) [hereinafter *UNGPBHR*].

own activities, and address such impacts when they occur."[72] The adverse impact on human rights caused by the de-platforming, deletion, or suspension of cloud-based accounts can be mitigated or avoided by the moratorium mechanism outlined in Part IV above, thereby complying with the UNGPBHR principle requiring business entities to have in place policies and processes to meet their responsibility to respect human rights.[73] The UNGPBHR were presented as social norms that extended beyond black letter law,[74] as responsibilities rather than obligations. Accordingly, their normative force may be a step away from soft-law voluntarism, but it remains lacking and tilted toward the voluntary.[75]

In lieu of positive international law under which a mandatory moratorium mechanism could be established, as the human rights obligations of private corporate entities are mostly voluntary, another possible venue is regional or national legislation.[76]

Some regional or national data protection laws have extraterritorial reach.[77] However, their protection is typically limited by the nationality of the data subjects, rendering the overall extraterritorial blanket of data protection laws incomplete and leaving unprotected those regions and individuals that are more disaster-prone. Furthermore, mapping the right not to forget in existing second-generation digital rights yields incomplete results. First, contemporary data portability provisions, such as those in the GDPR, do not have a global reach. Secondly, they include certain limitations precluding them from providing a solid legal basis to the exercise of a right not to forget within the proposed moratorium. For example, data portability rights under both the GDPR and the CCPA are subject to the technical feasibility of their exercise.[78] The GDPR data

72 *UNGPBHR*, *supra* note 71, Principle No. 13(a).
73 *Id.* Principle No. 15.
74 *UN Commission on Human Rights, Report of the United Nations High Commissioner on Human Rights on the Responsibilities of Transnational Corporations and Related Business Enterprises with Regard to Human Rights—Business and Human Rights: Towards Operationalizing the "Protect, Respect and Remedy" Framework* (2009) (A/HRC/11/13), ¶ 46.
75 In the last 20 years, several attempts have been made to secure a consensual normative framework for attributing human rights duties to corporations. Most notable are the *UNGPBHR*, *supra* note 71. The UNGPBHR are both hailed as an important step away from soft law voluntarism and criticized for not offering real accountability mechanisms. *See* Florian Wettstein, *Normativity, Ethics, and the UN Guiding Principles on Business and Human Rights: A Critical Assessment*, 14 JOURNAL OF HUMAN RIGHTS 162–82 (2015); Surya Deva, *Treating Human Rights Lightly: A Critique of the Consensus Rhetoric and the Language Employed by the Guiding Principles*, *in* HUMAN RIGHTS OBLIGATIONS OF BUSINESS 78–104 (SURYA DEVA & DAVID BILCHITZ EDS. 2013).
76 *See, e.g.*, Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467 (2020).
77 *See, e.g.*, GDPR, Art. 3; Lei No. 13.709, de 14 de Agosto de 2018, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 15.8.2018 (Braz.), Art. 3. While the CCPA does not explicitly state its geographic scope, it may have some extraterritorial reach. Erin Illman & Paul Temple, *California Consumer Privacy Act: What Companies Need to Know*, 75 BUS. LAW. 1637 1641 (2019–2020). *See also* Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection Regulation?* 114 AJIL UNBOUND 5–9 (2020).
78 CCPA, Art. 1798.100(d); GDPR, Art. 20(2).

portability right is limited to data provided by the data subject under contract or consent (rather than unqualified data and secondary data relating to the data subject),[79] and the CCPA data portability right applies to the 12-month period preceding the porting request (thereby not necessarily applying to older data stored in the cloud).[80]

However, the lack of positive international law obligating private international business entities to comply, and the insufficiency of regional or national legal instruments, does not preclude the proposed moratorium from being developed as a voluntary framework by all stakeholders.

The increasing attention to corporate performance in environmental, social, and governance (ESG) issues,[81] and the recent adoption of corporate social responsibility rhetoric by leading global business entities,[82] may facilitate the voluntary establishment of the proposed moratorium mechanism. In an era when social media platforms exacerbate genocidal incitement[83] and cloud storage providers contemplate the deployment of controversial surveillance techniques,[84] a voluntary mechanism established by cloud-based service providers may be incentivized by potential reputational gains.

CONCLUSION

This chapter has offered an account of an overlooked digital right—a right not to forget—and proposed an initial outline of a mechanism supporting it in humanitarian contexts. Questions regarding the technical nature of the optimal data governance system for service providers' compliance with the moratorium in the context of the physical survival of data in the cloud, or whether similar mechanisms should be applied in other

79 GDPR, Art. 20(1); *see also* De Hert, Papakonstantinou, Malgieri, Beslay & Sanchez, *supra* note 42.
80 CCPA, Art. 1798.130(a)(2).
81 *See, e.g.*, Giovanni Landi & Mauro Sciarelli, *Towards a More Ethical Market: The Impact of ESG Rating on Corporate Financial Performance*, 15 SOC. RESPONSIBILITY J. 11–27 (2019); Mozaffar Khan, *Corporate Governance, ESG, and Stock Returns around the World*, 75 FINANCIAL ANALYSTS J. 103–23 (2019).
82 *Business Roundtable Redefines the Purpose of a Corporation to Promote "an Economy That Serves All Americans,"* BUSINESS ROUNDTABLE (Aug. 19, 2019), https://www.businessroundtable.org/business-roundtableredefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans (last visited Sept. 15, 2021).
83 Neriah Yue, *The "Weaponization" of Facebook in Myanmar: A Case for Corporate Criminal Liability*, 71 HASTINGS L.J. 813 (2019–2020); Alexandra Stevenson, *Facebook Admits It Was Used to Incite Violence in Myanmar*, N. Y. TIMES, Nov. 6, 2018.
84 Matthew Panzarino, *Interview: Apple's Head of Privacy Details Child Abuse Detection and Messages Safety Features*, TECHCRUNCH, Aug. 10, 2021 (last visited Sept. 15, 2021).

scenarios of prolonged user inactivity, can and should be addressed by policy-makers and technical experts. Since it appears that such a proposed moratorium is likely to be based on service providers' goodwill, it is imperative to further design an optimal framework to be compared with its eventual voluntary application on the ground.

The right not to forget may be proven to offer additional benefits apart from securing the digital self in a manner contributing to its owner's struggle to survive calamity. Mass retention of personal data archives during a humanitarian crisis may allow the preservation of historical records[85] or of evidence to be used later in international criminal proceedings once the violence has ended.[86] In extreme cases of mass atrocities and genocide, the right not to forget may transform into the right not to be forgotten, resulting in a digital monument for cultures and lives destroyed in the conflict—a database from which academics and researchers could resurrect the memory of the dead.[87]

The reliance on external technologies to supplement and replace human memory calls for further protection of users' data from one-sided deletion or purging by service providers, especially when users are unable to respond in a timely fashion to providers' warnings. Another potential venue for the right not to forget is its application outside the humanitarian context—in situations in which users are unable to access internet services for an extended period, such as during incarceration or hospitalization.

However, the precariousness of refugees, internally displaced persons, and survivors of humanitarian disasters emphasizes the importance of the right not to forget. While cloud storage renders obsolete the trope of rescuing the family photo album from a burning house, without a mechanism ensuring that its digital successor remains stored in the cloud, our memory—and a part of ourselves—will fade away.

85 *See, e.g.*, Mathew Ingram, *Critics Say Facebook is Erasing Pieces of History by Deleting Pages about the War in Syria*, GIGACOM (Feb. 5, 2014), https://gigaom.com/2014/02/05/critics-say-facebook-is-erasing-pieces-of-history-by-deleting-pages-about-the-war-in-syria/ (last visited Dec. 15, 2021).

86 See, for example, the importance of access to deleted accounts and information that goes beyond public social media posting for international criminal proceedings in the case of *In re: Application Pursuant to 28 U.S.C. § 1782 of Republic of the Gambia v. Facebook, Inc. Case 1:20-mc-00036-JEB-ZMF* (Sept. 11, 2021). However, it should be noted that following that ruling, de-platformed personal accounts are not subject to the statutory controls of the Stored Communications Act (SCA) and are therefore easier to obtain in international criminal investigations, while accounts that are not deleted are subject to its protection.

87 See, for example, the comments to rule 142 (Respect for and protection of cultural property) in TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, cmt. to rule 142, ¶ 6, at 535 (MICHAEL N. SCHMITT ED. 2017). It may be that the sum of all online accounts of a nation qualifies as a unique digital manifestation of cultural property, and due to its collective volume, it is not as easily replicated as a digital reproduction of the *Mona Lisa.*

Recent armed conflicts in Iraq, Afghanistan, Palestine, and Ukraine have demonstrated the profound risks posed to the rights to privacy and data protection in contemporary warfare. Technological advances in the fields of electronic surveillance, predictive algorithms, big data analytics, user-generated evidence, artificial intelligence, cloud storage, facial recognition, and cryptography are redefining the scope, nature, and contours of military operations. Against this backdrop, international humanitarian law offers very few, if any, *lex specialis* rules for the lawful processing, analysis, dissemination, and retention of personal information. This book offers a first-of-its-kind account of the current and potential future application of digital rights in armed conflict situations and serves as a valuable reference piece for practitioners and scholars alike.

9 789916 956564