Protecting Civilian Data in Armed Conflict: A Corporate Duty of Constant Care?

What obligations does the duty of constant care stipulated in Additional Protocol I Article 57(1) impose on information and communications technology companies instructed by State parties to share customer data for intelligence purposes during an armed conflict?

Candidate Number: 144

Word Count: 14 958

JUS399 Masteroppgave

Faculty of Law

UNIVERSITY OF BERGEN

11.12.2023

Table of Contents

List of abbreviations

AP I	Additional Protocol I to the Geneva Conventions of 1949
CCPR	Human Rights Committee
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
GCs	Geneva Conventions of 1949
GNI	Global Network Initiative
IAC	International Armed Conflict
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
IHRL	International Human Rights Law
ISP	Internet Service Provider
MNO	Mobile Network Operator
NIAC	Non-International Armed Conflict
OECD	Organization for Economic Cooperation and Development
UNGP	United Nations Guiding Principles on Business and Human Rights
VCLT	Vienna Convention on the Law of Treaties of 1969

1 INTRODUCTION

1.1 Topic and Research Question

During armed conflict, intelligence gathering from digital sources is crucial. This information aids in distinguishing military objectives from civilians and civilian objects,[1] facilitating the implementation of necessary precautions,[2] and assessing the proportionality of attack.[3] In today's data-centric world, states are more than ever reliant on businesses to gain access to digital information. As a result, information and communications technology (ICT) companies in conflict zones are increasingly finding themselves amid geopolitical storms, contending with governmental demands to grant access to customers' data[4] – such as medical, legal, and financial data stored in clouds, ongoing communication between subscribers on apps, and real-time location information from mobile devices – impacting digital privacy rights.[5]

In the wake of the war in Ukraine, EU officials have stated that the invasion shows a "dividing line" between countries with privacy regulations and those prepared to misuse data, highlighting the need for world-wide convergence.[6] Moreover, the International Committee of the Red Cross (ICRC) has identified the misuse of data for purposes other than as means and methods of warfare by state and non-state actors, including "unprecedented levels of surveillance of the civilian population," leading to humanitarian consequences, as a risk of particular concern during armed conflict.[7]

While not precisely defined in international law, privacy essentially encompasses the notion that individuals should enjoy an area of personal development, interaction, and freedom from government intervention or unwarranted intrusion by other actors.[8] It serves as a safeguard for human dignity, and plays a crucial role in upholding personal security, preserving identity, and

[1] Additional Protocol I to the Geneva Conventions [AP I] Article 48.
[2] AP I Article 57(2)(a)(i).
[3] AP I Article 51(5)(b): "expected incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof [cannot] be excessive in relation to the concrete and direct military advantage anticipated."
[4] Carrillo (2022) 80; Satariano and Frenkel (2022).
[5] Velde (2022) 67-68; Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR] Article 8; International Covenant on Civil and Political Rights [ICCPR] Article 17.
[6] Stupp (2022).
[7] ICRC (2019) 895; Millett (2023); Solinge (2019); Other data misuse include political oppression, religious or political prosecution, blackmailing, discrediting through legal or reputational harm, discriminatory practices, and personalized persuasion, see Kröger, Miceli and Müller (2021) for a thorough review of consequences.
[8] Watt (2022) 174.

promoting freedom of expression.[9] Hence, the right to privacy is fundamental in democratic societies, shaping the power dynamics between authorities and individuals.[10]

The thesis explores the obligations of ICT companies confronted with government requests impacting customers' digital privacy during armed conflicts. Specifically, the concern lies in instances where governments leverage digital technologies, justified by, or claimed to be justified by, the necessities of armed conflict, to facilitate surveillance on civilians, potentially leading to real-world consequences like arrests, detentions, or discriminatory practices. The point of interest is when state parties to an armed conflict demand ICT companies to share customer data or circumvent them to gain direct access to such data, and whether the company in question is obligated to comply.

This raises questions about the adaptation of international humanitarian law (IHL) to the current and evolving landscape of modern conflict, specifically the status of digital privacy during armed conflict. While international human rights law (IHRL), including the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) Article 8 on the right to respect for private and family life and the International Covenant on Civil and Political Rights (ICCPR) Article 17 on the right to privacy, has been evolving at a swift pace to tackle the issues posed by new technologies, there is a noticeable deficiency in judicial and scholarly work concerning digital privacy under IHL.[11]

As appeals have been made to identify constraints within the current IHL frameworks to regulate the evolving data invasive practices during armed conflict,[12] this thesis delves into the examination of one possible constraint; the duty of constant care stipulated in Additional Protocol I (AP I) Article 57(1). The duty of constant care offers general protection to the civilian population from the impacts of armed conflict. At the 1975 Diplomatic Conference, the ICRC representative anticipated that the application of the general duty of constant care would later be specified through interpretation in practice.[13] The evolving importance of data, triggers an assessment of whether the duty of constant care comprises data privacy.[14] Moreover, to

[9] GNI Principles (2008).
[10] Hellestveit and Wilhelmsen (2022) 22.
[11] Lubin (2022a) 16; Lubin (2022b) 464.
[12] ICRC (2023); Lubin (2022a) 1.
[13] ICRC (1975) 182; Lubin (2022a) 10.
[14] Some scholars argue that the duty extends to data privacy, see Lubin (2022a) and Watt (2022).

establish the comprehensive legal framework under which the duty of constant care operates, the application of the human right to privacy during armed conflict must be considered.[15]

With the aforementioned in mind, this paper will answer the following research question: *What obligations does the duty of constant care stipulated in Additional Protocol I Article 57(1) impose on information and communications technology companies instructed by State parties to share customer data for intelligence purposes during an armed conflict?*

1.2 Example for Contextualization

To contextualize, an example of the situation at hand will be provided, which will be returned to in Section 4.4 to operationalize the rules delineated in the thesis. The following demands are put forward by State A:

State A demands to install surveillance equipment to gain direct access to information from mobile network operators (MNOs) and internet service providers (ISPs) within its territory, claimed to be justified by military necessity. Presupposing that the companies decline, State A requires real-time location information of subscribers from MNOs and ISPs. Finally, State A demands personal information from multiple ICT companies, including medical, legal, and financial data, as well as communication records.[16]

1.3 Digital Data and ICT Companies

Digital data is defined as "any information recorded by electronic or digital means [which] is retrievable, whether perceivable to a human or machine."[17] Personal data is "any information relating to an identified or identifiable natural person."[18]

ICT companies are an umbrella term for "manufacturing and services industries that capture, transmit and display data and information electronically."[19] ICT companies span internet-enabled technologies and the mobile domain powered by wireless networks, including ISPs and MNOs.[20] ISPs track subscribers' website visits, viewing habits, app usage, real-time and

[15] Carrillo (2022) 64; Vienna Convention on the Law of Treaties [VCLT] Article 31(3)(c).
[16] Inspired by Carrillo (2022) 98, but modified for the purpose of this thesis.
[17] Ritter and Mayer (2017) 224.
[18] General Data Protection Regulation 2016/679 [GDPR] Art. 4.
[19] OECD (2002) 8.
[20] Pratt (2019).

historical locations, search queries, and email content. Additionally, some ISPs combine subscriber data with third-party data, allowing for detailed insights into subscribers' sensitive information like race, religion, nationality, sexual orientation, financial status, billing and payment information, health, and political beliefs.[21] Similar data is typically gathered by MNOs, who manage the infrastructure that facilitates mobile phone and data connectivity, enabling customers to place calls, send text messages, and utilize the internet on their mobile devices.[22]

1.4 Business in Armed Conflict

1.4.1 Armed Conflict and Implications for Companies

During armed conflict, companies share a legal status akin to civilians, provided they refrain from direct participation in hostilities. IHL extends protection to the personnel, assets, and financial investments of companies. Protection as civilians may be temporarily lost if the company effectively contributes to a military attack amounting to direct participation, including "transmitting tactical targeting intelligence for a specific attack."[23] The act "must not only be objectively likely to cause harm directly, but it must also be specifically designed to do so in support of one party to an armed conflict and the detriment of another."[24] Conversely, if the information sharing supports hostilities in general terms but does not involve participation in a specific attack, the company retains its status of civilian nature.[25]

Still, company executives may face legal consequences, including criminal and civil liabilities in domestic or international courts for complicity in violations of IHL.[26] Complicity requires that the assistance had a "substantial effect on the perpetration of the crime" and "knowledge that these acts assist the commission of the offence."[27] The Lafarge and Lundin cases stand as significant markers in the effort to hold companies accountable. In May 2022, following four years of legal proceedings, the Paris Court of Appeal, affirmed accusations against the cement group Lafarge for aiding and abetting crimes against humanity. Allegedly Lafarge acquired

[21] US Federal Trade Commission (2021) 34.
[22] Ibid.
[23] ICRC (2009); German Military Manual (2013) 82; United States Military Manual (2023) 240.
[24] Fleck (2007) 689; ICRC (2009).
[25] Fleck (2007) 689.
[26] The thesis will not delve into rules on criminal and civil liability, nor legal accountability mechanisms.
[27] *Prosecutor v. Anto Furundzija* [ICTY], para. 249.

extraction permits of oil and pozzolan from ISIS and compensated them with fees.[28] September 5th, 2023, marked the beginning of a trial against two former executives of the Swedish oil company Lundin Oil in the Stockholm District Court, accused of violating IHL by providing financial and material support for war crimes, including looting, killing, rape, abduction of children, torture, and forced displacement, related to their oil exploration in South Sudan.[29] The cases show that companies offering services potentially related to the conduct of hostilities must exercise caution to avoid aiding parties in violating IHL.[30]

Third, the United Nations Guiding Principles for Business and Human Rights (UNGPs), endorsed unanimously by the United Nations Human Rights Council in 2011, are a set of global standards outlining states' and businesses' respective duties and responsibilities in preventing and addressing human rights abuses related to corporate conduct, through three pillars; "Protect, Respect and Remedy." Pillar I comprises principles related to states' "duty to protect" human rights. Pillar II comprises principles addressing companies' "responsibility to respect" all internationally recognized human rights, including ECHR Article 8 and ICCPR Article 17. Pillar III comprises principles designed to enable "access to remedy" for victims of human rights abuse. Although the UNGPs are not legally binding, representing *soft law*,[31] they shape and inform national and international laws, regulations, and policies, and serve as a reference point for corporate accountability.[32] Moreover, by integrating the UNGPs into internal policies, numerous companies are obligated to ensure compliance. To evaluate the obligations of ICT companies, this thesis will focus on Pilar II of the UNGPs, by analyzing how the "responsibility to respect" can be operationalized by ICT companies when ordered to share customer data with authorities.

In situations of armed conflict companies are expected to "respect the standards of international humanitarian law," as stated in the commentary to UNGP Principle 12, concerning legal frameworks included within corporate responsibility.[33] The same follows from the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, recommendations addressed by governments to multinational corporations to enhance sustainable development.[34]

[28] *Lafarge*, Paris Court of Appeal, 22 May 2022; ECCHR (2022).
[29] Harlem and Taylor (2022) 11.
[30] ICRC (2012) 1128.
[31] The term *soft law* encompasses non-binding quasi-legal instruments, contrasted with binding *hard law*.
[32] Macchi and Bright (2020) 218, Sarfaty (2022) 8.
[33] UNGP (2011) 14.
[34] OECD (2023).

Further stating that "[i]n the context of armed conflict […] enterprises should conduct enhanced due diligence in relation to adverse impacts, including violations of international humanitarian law."[35] To answer whether corporations have a duty to share or withhold customer data during armed conflict, one must therefore consider whether the duty of constant care comprises a right to privacy.

Dilemmas can arise when domestic legislation contradicts IHRL and IHL, thus allowing for directives inconsistent with international legal norms. However, the corporate duty to uphold IHRL and IHL extends beyond the requirement to adhere to national legislation.[36] The obligation to reject directives that contravene IHRL and IHL is founded on the principle that any sovereign government permitting human rights violations is not acting with legitimate authority, as enshrined in VCLT Article 27. This can also be inferred from the autonomous nature of UNGP Pillar II, representing a distinct corporate responsibility unrelated to the behaviour of the State.[37] Hence, companies shall respect IHL and IHRL, even when the respective state is breaching them.[38]

The above implies that ICT companies have a *soft law* obligation to respect the rules in AP I Article 57(1), ICCPR Article 17, and ECHR Article 8. Moreover, as illustrated by the Lafarge and Lundin cases, complicity in grave violations of IHL may lead to corporate criminal liability. Information sharing holds the potential for complicity.[39] The company may also lose its status of civilian nature, and thus the protection from attack, if directly participating in hostilities.

1.4.2 Legal Relevance to Norwegian Companies

The Norwegian Transparency Act of 18 June 2021[40] regulates the obligations of larger companies to conduct due diligence assessments to map, prevent, and limit negative impacts on human rights and working conditions in their own business, supply chains or business relationships. The companies' obligations relate to "basic human rights,"[41] thus including the human right to privacy.[42]

[35] Ibid, para. 45.
[36] Backer (2015) 493; Čertanec (2019) 107; Karp (2014) 52.
[37] Uvarova (2023) 5; UNGP (2011) 13.
[38] Karp (2014) 52.
[39] ICRC (2012) 1127-1128.
[40] Åpenhetsloven, LOV-2021-06-18-99.
[41] Ibid, § 3(b).
[42] Hellestveit and Wilhelmsen (2022) 15.

Although the definition of "basic human rights" does not mention IHL, the list is not exhaustive, cf. the wording "amongst others." The preparatory works state that due diligence assessments must be conducted in accordance with the UNGP and OECD guidelines, which highlight the duty to respect IHL during armed conflict.[43] Thus, these *soft law* instruments become *hard law* for the relevant companies, including the obligation to respect IHL when operating in areas affected by armed conflict.[44]

1.4.3 On the Further Analysis of ICT Companies' IHL Obligations

Before embarking on the further analysis of ICT companies' obligations under IHL, an important preliminary point must be made: My interpretation of AP I Article 57(1) and its interplay with the human right to privacy centers on the scope of States' international legal obligations concerning digital privacy rights during armed conflict. This serves as the fundamental framework for ICT companies dealing with potential government outreach. It is only through understanding the obligations imposed by international law upon the respective government that the company can assess whether the demands align with the State's legal obligations, which is a crucial element in the company's human rights due diligence.[45]

1.5 Delimitation

The thesis focuses on whether the duty of constant care comprises digital privacy protection. Specifically, whether companies have a duty to share or withhold customer data requested by a state party for intelligence purposes during armed conflict. With customer data I solely refer to data obtained from civilians, as opposed to military entities. The thesis will not delve into rules and procedures on storage and processing. It also excludes an in-depth exploration of digital privacy issues under IHRL, due to the word limit. The reason for the focus is that human rights protection of digital privacy has been explored to a far greater extent in both case law and literature, in contrast to privacy under IHL.[46] Hence, only a brief presentation of privacy rules under IHRL will be provided, followed by an analysis of how the human right to privacy interplay with the duty of constant care. Nor will the thesis delve into questions of extraterritorial application of IHRL and derogation.

[43] Prop. 150 L (2020-2021) 6; Harlem and Taylor (2022) 35.
[44] Harlem and Taylor (2022) 35.
[45] Carrillo (2022) 64; GNI Principles (2008).
[46] Lubin (2022a) 16.

The framework of IHL delineates two categories of armed conflict, namely international (IACs) and non-international armed conflicts (NIACs), in which different rules apply. AP I applies to IACs.[47] AP I Article 57 is, however, considered customary law, extending its applicability to NIACs.[48] Hence, my analysis has relevance to NIACs, although not taking into account any potential different outcomes.[49]

1.6 Structure

In Chapter 1, the groundwork has been laid by situating companies within the legal landscape and providing definitions essential for addressing the research question. Chapter 2 will outline the relevant legal sources and method required to interpret AP I, ECHR and ICCPR. Thus, this chapter will serve as a frame for the remaining chapters. Chapter 3 will assess whether the duty of "constant care" to spare the civilian population, enshrined in AP I Article 57(1), protects personal data for intelligence purposes. This necessitates an analysis of the terms "constant care," "military operations," "civilian objects," and "spare." To determine the comprehensive application of the duty of constant care, the demarcation, and interaction with the human right to privacy must be assessed. Chapter 4 will examine the interplay with the human right to privacy in the discourse of information sharing from an ICT company to a state party in an armed conflict. Chapter 5 concludes.

[47] IACs occur when two or more states use armed force against each other.
[48] Henckaerts and Doswald-Beck (2005) Rule 15; *Prosecutor v. Kupreškić et al.* [ICTY] para. 524; NIACs occur within the territory of a state and involves hostilities between governmental forces and non-State armed group(s), or between such groups.
[49] Different outcomes may follow, as state practice of the United States, Iran, Israel, and other non-signatories will not be considered under AP I Article 57(1), opposed to the customary rule, see Pomson (2023) 373.

2 SOURCES AND METHODOLOGY

2.1 Introduction

To assess what obligations the duty of constant care stipulated in AP I Article 57(1) imposes on companies requested to share customer data with States, it is necessary to provide some preliminary considerations about the interpretation of AP I and the human rights treaties ECHR and ICCPR. First, sources of international law relevant to the subsequent interpretation will be presented (2.2). Second, relevant rules of interpretation will be analyzed (2.3).

2.2 Relevant Sources

Article 38(1)(a) of the Statute of the International Court of Justice (ICJ) outlines the primary and subsidiary sources of international law. The Court is mandated to enforce "international conventions,"[50] which are agreements between sovereign states, including AP I, ECHR and ICCPR, as defined in VCLT Article 2(1)(a).

Additionally, the Court shall apply "international custom" as proof of general practice recognized as law, which hinges on the presence of objective state practice and subjective *opinio juris* expressed by those states, cf. ICJ Statute Article 38(1)(b). All states are bound by international custom.[51] Customary international law plays a pivotal role within IHL by addressing gaps in treaty provisions.[52]

Further, Article 38(1)(c) dictates that the Court must utilize the "general principles of law" acknowledged by civilized nations, with the purpose of avoiding lacuna in international law.[53] In the realm of IHL, four key principles – distinction, military necessity, proportionality, and humanity – hold great significance.

The principle of distinction requires parties to an armed conflict to distinguish between combatants and civilians, and between military objectives and civilian objects.[54] Civilians, including companies, are inherently non-combatants as long as they do not actively engage in

[50] Statute of the International Court of Justice [ICJ Statute], 24 October 1945, Article 38(1)(a).
[51] For exceptions see Hellestveit and Nystuen (2020) 40.
[52] ICRC (2022c) 3.
[53] Hellestveit and Nystuen (2020) 41.
[54] AP I Article 48.

hostilities. As a result, they should receive the utmost level of protection, as explained in Section 1.4.1.[55] Military necessity allows for actions required to achieve a legitimate military objective, i.e., weakening the other party, and are not otherwise prohibited by IHL.[56] Proportionality is a restraining element in military operations that would otherwise be deemed necessary, ensuring that the harm caused, is not excessive compared to the military advantage anticipated.[57] Humanity, a cornerstone of IHL, upholds the humane treatment of non-combatants and those no longer engaged in conflict, also extending protection to combatants and others involved in hostilities to prevent unnecessary suffering and superfluous injury.[58]

Lastly, the Court shall apply "judicial decisions and teachings" of highly qualified legal scholars as subsidiary means of interpretation.[59] There is no dedicated court for IHL, however the ICJ is central in interpreting general international law, including IHL. While ICJ judgments are only binding "between the parties and in respect of that particular case,"[60] its interpretation of a treaty is binding upon the parties to the respective treaty. ICJ advisory opinions are not legally binding, but carry significant weight, especially when the judges agree.[61] Both ad hoc criminal tribunals and the permanent International Criminal Court (ICC) adjudicate in war crime cases, thus rendering rulings potentially pertinent in interpreting AP I Article 57(1). Because considerations of IHL are distinct from other areas of international law, including criminal liability for war crimes often dealt with in these courts, one must exercise caution when attempting to derive general rules to questions within IHL.[62]

2.3 Interpretation of International Law

2.3.1 Rules of Interpretation

VCLT Article 31 and 32 are the foundation for interpreting treaties, widely acknowledged as international custom. Although concluded before the VCLT entered into force, the customary rules of VCLT apply to AP I, ECHR, and ICCPR.[63]

[55] Carrillo (2022) 92; ICRC (2009); German Military Manual (2013) 82.
[56] Carrillo (2022) 93.
[57] API Article 51(5)(b); Ingvarsson and Sannem (2021) 64-65; Watt (2022) 168.
[58] Carrillo (2022) 94.
[59] ICJ Statute Article 38(1)(d).
[60] ICJ Statute Article 59.
[61] Hellestveit and Nystuen (2020) 43.
[62] Ibid.
[63] *Kasikili/Sedudu Island (Botswana/Namibia)*, Judgment [ICJ], para. 20; *Navigational Rights (Costa Rica v. Nicaragua)*, Judgment [ICJ], para. 47; Pomson (2023) 357.

VCLT Article 31(1) mandates that a treaty be "interpreted in good faith in accordance with the *ordinary meaning* to be given to the terms in their *context* and in the light of its *object and purpose*" (emphasis added). These elements – ordinary meaning, context, and object and purpose – shall be considered as a whole.[64]

The context of a term is primarily the treaty's "text, including its preamble and annexes."[65] Together with the context, any "subsequent state practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation"[66] and "relevant rules of international law applicable in relations between the parties" shall be considered.[67] The latter mandates an analysis of the interplay between AP I Article 57(1) and relevant provisions under IHRL, as the human right to privacy holds nearly universal acceptance, with some even arguing for its customary nature.[68] The application of IHRL is addressed separately in Section 4 due to the specific methodological questions it raises, requiring a distinct presentation.

The "object and purpose" of a treaty can often be found in its preamble and by examining the provisions from a holistic perspective.[69] The title of AP I states that it relates "to the Protection of Victims of International Armed Conflicts."[70] The preamble stresses the need "to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application."[71] The rules enshrined in Part IV of AP I, including Article 57(1), are centered on civilians as victims. Read as a whole, AP I aims to balance humanitarian interests and military requirements of the parties involved in armed conflict.[72] Consequently, one can deduce that the object and purpose of AP I is to strengthen civilians' protection during armed conflicts, balanced with military necessity.

VCLT Article 32 regards supplementary sources, including but not limited to the "preparatory work of the treaty and the circumstances surrounding its formation." The ICRC has issued revised Commentaries and Interpretive Guidelines to furnish practical guidance for interpretation. In the context of cyber operations, the Tallinn Manual, a comprehensive

[64] *Maritime Delimitation (Somalia v. Kenya)*, Judgment [ICJ], para. 64.
[65] VCLT Article 31(2).
[66] See Section 2.3.2 and 2.3.3.
[67] VCLT Article 31(3)(b)-(c).
[68] West (2022a) 143; Rengel (2013) 108; Pillai and Kohli (2017); The "parties" is also interpreted to signify that the rules must apply to the disputing parties, see Todeschini (2018) 366; See Section 4.3.
[69] Pomson (2023) 366.
[70] See also ICRC Commentary AP I (1987) para. 3685.
[71] AP I Preamble.
[72] Pomson (2023) 359; *Maritime Delimitation (Somalia v. Kenya)*, Judgment [ICJ], para. 64.

guidebook on applying international law to cyber operations developed by international legal experts, is considered a resource for interpretation, although not legally binding.[73]

2.3.2 Evolutive Interpretation

The interpretative principles in VCLT Article 31 do not address whether a treaty shall be interpreted based on the historical or contemporary meaning of the terms. As AP I predates digitalization, it is plausible to assume that the drafters did not contemplate the notion of cyber warfare and intelligence.[74] Altered factual or legal circumstances can lead to changes in the "ordinary meaning" of a term.[75] This brings up a significant temporal dimension: Should the terms in AP I Article 57(1) be decided upon the "ordinary meaning" when the treaty was adopted, or can this meaning evolve? The answer to this question will impact the interpretation of AP I Article 57(1) in Section 3.

The VCLT is often construed as implicitly supporting evolutive interpretation. This understanding finds its basis in VCLT Article 31(1), which pertains to the interpretation of treaties in accordance with their "object and purpose," and Article 31(3)(c), on the interpretation of treaties considering "relevant rules of international law," which can change over time.[76] Similarly, Article 31(3)(a)-(b) mentions the importance of *subsequent* agreements and practices of the parties as means of interpretation.[77]

As established by the ICJ in *Costa Rica v. Nicaragua*, when parties select a broad or generic term in a treaty with a long-lasting effect, it should be assumed that they intended for the meaning to evolve.[78] Given that AP I is a treaty without a fixed end date, and terms such as "objects" and "military operations" are generic,[79] an evolutive interpretation is possible. Recent regional consultations on IHL and cyber operations during armed conflicts affirm this through a broad agreement that "the interpretation of generic legal terms – like the word 'object' – should be done considering evolving circumstances"[80] and that "international law can only perform its

[73] Mačák (2015) 60.
[74] Ibid.
[75] Arato (2010) 467.
[76] Ibid, 446.
[77] Pomson (2023) 369.
[78] *Navigational Rights (Costa Rica v. Nicaragua)*, Judgment [ICJ], para. 66.
[79] McKenzie (2021) 1176.
[80] ICRC (2022b) 8.

functions in a rapidly developing world if it embraces evolutionary interpretation."[81]

Second, several terms within AP I have previously been interpreted considering prevailing circumstances at the time of application.[82] In *Costa Rica v. Nicaragua* factual developments necessitated an evolutive interpretation of "comercio" to uphold the treaty's effectiveness in accordance with its "object and purpose."[83] Further, in the *Nuclear Weapons* Advisory Opinion, the ICJ stressed the significance of the Martens Clause, as a means of addressing what the Court described as "the rapid evolution of military technology."[84] It has been noted that this passage advocated for a dynamic approach to IHL as a whole.[85]

Third, the purpose of AP I, to serve as a treaty safeguarding victims of armed conflict balanced with military necessity, as established in Section 2.3.1, encourages the application of evolutive interpretation. This aligns with the principles established by the most influential human rights tribunals, emphasizing that treaties serving humanitarian concerns are dynamic instruments that should be interpreted considering contemporary conditions.[86] This characteristic is partly shared by human rights treaties and AP I.[87]

On the other hand, the scope and purpose of human rights conventions and IHL are different. While the human rights treaties cover a broad range of abstract civil and political rights, the Geneva Conventions and Additional Protocols contain more fixed and specific provisions. The latter not only protects civilians but also preserve belligerents' capacity to use force for military needs, as noted in Section 2.3.1. While the ECHR and CCPR rulings adapt quickly to evolving social norms and new human rights concerns, developments within IHL are impacted to a greater extent by state practice, leading to less flexible and slower developments.[88]

In summary, an evolutive interpretation must stem from the intention of the parties to create a treaty with evolving obligations, which may implicitly be derived from generic terms in a long-lasting treaty. Since the generic terms of AP I Article 57(1) open up a possibility for evolutive interpretations, such an interpretation will be conducted in Chapter 3. Nevertheless, it is

[81] ICRC (2022a) 7.
[82] *Continued Presence of South Africa in Namibia*, Advisory Opinion [ICJ], para. 53: "an instrument has to be interpreted and applied within the framework of the entire legal system prevailing *at the time of the interpretation*."
[83] *Navigational Rights (Costa Rica v. Nicaragua)*, Judgment [ICJ], para. 46; Arato (2010) 467.
[84] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [ICJ], para. 78.
[85] Mačák (2015) 71.
[86] *Tyrer v. United Kingdom* [J], no. 5856/72, para. 31; *Roger Judge v. Canada* [CCPR], para. 10.3.
[87] Mačák (2015) 70.
[88] Lubin (2022b) 491.

essential to factor in "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation."[89]

2.3.3 State Practice

According to the orthodox interpretation of "subsequent practice" under Article 31(3)(b), inconsistency prevents the majority's practice from being considered due to a lack of required "agreement" among the parties. However, international courts have taken a broader perspective on subsequent practice within Article 31(3)(b). The courts have regarded the practice of most state parties, even when faced with explicit disagreement, as a legitimate method of interpretation under Article 31(3)(b), rather than categorizing it as a supplementary means under Article 32.[90] Still, the weight given to state practice varies depending on the level of consensus among the parties and how it interacts with the other methods of interpretation enshrined in VCLT Article 31.[91] This also implies that in absence of state practice, the treaty text's "ordinary meaning" interpreted in its "context" and in light of the treaty's "object and purpose" is decisive.

[89] VCLT Article 31(3)(b).
[90] *Continued Presence of South Africa in Namibia*, Advisory Opinion [ICJ]; *Palestinian Wall*, Advisory Opinion [ICJ]; *Prosecutor v. Tadić*, Decision [ICTY]; Hill-Cawthorne (2023) 892-893; International Law Commission (2018) conclusion 10.2; Scholars and judicial decisions disagree on whether inconsistent practice falls under VCLT Article 31(3)(b) or Article 32. This thesis will not explore this debate, nor the legal effect of state "silence."
[91] Hill-Cawthorne (2023) 895.

3 THE DUTY OF CONSTANT CARE

3.1 Introduction

This Chapter will analyze whether the duty of constant care codified in AP I Article 57(1) comprises digital privacy, with an overall emphasis on companies requested to share customer data with State parties for intelligence purposes. Article 57(1) states:

> *"In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."*

The term "shall" signify that the obligations enshrined are legally binding.[92]

In the following, the key terms "constant care," "military operations," "objects," and "spare" will be interpreted in accordance with the rules on interpretation outlined in Section 2.3. First, the "ordinary meaning" of the terms will be clarified and interpreted in their "context" and in light of the treaty's "object and purpose."[93] Second, any subsequent state practice shall be taken into account.[94]

3.2 Constant Care

As implied by the ordinary meaning of "constant," the duty is always applicable. This aligns with the object and purpose AP I; to protect civilians for the duration of armed conflict, balanced with military necessity. This interpretation is confirmed by the International Law Association Study Group, consisting of multiple prominent scholars, characterizing it as a "continuous obligation."[95] Hence, the duty is applicable throughout armed conflict, irrespective of the time or stage of hostilities.

The ordinary meaning of "care" is to provide for the needs of someone. The wording is vague, making it challenging to discern specific requirements.[96] However, it is widely accepted that the duty imposes a broad obligation "to bear in mind the effect of the civilian population of

[92] Gill et. al. (2017) 42.
[93] VCLT Article 31(1).
[94] VCLT Article 31(3)(b).
[95] Gill et. al. (2017) 43; ICJ Statute Article 38(1)(d).
[96] Schmitt (2019) 354.

what he is planning to do and take steps to reduce that effect as much as possible."[97] Hence, the duty necessitates a balance between humanitarian concerns that advocate for precautionary measures and military considerations that may oppose taking those precautions.[98]

Given the vagueness of the term "care" and the absence of jurisprudence, guidance may be found in the obligation of "due regard" in the Exclusive Economic Zone and High Seas as stipulated by UNCLOS.[99] After all, "care" and "regard" are synonymous, and a similar balance of interests is anticipated under both.[100] In *Mauritius v. the United Kingdom*, the Permanent Court of Arbitration provided the following clarification: "The extent of the regard required […] will depend on the nature of the rights […], their importance, the extent of the anticipated impairment, the nature and importance of the activities contemplated by [the State], and the availability of alternative approaches."[101] Hence, the requirement is to exercise fundamental due diligence, taking practically feasible actions, while considering all the prevailing circumstances, similar to the due diligence assessments required by the UNGPs.[102]

3.3 Application: "military operations"

The obligation of constant care is applicable "in the conduct of military operations." The ordinary meaning of "military operations" includes military activities with a connection to or objective of advancing combat.

Given the title of AP I Article 57 referring to "precautions in attack" and the scenarios delineated in Article 57(2)-(5), the provision may in its context be interpreted as relevant solely in situations involving attacks, which encompass "acts of violence against the adversary, whether in offense or in defense."[103] However, the ordinary meaning of "military operations" is broader than "attacks," indicating that the clause serves a wider set of activities, including but not limited to rules on precautions in attack. If Article 57(2)-(5) entirely covered the obligations stipulated in Article 57(1), then this clause would serve no distinct purpose. A broad interpretation is in accordance with the principle of "Verba accipienda ut sortiantur effectum,"

[97] United Kingdom Military Manual (2010) para. 5.32.1; Lubin (2022a) 15.
[98] Lubin (2022a) 16.
[99] United Nations Convention on the Law of the Sea [UNCLOS]; Lubin (2022a) 16.
[100] VCLT Article 31(3)(c).
[101] *Mauritius v. United Kingdom* [PCA], para. 519; Lubin (2022a) 16.
[102] Lubin (2022a) 17; UNGP (2011).
[103] AP I Article 49(1); Watt (2022) 169.

meaning words are to be construed so that they obtain effect.[104] Hence, Article 57(2)-(5) should be construed as derivative specifications of a broader obligation in Article 57(1).[105]

Further, the term "military operations" must be interpreted in light of the treaty's object and purpose. As stated in Section 2.3.1, the object and purpose of AP I is to protect civilians during armed conflicts, balanced with military necessity. A broad interpretation, including military intelligence in the digital space, aligns with this overarching purpose, meaning civilians would be protected against unwarranted intrusion regardless of the military activity conducted.

The original purpose behind Article 57(1) specifically was to affirm a comprehensive and adaptable duty serving as a catch-all provision.[106] A narrow interpretation of the rule, excluding informational operations and including artificial distinctions based on factors such as the entity conducting the collection or processing (civilian vs. military) or the nature of the collection and processing (commercial vs. governmental) would cause civilian protection gaps and thus undermine the intended purpose of the duty of constant care.[107]

In summary, the "ordinary meaning" to be given to "military operations" in AP I Article 57(1) "in [its] context" and in light of the "object and purpose," is military activities with a connection to combat, including digital and intelligence operations.

This interpretation is partly confirmed by ICRC Commentaries, stating that "military operations" encompass "any movements, manoeuvres, and other activities whatsoever carried out by the armed forces with a view to combat,"[108] and "means and methods of injuring the enemy."[109] It further states that such operations do not include "ideological, political or religious campaigns."[110] One could argue that intelligence falls under this category. On the other hand, intelligence has a closer proximity to military attacks, as it often is a prerequisite for the conduct. Therefore, the ICRC Commentary does not preclude a categorization of intelligence with the intent of advancing military objectives as "military operations."

[104] Lubin (2022a) 10.
[105] Gill et. al. (2017) 42.
[106] ICRC Commentary AP I (1987) para. 2184, 2189 and 2191.
[107] Lubin (2022a) 12.
[108] ICRC Commentary AP I (1987) para. 2191.
[109] Melzer (2009) 43.
[110] ICRC Commentary AP I (1987) para. 1875; Rodenhäuser (2023) 571.

Further, one must consider whether any subsequent practice between the parties, supports or contradicts the above interpretation.[111] The United Kingdom Manual on the Law of Armed Conflict regards "military operations" as a broader term than "attack," including activities such as the mobilization and positioning of armed forces.[112] According to the German Manual, military operations refers to "all acts committed by military means by one Party to a conflict against another Party, as well as to any threat or actual execution of military operations."[113] These manuals mainly treat physical operations, while not explicitly excluding intelligence operations.

The Norwegian Manual states that "'military operations' is a broader term than attack and includes all movements and activities by armed forces in connection with hostilities, i.e. *in connection with the planning* and use of means and methods of warfare. Attack is therefore an aspect of military operations, although the term "operations" will also *encompass activities not intended to cause injury or destruction*" (emphasis added).[114] The medium where operations are conducted is not of relevance according to the New Zealand Manual, stating that "LOAC apply to all military operations regardless of the medium employed."[115] These manuals take a broad approach, conceivably including digital intelligence.

As mentioned in Section 2.3.3 the weight attributed to non-consistent practice is influenced by its alignment with other methods of interpretation, meaning that state practice deviating from the "object and purpose" of a treaty, may need unanimous or at least broad endorsement to impact the interpretation.[116] Therefore, in the absence of consistent state practice on whether "military operations" include digital operations and intelligence, an evolutive interpretation in light of AP I's "object and purpose," implies that the duty to exercise constant care extend to the entire spectrum of military activities with a connection to combat. This includes intelligence gathering, regardless of its form and the entities conducting it, if serving the general objective of advancing combat efforts.[117] Consequently, the duty is applicable when relevant information reaches a military entity, requiring the company to conduct due diligence in advance.

[111] VCLT Article 31(3)(a)-(b).
[112] United Kingdom Military Manual (2010) 5.32.
[113] German Military Manual (2013) 32.
[114] Norwegian Military Manual (2013) 14.
[115] New Zealand Military Manual (2017) 8-39.
[116] Hill-Cawthorne (2023) 898.
[117] Davenport (2022) 193; Lubin (2022a) 11.

3.4 Is Data an “object”?

This Section will interpret the terms "civilian population, civilians and civilian objects." The main emphasis is on the latter, as this is the most contentious and relevant term for this thesis.[118] Whether customer data is included in the term "civilian object" holds substantial significance to the final conclusions. If data is classified as an object, the principle of distinction applies, meaning targeting civilian data is prohibited.[119] However, if data is not an object, the principle of distinction does not apply, meaning civilian data will not be protected from targeting nor surveillance. First, I will shortly present the terms "civilians" and "civilian population," then I will analyze the salient point of whether data is an "object."

AP I Article 50(1) defines civilians as persons not belonging to one of the categories referred to in Article 4(A)(1), (2), (3) and (6) of Geneva Convention (III), as well as in AP I Article 43, adding that "[i]n case of doubt whether a person is a civilian, that person shall be considered to be a civilian." The key feature of civilians derived from this is that they are not affiliated with the armed forces, nor engage directly in hostilities.[120] The "civilian population" is defined in AP I Article 50(2) as encompassing all persons who are civilians.

According to AP I Article 52 "[c]ivilian objects are all objects which are not military objectives as defined in paragraph 2." That means civilian objects are all objects except "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."[121] As specified in Section 1.5, customer data solely refers to "civilian" data in this thesis. Hence, the question in the following is whether the meaning of the term "object" today extends to cover data. To answer this, one must look at the "ordinary meaning" of the term, as well as examine the "context" in which it appears and the "object and purpose" of AP I.[122]

The ordinary meaning of "object" suggests something visible and tangible in the physical world.[123] The Oxford English Dictionary defines it as "a thing that can be seen and touched" or

[118] Data characterization is one of many controversial topics currently being explored by cyber law experts, see Graboritz, Morford and Truax (2020) 122.
[119] Grote (2023) 194.
[120] Dinstein (2016) 142.
[121] API Article 52(2); O'Connell (2022) 26.
[122] VCLT Article 31; See Section 2.
[123] Geiß and Lahmann (2021) 565; Graboritz, Morford and Truax (2020) 123.

"an aim or purpose."[124] In this respect, the other authentic language versions may be of assistance. Along with English, the Arabic, Chinese, and Russian versions use the term "object." Whereas the French and Spanish use the word "bien," translating into "a good" or "a property" in English.[125] What concerns the word "bien," it is divided into both tangible and non-tangible sub-categories in French legal literature and several French-speaking jurisdictions.[126] Although relocating the term from domestic law into international law is not the aim here, it sheds some light on the ordinary meaning, which does not categorically exclude intangible objects.[127]

The ordinary meaning must be interpreted in its context. The term is positioned in Section I of Part IV of AP I. While this section is titled "General protection against effects of hostilities," it also outlines the fundamental regulations on targeting in international armed conflicts. Within this section, the term "object" typically refers to something that can be the target of attacks. These include "a place of worship, a house or other dwelling or a school;"[128] "historic monuments, works of art or places of worship;"[129] "food-stuffs, agricultural areas for the production of food-stuffs, crops, livestock, drinking water installations and supplies and irrigation works;"[130] and "dams, dykes and nuclear electrical generating stations."[131] Consequently, an "object" is something that can be destroyed, captured, or neutralized.[132]

Contrary to most of the Tallinn Manual experts I argue that data meets this criterion and therefore must be considered an "object" under AP I Article 57(1). The Tallinn Manual states that attacks solely destroying data, fall outside the scope of IHL, unless they also disrupt the functionality of the control system to a degree that necessitates the replacement of physical components.[133] This is not a satisfactory solution. Take, for example, an attack on digital weapon logs, timetables for military logistics, or air traffic control information. The destruction of this data would not involve physical force, but it would satisfy the dual criteria outlined in Article 52(2). Such data significantly contributes to the military operations of one party; in fact, their military actions are intricately linked to and dependent on this specific dataset.

[124] 'Object', Oxford English Dictionary, https://www.oed.com/search/dictionary/?scope=Entries&q=object.
[125] Mačák (2015) 72.
[126] Ibid.
[127] Ibid.
[128] API Article 52(3).
[129] API Article 53.
[130] API Article 54(2).
[131] API Article 56(1).
[132] Mačák (2015) 73.
[133] Tallinn Manual (2017) rule 92 commentary para. 10.

Consequently, its destruction would provide a clear military advantage to the opposing party.[134] As shown by this example, physical interference is not always necessary to achieve the attacker's aims. Hence, considering contemporary circumstances, I argue that an interpretation of data as an "object" aligns better in the context of the provision.

While most of the Tallinn Manual experts did not delve into this matter extensively, the chairman of the group of experts has raised two reasons for the Manual's perspective. First, Professor Schmitt contends that the destruction of data without direct physical consequences is more analogous to psychological operations, which are beyond the scope of the rules governing targeting in AP I.[135] Similarly, the ICRC Commentary described objects as tangible to distinguish them from abstract concepts such as civilian morale and the aims of the parties.[136] Second, Smith asserts that if all data were considered objects, it would require states to relinquish their capacity to conduct certain operations with potential consequences for civilians, which they would be unwilling to accept.[137]

Regarding the first point, the question is whether computer data is more comparable to abstract concepts like civilian morale, or more akin to tangible objects like a bridge. Morale can be influenced by attacks, but it is a subjective concept whose existence or extent cannot be objectively measured. In contrast, a bridge can either remain undamaged, sustain damage, or cease to exist altogether. The presence and condition of a bridge do not rely on subjective assessments or beliefs.[138] Computer data, commonly understood in contemporary terms, aligns more with a bridge. According to the Oxford English Dictionary, in the context of computing, data is defined as "the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media."[139] As proved by this definition, data is conceptually associated more with tangible objects since it can be singled out and destroyed.[140]

The second objection pertains to the perceived reluctance of states to adopt a definition of objects including data, citing concerns about it being too broad. Schmitt writes, "[i]t would appear overbroad to characterize all data as objects. Surely a cyber operation that deletes an

[134] Mačák (2015) 77.
[135] Schmitt (2011) 92-96; Mačák (2015) 73.
[136] ICRC Commentary AP I (1987) para. 2008.
[137] Schmitt (2014) 298; Mačák (2015) 73.
[138] McKenzie (2021) 1177.
[139] 'Data', Oxford English Dictionary, https://www.oed.com/dictionary/data_n?tab=factsheet.
[140] Geiß and Lahmann (2021) 566; Mačák (2015) 73.

innocuous e-mail or temporarily disrupts a television broadcast does not amount to an unlawful attack on a civilian object."[141] While it may be accurate to conclude that this objection holds merit in certain situations, the foundational premise of this argument is flawed.

To illustrate, I will use the example of an "innocuous e-mail" written on paper rather than stored as computer data. As the qualifying adjective "innocuous" implies the tampering or destruction of the letter would likely breach IHL, because the letter does not qualify as a military objective.[142] However, in most conceivable scenarios, the destruction of a civilian letter would result from a larger targeting operation. For instance, if a post office serving as a military outpost were attacked, leading to the destruction of letters stored within the building, this destruction may be lawful under the principle of proportionality, permitting collateral damage to civilian objects if the damage is not excessive compared to the military advantage, as explained in Section 2.2. The same principles would apply to the electronic equivalent of a physical civilian letter. Therefore, the ability of states to conduct cyber operations leading to the destruction of data, would not be excessively hindered.[143]

Another point of interest relates to medical data. The emerging perspective within customary IHL suggests that the obligation to respect and protect "medical units" in AP I Article 12 extends to medical data.[144] A similar imperative for preserving medical data may be applicable to the protection of civilian data in general, especially sensitive data. This illustrates the legal principle of construction, known as "nocitu a sociis," meaning "it is known by its associates."[145] Conversely, one may highlight the explicit reference to "medical" in treaties and contend that non-medical data falls outside the scope of protection. This would correspond to the legal principle "ejusdem generis," which implies that mentioning a particular thing or characteristic excludes things that lack that thing or characteristic.[146] Hence, the extension of the obligation to respect and protect "medical units" to medical data does not necessarily equate to considering data as an "object."

Lastly, one must explore possible interpretations of the term "object" in light of AP I's object and purpose.[147] An interpretation of "object" encompassing data will contribute to advancing

[141] Schmitt (2011) 96.
[142] Mačák (2015) 75; AP I Article 52(2).
[143] Mačák (2015) 75.
[144] Geiß and Lahmann (2021) 564; Millett (2023) 2; O'Connell (2022) 24.
[145] O'Connell (2022) 25.
[146] Ibid.
[147] VCLT Article 31(1).

humanitarian safeguards.[148] As stated by the ICRC, "tampering with data [such as social security data, tax records, bank accounts, companies' client files or election lists or records] could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects."[149] The traditional barter goods of gold, silver, silk, and spices have been replaced by electronic banknotes and cryptocurrencies, which are accepted as payment but, according to the traditional ordinary meaning of "object," are neither real nor substantial, although having a significant impact on the global economy.[150] Asserting that the transition from paper-based records to digital data has compromised the safeguards provided by IHL proves difficult to reconcile with the object and purpose of AP I.[151]

In summary, the evolutive "ordinary meaning" to be given to "object" in AP I Article 57(1) "in [its] context" and "in light of [the treaty's] object and purpose" includes data.[152] However, since "any subsequent agreement between the parties regarding the interpretation" shall be taken into account, as mentioned in Section 2.3.3, one must assess whether state practice supports or contradicts this interpretation.

States' positions on the matter are scarce and inconsistent.[153] France contends that intangible objects like civilian data is protected, highlighting that societies have become too dependent on data to exempt it from the protections under IHL.[154] Norway,[155] Germany,[156] and Romania,[157] argue that safeguarding civilian objects extends to civilian data in the context of targeting.[158] Estonia, Finland, the Netherlands, and the United Kingdom[159] have asserted the applicability of international law to cyber operations, yet they have not specified the extent to which IHL protects data.[160]

[148] Mačák (2015) 77-78; McCormack (2018) 240.
[149] ICRC (2019) 8.
[150] Graboritz, Morford and Truax (2020) 128.
[151] Gisel and Rodenhäuser (2020).
[152] VCLT Article 31(1).
[153] McKenzie (2021) 1174.
[154] Geiß and Lahmann (2021) 567; Ministère des Armèes de France (2019) 15.
[155] Norwegian Military Manual (2013) 9.58; Cooper (2021) 23.
[156] German Position Paper (2021) 8.
[157] UNODA (2021) 78.
[158] Grote (2023) 195; McKenzie (2021) 1174.
[159] United Kingdom Attorney General (2021).
[160] McKenzie (2021) 1175-1176.

The Danish Military Manual suggests that while data is not typically an object, harm to "irreplaceable data" is recognized as collateral damage.[161] Peru and Chile believe that certain data may be protected if it is not a military target, while Guyana focuses on the far-reaching effects of cyber operations.[162] New Zealand does not explicitly address data but acknowledges that international law is relevant to all state activities in cyberspace, encompassing "its intangible, virtual component."[163] The ICRC recognizes the unresolved nature of whether civilian data qualifies as civilian objects, however, clearly leaning towards a comprehensive approach encompassing civilian data.[164]

Although states' positions on the matter are imprecise and inconsistent, meaning it is unclear from state practice whether "object" extends to cover data, most states seem inclined to accept the relevance of data and the possible implications attacks on data may have.[165] At least, there is no "agreement" among states to the contrary that would render VCLT Article 31(3)(b) decisive. Hence, the "ordinary meaning" in its "context," together with the "object and purpose" of AP I, point in favor of regarding data as an "object," with the support of some state practice. With data constituting an "object," the question remains whether the sharing of civilian data enjoys protection under the duty of constant care.

3.5 Obligation to “spare”

3.5.1 Introductory Remarks

Even if one accepts that "military operations" apply to war-related intelligence gathering and that data constitutes an "object," a fundamental question persists regarding the meaning of "spare" civilians and civilian objects, and whether it extend beyond physical kinetic consequences. The interpretation of "spare" is decisive in determining whether there exists an obligation to share or withhold customer data.

The ordinary meaning of "spare" is to refrain from inflicting injury upon a person, leave someone unhurt, unharmed, or injured, or allow them to go free or live.[166] As the title of Article 57 is "[p]recautions in attack" one may derive that "spare" in its context refers to refraining

[161] Danish Military Manual (2016) 310.
[162] McKenzie (2021) 1174.
[163] New Zealand Statement (2020); McKenzie (2021) 1175.
[164] ICRC (2019) 8.
[165] McKenzie (2021) 1174-1175.
[166] 'Spare', Oxford English Dictionary, https://www.oed.com/dictionary/spare_v1?tab=factsheet#21583829.

from inflicting physical harm on civilians and civilian objects. This would imply that actions impacting the availability of data is covered, while actions preserving the data itself and solely compromising the confidentiality, such as sharing, is not.[167] However, presuming that the duty of constant care is a broad obligation applicable in "military operations" in the wide sense, the duty to "spare" might have a broader application.

Examining the term "spare" in the context of other pertinent regulations within IHL, including medical data (3.5.2) respect of the person (3.5.3), and seizure of property (3.5.4) is valuable, as the provision constitutes a general duty reaffirming several other rules within the IHL framework.[168] The rules will be looked at to gain some context and will not be thoroughly interpreted *per se*.

3.5.2 Medical Data

The customary protection of medical data, mentioned in Section 3.4, is recognized as not only pertaining to attacks, but also preserving the confidentiality, integrity, and availability of the data. The protection limits the entire range of digital activities that may leverage medical data, including situations when neither patients nor infrastructure are impacted.[169] An exemption pertains to "non-damaging cyber reconnaissance to determine whether the medical facility [is] misused for military harmful acts,"[170] which hardly applies to medical data on customers obtained by companies. Hence, ICT companies cannot share customers' medical data.

A similar imperative for protecting privacy concerning medical data may be applicable to civilian data in general, especially sensitive data. However, the special protection given to medical units in written IHL sources implies that the same protection not necessarily extend to other civilian data.[171] At least, such an extension must rely on further sources.

3.5.3 Respect of the Person

The right to respect of the person is expressed in several provisions. AP I Article 75(2)(b) safeguards against outrages upon personal dignity, GC IV Article 25 protects communication with family members, and GC IV Article 27 guarantees protected persons "respect for their

[167] Millett (2023) 2.
[168] ICRC Commentary AP I (1987) para. 2184, 2189 and 2191; VCLT Article 31(1)-(2).
[169] Schmitt (2015) 101; Millett (2023) 2.
[170] Tallinn Manual (2017) rule 132 commentary para. 2.
[171] See account on medical data in Section 3.4.

persons, their honour, their family rights, religious convictions and practices, and their manners and customs." They shall be protected "against insults and public curiosity," and "be treated with the same consideration […] without any adverse distinction based, in particular, on race, religion or political opinion."[172]

These provisions share two common characteristics: they directly safeguard human dignity, including physical, moral, and intellectual integrity,[173] and they are applicable once an individual is "in the power" or "in the hands" of a belligerent. This implies that IHL offers protection for non-physical interests but confines such protection to circumstances where a belligerent has physical authority over a person or the territory in which that person is located.[174]

As the provisions were produced in the pre-internet age, they lack a reference to digital privacy and data protection. Although the broad provisions make it difficult to derive specific rules, discrimination is explicitly illegal. This means that intelligence cannot be gathered on a particular group, such as human rights defenders or based on ethnicity, without a justified reason. Further, protection against public curiosity means that "[i]ndividual persons' names or photographs, or aspects of their private lives must not be given publicity."[175] In other words, civilian data obtained from ICT companies cannot be publicly shared or used to humiliate the person or the group. Conversely, protection of civilian data obtained solely for intelligence purposes, not used to humiliate, or commit other violations stipulated in the Articles, cannot be explicitly derived.

The "respect for honour," as delineated in GC IV Article 27, corresponds to GC III Article 14. The updated Commentary on GC III acknowledges that contemporary surveillance technologies engender concerns about "the right of prisoners to respect for their persons and honour." It posits that the deployment of "limited, well-regulated and well-managed video-surveillance" in prisoner-of-war camps "should not in principle be considered as prohibited" by Article 14, given its potential to mitigate or prevent escape or self-harm endeavors, misconduct by guards, and conflicts among detainees. In contrast, constant video surveillance of all prisoners appears disproportionate. Similarly, filming familial visitations and restroom usage is impermissible if alternative means of averting security breaches are equally efficacious.[176]

[172] GC IV Article 27.
[173] ICRC Commentary GC IV (1958) 1.A.
[174] Grote (2023) 217.
[175] West (2022a) 147.
[176] ICRC Updated Commentary GC III (2020) para. 1677; Mahnad (2022); Shehabi (2022) 97-98.

The updated Commentary, limited in examining emerging surveillance technologies solely to video surveillance and electronic tracking bracelets, has received criticism for not affording sufficient weight to state practice in applying the Convention.[177] Nevertheless, it might reflect a trend towards acknowledging digital privacy within IHL, aligning with the dual purpose of AP I; to protect civilians balanced with military necessity.

3.5.4 Seizure of Property

According to Hague Convention IV Article 23 it is forbidden to "seize the enemy's property, unless such […] seizure be imperatively demanded by the necessities of war." With data constituting an "object," and thus also encompassed by the broader term "property," IHL prohibits the seizure of data unless imperatively demanded by the necessitates of war.

Although there is no formal definition of "seize" in treaty or case law, it is generally understood to encompass custody or utilization of property, such as by appropriation or control. This is relatively straightforward applied to physical items. However, regarding data, one can establish control in various ways beyond and differently from physical possessions. This might include using, copying, tampering with, or obstructing access.[178]

Actions hindering the original owner from using or accessing data fall under the definition unequivocally. Conversely, the use and copying of data, including information sharing, presents a more complex question because the original owner may still retain access to the data. A strict and technical interpretation excludes such actions from consideration. However, a more purpose-driven interpretation based on the object and purpose of IHL minimizing the impact and dangers to civilian populations, balanced with military necessity, could encompass such acts.[179] The latter part of the object and purpose, would imply that any data relevant to advancing combat efforts is permitted to be shared.

State practice on the matter appears to be absent. However, since most of the States viewing data as objects, only do so in the context of targeting, as established in Section 3.4, sharing, and consequently obtaining civilian data, without impacting the data *per se*, does not amount to "seize," as this would significantly deviate from the majority of states' current legal positions.[180]

[177] Shehabi (2022) 98.
[178] Blank and Jensen (2022) 63.
[179] Ibid.
[180] VCLT Article 31(3)(a)-(b).

3.5.5 Summarizing “spare”

In summary, the term "spare" may be interpreted to include a right to privacy covering all civilian data irrelevant to combat. This would align with the dual purpose of AP I, as the information would not advance combat while enhancing the protection of civilians. However, since sharing constitutes an expanding interpretation of the term "spare" combined with deviating state practice, the protection offered in the context of data sharing for combat intelligence purposes remains absent. An exception applies to intelligence gathering reasonably presumed to have an unlawful purpose, such as discriminatory practices or public curiosity.

3.6 Summarizing the Interpretation of AP I Article 57(1)

The duty of constant care, stipulated in AP I Article 57(1), establishes a continuous duty of due diligence during armed conflict. Although disputed, it may be regarded as a broad obligation applicable to military activities with a connection to combat, including information gathering. Consequently, the duty is applicable when relevant information reaches a military entity, requiring the company to conduct due diligence before sharing.

Whether civilian data, is regarded as a "civilian object" is currently contested, and resultingly, it is contested whether ICT companies' customer data is protected under the provision. Moreover, I contend that the term "civilian objects" include civilian data by following the rules of interpretation in VCLT Article 31.

However, due to deviating state practice, the term "spare" does not extend to the sharing of civilian data, unless the data itself is affected or the gathering is presumed to have an unlawful underlying purpose, such as discriminatory practices or public curiosity. Hence, the duty of constant care codified in AP I Article 57(1) only impose minor restrictions on ICT companies sharing customer data with a state party. Further, medical data benefits from a customary legal protection against sharing.[181] *De lege ferenda*, updated ICRC Commentaries signal a possible shift towards adopting a necessity assessment with regard to digital surveillance.[182]

In summary, digital privacy protections under the duty of constant care are, at this point, inadequate, leading to a lacuna within IHL.

[181] Millett (2023) 2.
[182] ICRC Updated Commentary GC III (2020) para. 1677.

4 COMPLEMENTING THE LACUNA WITH THE HUMAN RIGHT TO PRIVACY

4.1 Introduction

This Chapter will analyze whether the lacuna within IHL concerning data privacy may be solved by interpreting the duty of constant care in light of the human right to privacy according to VCLT Article 31(3)(c), founded on the notion that international law should constitute a coherent body of law.[183] The provision states that "any relevant rules of international law applicable in relations between the parties" shall be taken into account, as mentioned in Section 2.3.

The application of IHRL relies traditionally on three conditions: (1) the human right to privacy is not validly derogated,[184] (2) the conduct is that of a State and its organs, and (3) the conduct in question pertains to an individual within the jurisdiction of the State.[185] Conversely, derogation is not possible for IHL rules; IHL applies to states, armed groups and others directly participating in the conflict; and IHL applies irrespective of effective control.[186] The updated ICRC Commentaries refers to "human rights *where applicable,*"[187] and adds in the updated Commentary on GC III that it is "important to note that treaties other than the Conventions themselves are referred to in the Commentaries on the understanding that they *apply only if all the conditions relating to their geographic, temporal and personal scope of application are fulfilled"* (emphasis added).[188] Hence, the human right to privacy is only relevant when the conditions for application are present.[189]

[183] Grote (2023) 211.
[184] Multiple questions arise in regards derogations, awaiting academic exploration, including whether derogation by State A may cover the area occupied by State B, and whether State B exercising effective control over occupied area may derogate extraterritorially. Concerning the latter, if the war does not extend to State B's territory the condition "threatening the life of the nation" in ECHR Article 15 is unlikely fulfilled.
[185] The ECtHR Grand Chamber held in *Georgia v. Russia (II)*, para. 137 that "the context of chaos" or level of violence in an armed conflict is a determinate factor on whether a foreign military has *effective control* and, consequently, the extent of the State's human rights obligations. Further, scholars are discussing extraterritorial application of IHRL in the virtual space, see Milanovic (2022). In *Big Brother Watch v. United Kingdom*, the ECtHR Grand Chamber presumed cross-border surveillance to fall within its jurisdiction, para. 272.
[186] Exception: the right to respect of the person applies when an individual is "in the power" of a belligerent.
[187] ICRC Updated Commentary GC I (2016), para. 35; ICRC Updated Commentary GC II (2017), para 35; ICRC Updated Commentary GC III (2020), para. 95.
[188] ICRC Commentary GC III, para. 94.
[189] Steenberghe (2022) 1353.

Yet, a clarification is necessary concerning the application of IHRL for companies. As outlined in Section 1.4.1 companies shall respect IHRL even when the respective state is breaching them. Moreover, legal derogations or lack of effective control may lead to domestic directives consistent with the State's international legal obligations at the time, although the human right to privacy is not addressed.[190] Simultaneously, the company may be bound by the UNGPs or other human rights reporting requirements in its home state (if it is a transnational company). When faced with conflicting requirements, the company should "seek ways to honour the principles of internationally recognized human rights."[191] This implies that ICT companies should consider the human right to privacy, regardless of whether the right applies to the state at the time of question.

Following a presentation of the human right to privacy in Section 4.2, Section 4.3 will delve into the interplay between the human right to privacy and the duty of constant care. Finally, Section 4.4 will operationalize the legal framework.

4.2 Human Right to Privacy

The right to respect for one's private life, home and correspondence is outlined in several international legal frameworks.[192] Two of the most prominent are ICCPR Article 17 and ECHR Article 8.

Article 17 of the International Covenant on Civil and Political Rights states:

> "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."

The ordinary meaning of "privacy" indicates a right to keep personal matters a secret, while "correspondence" signifies means of communication. The latter has been interpreted to include written letters, telephone, facsimile, and email communications.[193] General Comment No. 16

[190] UNGP (2011) 9.
[191] UNGP (2011) 25.
[192] ECHR Article 8; ICCPR Article 17; Universal Declaration of Human Rights, 10 December 1948, Article 12; Organization of the Islamic Conference, Cairo Declaration on Human Rights in Islam, 5 August 1990, Article 18.
[193] *Angel Estrella v. Uruguay* [CCPR], no. 74/1980.

states that gathering and holding of personal information on digital devices must be subject to state regulation and safeguards consistent with Article 17.[194] Further, the CCPR has provided commentaries on issues like telephone tapping,[195] interception of postal articles and telegrams,[196] and monitoring of electronic communications to fight terrorism.[197] In the latter the CCPR stated:

> "The State Party shall take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant and be consistent with obligations under Article 17 of the Covenant. To that effect, the State party should guarantee that the processing and gathering of information be subject to review and supervision by an independent body with necessary guarantee of impartiality and effectiveness."[198]

In sum, electronic surveillance and intelligence gathering is covered by the right to "privacy" and "correspondence" in ICCPR Article 17.

Similarly, ECHR Article 8 states that everyone has "the right to respect for his private and family life, his home and his correspondence." Interference by a public authority is allowed if it is "in accordance with the law" and is "necessary in a democratic society" in the "interests of national security" or other listed purposes.

The term "private life" covers aspects relating to personal identity, including a person's name, photo, or physical and moral integrity.[199] The protection provided by Article 8 is primarily designed to ensure the unfettered development of everyone's personality in their interactions with others, free from external interference.[200] It encompasses the protection of personal data and the privacy of communications,[201] including phone, email, and internet usage,[202] systematically collected and stored in a record,[203] regardless of whether the information is of a

[194] *General Comment No.16: Article 17* [CCPR], para. 10.
[195] *Concluding Observations on Poland* [CCPR], para. 22.
[196] *Concluding Observations on Zimbabwe* [CCPR], para. 25.
[197] *Concluding Observations on Sweden* [CCPR].
[198] Ibid, para. 18.
[199] *Vavřička and Others v. Czech Republic* [GC], no. 47621/13, para. 261.
[200] *Von Hannover v. Germany (no. 2)* [GC], no. 40660/08, 60641/08, para. 95.
[201] *S. and Marper v. United Kingdom* [GC], no 30562/04, 30566/04, para. 41.
[202] *Copland v. the United Kingdom* [J], no 62617/00.
[203] *Rotaru v. Romania* [GC], no. 28341/95, para. 44.

personal nature or not.[204] Nevertheless, sensitive data enjoys a heightened level of protection.[205]

The degree of the privacy invasion in the context of covert surveillance operations has been the focus of a thorough investigation by the ECtHR. Secret surveillance of citizens is only allowed when strictly necessary for safeguarding democratic institutions.[206] Such interference must be justified by relevant and sufficient reasons and must be proportionate to the legitimate objectives pursued.[207]

In *Big Brother Watch and Others v. the United Kingdom*, the ECtHR used eight criteria to establish the procedural safeguards of mass-surveillance. These include whether the domestic legal framework clearly defined the grounds and circumstances for the interception, procedure for authorization, procedures for selecting, examining, and using intercepted material, precautions when sharing the material, limits on the duration of interception, storage, and circumstances requiring erasure or destruction, procedures for independent compliance with the safeguards and independent ex post facto review.[208] The court envisioned the invasion of privacy as occurring in stages, starting with the initial data interception, increasing with its storage and automatic processing, and peaking with an intelligence analyst's assessment.[209] According to the court's reasoning, the growing invasion of privacy called for a stricter examination of the State's procedural protections.[210]

In *Centrum för Rättvisa v. Sweden*, also concerning bulk signals-intelligence, the court stated that data could only be shared if there was "an adequate level of data protection and […] no reason to fear that the information would be used to violate fundamental principles of the rule of law."[211] Although the statement concerned intelligence sharing between states, similar requirements must be expected of a company.[212]

[204] *Big Brother Watch and Others v. United Kingdom* [GC], no. 58170/13, 62322/14, 24960/15, para 330; Hellestveit and Wilhelmsen (2022) 23.
[205] *S. and Marper v. United Kingdom* [GC], para. 76.
[206] *Klass and Others v. Germany* [P], no. 5029/71, para 36; *Weber and Saravia v. Germany* [A], no. 54924/00, para. 106.
[207] *Segerstedt-Wiberg and Others v. Sweden* [J], no. 62332/00, para. 88.
[208] *Big Brother Watch v. United Kingdom* [GC], para 361.
[209] Ibid, para. 330-331.
[210] Ibid, para. 347; Shehabi (2022) 102; Watt (2022) 174; Davenport (2022) 203-204.
[211] *Centrum för Rättvisa v. Sweden* [GC], no. 35252/08, para. 140.
[212] See Section 1.4 and 4.1 on corporations' obligations to respect IHRL.

The above shows that ICCPR Article 17 and ECHR Article 8 protect the sharing of personal data, allowing interference if prescribed by law, necessary and proportionate, and accompanied by adequate safeguards and remedies.[213]

4.3 Human Right to Privacy in Armed Conflict

The application of IHRL during armed conflict was first recognized in the ICJ Advisory Opinion on *Nuclear Weapons* in 1996,[214] and later reaffirmed and expanded upon in 2004 in the *Wall in the Occupied Palestinian Territory* Advisory Opinion emphasizing the need to "take into consideration both these branches of international law, namely human rights laws, and as *lex specialis*, international humanitarian law."[215] The reference to *lex specialis* has been the origin of discussion since.

Contrary to common belief, some argue that the *lex specialis* reference is not about IHL taking precedence over IHRL, but is a shorthand for saying that the relevant obligations must be interpreted in light of, and consistently with, IHL rules.[216] In *Nuclear Weapons* this implies that what constitutes an unlawful killing under IHRL must be determined based on relevant IHL rules, including the fact that combatants and people taking a direct part in hostilities may be lawfully killed. This may be perceived as an application of the principle of systemic integration enshrined in VCLT Article 31(3)(c).[217]

As a legal concept, systemic integration presents a solution that may seem inclined towards integration. Certain scholars argue that when IHL incorporates aspects of IHRL through systemic integration, it becomes an inherent part of the IHL norm, applicable regardless of whether the IHRL rule applies.[218] I disagree, as the application of IHRL differs on a case-by-case basis dependent on the factual and legal circumstances. Whenever the IHRL rule is not applicable (see account on application of IHRL in Section 4.1) it will simply not serve as a means of interpretation. This is affirmed by the updated ICRC Commentaries mentioned in Section 4.1.[219]

[213] Grote (2023) 206.
[214] *Nuclear Weapons*, Advisory Opinion [ICJ], para. 25.
[215] *Palestinian Wall*, Advisory Opinion [ICJ], para. 106.
[216] Borelli (2015) 7.
[217] Ibid, 9.
[218] Steenberghe (2022) 1355.
[219] ICRC Updated Commentary GC I (2016), para. 35; ICRC Updated Commentary GC II (2017), para 35; ICRC Updated Commentary GC III (2020), para. 95.

Although presupposing that conditions for applying IHRL are present, one may argue that systemic integration is not applicable in the present case, as the human right to privacy stands contrary to current state practice within IHL.[220] Hence, integrating a right to privacy within the duty of constant care would not only complement an already existing rule, but establish a new one, supposedly rendering VCLT Article 31(3)(c) inapplicable.

However, if using the human right to privacy as the starting point, instead of the duty of constant care, the appliance of VCLT Article 31(3)(c) seems more intuitive. The human right to privacy is not an absolute, but a flexible norm dependent on the circumstances. Hence, it allows for an interpretation considering IHL, like the abovementioned interpretation of *Nuclear Weapons*. This stance also finds resonance with the latest ICRC Commentaries, indicating a shifting emphasis towards assessing the necessity of employing surveillance technologies during armed conflict.[221] The appliance of VCLT Article 31(3)(c) cannot be dependent on whether an IHL or IHRL norm is the primary legal basis before the Court.

Rather than suggesting one body of law becomes part of another, other scholars argue that systemic integration fosters an interconnectedness between two legal frameworks, allowing each body of law to maintain its characteristics while accommodating the other.[222] The ICJ affirmed in the *Namibia* Advisory Opinion that "an instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation."[223] Supporters of the narrow and first stated interpretation of Article 31(3)(c) will contend that such an interpretation is in reality, a joint application of two distinct bodies of law, not an interpretation of the IHL provision through systemic integration. Whether a broad interpretation of VCLT Article 31(3)(c) or a joint application is the most appropriate categorization in theory is left open for future research. In practice, the two branches of law must be considered in light of each other in any case. Thus, the question in the following is how the human right to privacy and the duty of constant care interplay.

In the 2004 *Palestinian Wall* Advisory Opinion, the ICJ acknowledged ICCPR Article 17 regarding privacy rights in the occupied Palestinian territories but provided limited clarification on its scope and limitations.[224] Similarly, the updated ICRC Commentary on GC II discussed

[220] See Section 3.6 and VCLT Article 31(3)(b).
[221] See Section 3.5.3.
[222] Fortin (2022) 348.
[223] *Continued Presence of South Africa in Namibia*, Advisory Opinion [ICJ], para. 53.
[224] *Palestinian Wall*, Advisory Opinion [ICJ], para. 128.

hospital ships sharing personal health data during armed conflict, referencing international privacy and data-protection standards without specifying their applicability.[225] Hence, both the ICJ and ICRC indicate that the human right to privacy may complement the duty of constant care within IHL.[226] Such an interplay will not interfere with the States' autonomy nor intention, as the interplay will only be relevant to the State in question when it has not derogated from its human rights obligations.

Two models reconciling IHL and IHRL dominate in legal scholarship. The so-called complementarity model holds that IHL and IHRL must be interpreted considering one another during armed conflict. Another approach is the conflict resolution model, which posits that IHL and IHRL are complementary unless a conflict emerges, at which one must choose between the IHL or IHRL rule.[227] As the right to privacy is not absolute, pertaining to freedom from the State's arbitrary and unlawful intrusions into an individual's private life, this relationship can be comprehended through the lens of the complementary approach. While a state may take actions that impinge upon an individual's right to privacy, if those actions are prescribed by law, necessary and proportionate, and accompanied by adequate safeguards and remedies, they remain in accordance with IHRL.[228]

The criteria of what is deemed necessary, proportionate, and adequate is highly dependent on the specific context and factual circumstances, of which IHL serves as the guiding framework. Within an armed conflict, there will thus exist an ongoing interpretative relationship between the protection of privacy and the principles of precautions in AP I Article 57 and military necessity.[229] The precautionary principle prescribes that military commanders are obligated to undertake everything feasible to verify that intended targets are not of a civilian nature. Moreover, they must take all feasible precautions when selecting the means and methods of attack to minimize unintended harm to civilians. These regulations impose an obligation on states to actively gather intelligence and conduct surveillance to differentiate between enemy forces and civilians proficiently. Consequently, the imperative to adhere to the Geneva Conventions and the Additional Protocols must shape the understanding of whether sharing specific information is necessary and proportionate under IHRL during armed conflict.[230] This

[225] ICRC Updated Commentary GC II (2017) para. 2403.
[226] Grote (2023) 210.
[227] West (2022a) 149.
[228] Lubin (2022b) 468-469.
[229] West (2022a) 150.
[230] Ibid.

evaluation is impacted by several factors.

First, the purpose of the intelligence gathering is of importance. For the duty of constant care and other principles of IHL to be applicable the information must be relevant to advancing combat. If not, only IHRL will apply.[231] Further, the purpose will impact the weight attributed to IHL. If the gathering has a clear targeting purpose, IHL must be given strong weight, often leading to lawful interference with the human right to privacy. Whenever the gathering has a broader or diffuse purpose, IHRL will set a higher threshold for legitimate interference. The latter will be the case for mass surveillance claimed to be justified by military necessity.[232]

Second, and as an extension of the previous point, data categorization is relevant. Location information is often important when planning an attack to distinguish civilians from combatants and to ensure proportionality. On the other hand, medical, financial, and legal information will rarely elevate military efforts. This means that civilian data that is irrelevant, or less relevant, for advancing combat, enjoys strong protection under IHRL. The sensitivity of the data will also impact the assessment, as sensitive data enjoys a heightened level of protection.[233]

Third, the situation on the ground is of relevance. The requirements for adhering to IHRL can fluctuate within the course of a conflict.[234] Due to the inherent nature of warfare, it must be recognized that choosing the least obtrusive methods, is not always feasible. It can be exceedingly challenging, particularly amid violence, to make determinations and guarantee that the information gathered on the battlefield is limited to what is necessary.[235] Thus, the higher the degree of intensity and difficulty in distinguishing civilians from combatants, the greater the encroachment on IHRL must be accepted. Instead, the State must be given great discretion to gather essential intelligence and conduct analyses to uphold the precautionary principles, as the human right to life stands stronger than privacy. Nevertheless, as the violence and risk of violence diminish, and territorial control consequently strengthens, infringements on privacy become less warranted.[236] When alternative methods can safely and effectively confirm the nature of a target with reduced impact on civilians, it must be used in alignment with IHRL.[237]

[231] Surveillance conducted with the aim of prosecuting an individual for a domestic crime would only be subject to IHRL, see Hellestveit and Nystuen (2020) 370 and 390.
[232] Davenport (2022) 189.
[233] *S. and Marper v. the United Kingdom* [GC], para. 76.
[234] West (2022a) 154; *Georgia v. Russia (II)* [GC], no. 38263/08.
[235] West (2022a) 151.
[236] Ibid, 154.
[237] Ibid, 151.

Based on the above, I suggest that the complementarity between IHRL and IHL during armed conflict in the discourse of privacy may be illustrated with the following rule:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.[238]
2. There shall be no interference by a public authority or non-state actor with the exercise of this right except when necessary to adhere to the principle of precautions[239] or gain a definite military advantage.

Hence, the human right to privacy constitutes the right, while the interference assessment must be based on the context at the relevant time considering the IHL principles of precautions and military necessity. The term "necessary" refers to an assessment of proportionality between the intensity of the privacy infringement and the legitimate purposes of precautions or military necessity. Furthermore, I suggest that this rule may hold the potential as a future rule of IHL *per se*. State acceptance of such a rule hinge on various factors, including its alignment with national interests, security considerations, and perspectives on balancing individual privacy and military priorities. Since the above privacy rule serves the dual objective of enhancing digital privacy protections during armed conflict while accommodating military necessity, there is a reasonable possibility for acceptance. Updated ICRC Commentaries may signal a shift towards a possible adaptation of such a necessity assessment in regards digital surveillance technologies.[240] However, any outcome rests upon negotiations and discussions among states and relevant stakeholders.

4.4 Operationalization of the Law

Thus far, the discourse has predominantly focused on mapping the privacy boundaries of IHL and IHRL binding upon the stakeholders involved in international armed conflicts. As mentioned in Section 1.4.1, the UNGP framework places responsibilities on corporations, although needing clarification to address the specific challenges encountered during armed conflict. With the IHL and IHRL framework established in Section 3 and 4.1-4.3 in mind, I will revisit the introductory examples provided. The legal solution to the scenarios in this section is

[238] Inspiration ECHR Article 8.
[239] See AP I Article 57.
[240] See Section 3.5.3 and 3.6.

valid both under the current interplay between IHL and IHRL, and in relation to the proposed IHL privacy rule.

State A demands to install surveillance equipment to gain direct access to information from MNOs and ISPs within its territory, claimed to be justified by military necessity. Approval would give State A access to all data stemming from telecommunications in the area. Networks tapping inherently encompass bulk interception of data, so-called mass surveillance, distinguishable from targeted cyber intelligence.[241] While some of the information obtained might be relevant for the hostilities, much of the information will be irrelevant. The purpose of the gathering therefore seems somewhat unclear, leading to questions of which legal frameworks apply, and to what extent. If the gathering is not related to hostilities, only IHRL will apply. As the claimed purpose of the gathering is military aims, one must however assume that both IHRL and IHL are applicable. The question is whether the information is necessary to adhere to the precautionary principle or gain a definite military advantage, thus legitimizing interference with the human right to privacy.

Although mass surveillance is very intrusive, especially when the data reaches an intelligence analyst,[242] it might be necessary to gather an overall picture of the situation. This holds especially true during intense hostilities, and the first stages of war, often being chaotic. This implies that full compliance with the eight requirements set forth by the ECtHR hardly can be expected.[243] However, as the intensity lessens, the interference might gradually become less warranted.[244] The case of Afghanistan is illustrative, where reports indicate that the coalition gathered biometric information from Afghans to maintain an advantage in identifying the enemy. During the early stages of force-on-force fighting this may have been justified, but not as the operation gradually transitioned into covert and law enforcement-style operations.[245]

Presupposing that the intelligence equipment was not installed, State A's authorities require real-time location information of subscribers from MNOs and ISPs. As the armed forces must distinguish civilians and civilian objects from military objectives and take all feasible precautions in attack, information suitable to shed light on the whereabouts of both combatants and civilians is crucial, and therefore normally proportional. The access must, however, be

[241] Davenport (2022) 189.
[242] *Big Brother Watch v. United Kingdom* [GC], para. 330-331.
[243] See Section 4.2.
[244] West (2022a) 151.
[245] West (2022b).

limited to areas of active or planned hostilities, and must cease whenever the area in question no longer is a place of planned attacks or hostilities.

Finally, State A demands personal information from multiple ICT companies, including medical, legal, and financial data, as well as communication records. Whether sharing personal information with State A is lawful, will depend on the categorization of the data. Medical data enjoys protection under IHL. Whereas legal and financial data seldom elevate combat and is therefore normally not shareable under IHRL. If such data is to be shared, the requesting state must prove its relevance, satisfying a high threshold.

Conversely, communication records may contain relevant information for war conduct. State A must therefore specify communication from whom or where and justify why this information is relevant. If the requested information stems from people whom there is reason to believe interact with armed forces or have relevant information, then interference is normally lawful. The company must also consider whether the State previously has misused data and the likelihood that the submitted demand contains accurate information. A broad collection of communication records closely resembles mass-surveillance, and will rarely be proportional unless justified by the intensity on the ground or the safeguards established in the *Big Brother Watch* are present.[246]

The above examples provide a simplified image by drawing the main lines of protected personal data. Multiple components will impact the assessment when faced with a real-world sharing demand. Determining whether the informational activity in question has a sufficiently close connection in terms of space, time, and relationship with the objectives of advancing military combat or adhering to the precautionary principle will involve some degree of discretion, resulting in numerous borderline cases.[247] The fluid nature of data sharing, characterized by the fact that information can serve various interests and purposes and evolve over time, adds significant complexity to the assessment.[248] Therefore, it is crucial for a company to conduct thorough due diligence assessments *before* armed conflict, enabling swift assessments and response to requests *during* armed conflict.

[246] *Big Brother Watch v. United Kingdom* [GC], para. 330-331.
[247] West (2022b).
[248] Lubin (2022a) 11-12.

5 CONCLUDING REMARKS

With this thesis, I set out to answer what obligations the duty of constant care stipulated in AP I Article 57(1) imposes on companies instructed by authorities to share customer data for intelligence purposes during armed conflict. The answer to the research question lies in the interpretation of AP I Article 57(1) (Section 3), and an assessment of the interplay with the human right to privacy (Section 4). Hence, the thesis provides a roadmap delineating the international legal framework that can guide company executives and other stakeholders as they navigate a principled approach to addressing challenges related to digital personal information during armed conflict.

The duty of constant care, enshrined in AP I Article 57(1), establishes a continuous duty of due diligence during armed conflict (Section 3). I contend that it is a broad obligation applicable to military activities with a connection to combat, including information gathering. Hence, the duty is applicable when relevant information reaches a military entity, requiring the company to conduct due diligence before sharing. Despite debate, I argue that civilian data is a "civilian object," implying that customer data is protected against attack. However, due to deviating state practice, the term "spare" does not extend to the sharing of civilian data, unless the data is impacted *per se* or the gathering is reasonably presumed to have an unlawful underlying purpose, such as discriminatory practices or public curiosity. Consequently, the duty of constant care codified in AP I Article 57(1) imposes only minor restrictions on the sharing of customer data from ICT companies to a state party in an armed conflict. Further, medical data benefits from a customary legal protection against sharing.

Although the duty of constant care does not protect information sharing sufficiently, the human right to privacy comes to its rescue (Section 4). Companies are expected to respect the human right to privacy regardless of the state behavior.[249] Whereas ECHR Article 8 and ICCPR Article 17 stipulate the right, the principle of precautions, including the duty of constant care, and military necessity justify interference. This implies that information necessary to exercise precaution and/or gain a definite military advantage, such as location information, normally will justify interference with the human right to privacy. The opposite applies to medical, financial, and legal data irrelevant to combat.

[249] See Section 1.4 and 4.1.

The digital privacy protection afforded by the interplay between the human right to privacy and the precautionary principle and military necessity under IHL constitutes a reasonable rule in terms of protection and practicability. Hence, I suggest that this interplay holds the potential to be established as a rule within IHL *de lege ferenda*. Today, a protection problem arises in terms of state conduct when the human right to privacy has been derogated, a reality seen in Ukraine.[250] Therefore, implementing a digital privacy rule within IHL is necessary, resulting in a higher threshold for interference with privacy rights during armed conflict, compared to today's legal situation.

Regrettably, the current legal landscape is characterized by rapid technological advancement, surpassing international rule prescribers' and rule appliers' regulatory capacity.[251] Therefore, discussing and creating new guidelines for digital privacy within IHL, as well as due diligence requirements in the ICT sector in the context of armed conflict, is crucial. Success in addressing these unresolved concerns will necessitate the active involvement of multiple stakeholders, including states, companies, international bodies, civil society, and the media.

Numerous captivating and contemplative inquiries await those ready to engage in the discussion. In addition to the questions addressed in this thesis, one may explore the following: How should ICT companies respond to government requests to censor or propagate online content, including disinformation, during armed conflict? Under what circumstances do companies run the risk of losing their protections under IHL? What is the extent and applicability of privacy and data protection obligations concerning non-state armed insurgency groups? By presenting these questions, I aim to encourage further academic exploration of corporate conduct and privacy protection during armed conflict.

[250] UN Human Rights Office of the High Commissioner (2022) 2.
[251] Lubin (2022b) 491.

Bibliography

Conventions and Other International Legal Instruments

Additional Protocol I [AP I] (1977)	Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the protection of Victims of International Armed Conflicts, Geneva, 8 June 1977.
ECHR (1950)	Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950.
General Data Protection Regulation [GDPR] (2016)	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.
Geneva Convention I (1949)	Geneva Convention (I) for the amelioration of the condition of the wounded and sick in armed forces in the field, 12 August 1949, 75 UNTS 31.
Geneva Convention II (1949)	Geneva Convention (II) for the amelioration of the condition of the wounded, sick and shipwrecked members of armed forces at sea, 12 August 1949, 75 UNTS 85.
Geneva Convention III (1949)	Geneva Convention (III) relative to the treatment of prisoners of war, 12 August 1949, 75 UNTS 135.
Geneva Convention IV (1949)	Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 75 UNTS 287.
Hague Convention IV (1907)	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, 18 October 1907.
ICCPR (1966)	International Covenant on Civil and Political Rights, 16 December 1966, United Nations, 999 UNTS 171.
ICJ Statute (1945)	Statute of the International Court of Justice, 24 October 1945, Treaty No. 993.
UNCLOS (1982)	Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 397.
VCLT (1969)	Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331.

Domestic Acts and Legal Documents

Transparency Act, LOV-2021-06-18-99.	Lov 18. Juni 2021 om virksomheters åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige arbeidsforhold (åpenhetsloven) [Act relating to enterprises' transparency and work on fundamental human rights and decent working conditions, Transparency Act].
Prop. 150 L (2020-2021)	Prop. 150 L (2020-2021) om Åpenhetsloven (Preparatory Work on the Transparency Act).

Jurisprudence

European Court of Human Rights (ECtHR)

Big Brother Watch and Others v. United Kingdom	*Big Brother Watch and Others v. United Kingdom* [GC], no. 58170/13, 62322/14, 24960/15, 25 May 2021.

Centrum för Rättvisa v. Sweden	*Centrum för Rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021.
Copland v. the United Kingdom	*Copland v. the United Kingdom* [J], no. 62617/00, 3 April 2007.
Georgia v. Russia (II)	*Georgia v. Russia (II)* [GC], no. 38263/08, 21 February 2021.
Klass and Others v. Germany	*Klass and Others v. Germany* [P], no. 5029/71, 6 September 1978.
Rotaru v. Romania	*Rotaru v. Romania* [GC], no. 28341/95, 4 May 2000.
Segerstedt-Wiberg and Others v. Sweden	*Segerstedt-Wiberg and Others v. Sweden* [J], no. 62332/00, 6 June 2006.
S. and Marper v. the United Kingdom	*S. and Marper v. the United Kingdom* [GC], no 30562/04, 30566/04, 4 December 2008.
Tyrer v. the United Kingdom	Tyrer v. United the United Kingdom [J], no. 5856/72, 25 April 1978.
Vavřička and Others v. the Czech Republic	*Vavřička and Others v. the Czech Republic* [GC], no. 47621/13, 8 April 2021.
Von Hannover v. Germany (no. 2)	*Von Hannover v. Germany (no. 2)* [GC], no. 40660/08 and 60641/08, 7 February 2012.
Weber and Saravia v. Germany	*Weber and Saravia v. Germany* [A], no. 54924/00, 29 June 2006.

<u>UN Human Rights Committee (CCPR)</u>

Angell Estrella v. Uruguay	*Estrella v Uruguay* [CCPR], Merits, Communication No 74/1980, UN Doc CCPR/C/18/D/74/1980, IHRL 2557 (UNHRC 1983), 29th March 1983.

Concluding Observations on Poland	*Concluding Observations on Poland* [CCPR], UN Doc CCPR/C/79/Add.110, 29 July 1999.
Concluding Observations on Sweden	*Concluding Observations on Sweden* [CCPR], UN Doc CCPR/C/SWE/CO/6, 7 May 2009.
Concluding Observations on Zimbabwe	*Concluding Observations on Zimbabwe* [CCPR], UN Doc CCPR/C/79/Add.89, 6 April 1998.
General Comment No.16: Article 17	*General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of the Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* [CCPR], UN Doc. HRI/GEN/1/Rev.9, 8 April 1988.
General Comment No. 31	*General Comment No. 31 on the Nature of the General Legal Obligation Imposed on State Parties to the Covenant* [CCPR], UN Doc. CCPR/C/21/Rev.1/Add.13, 26. May 2004.
Roger Judge v. Canada	*Roger Judge v. Canada* [CCPR], UN Doc CCPR/C/78/D/829/1998, 13 August 2003.

<u>International Court of Justice (ICJ)</u>

Continued Presence of South Africa in Namibia	*Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) Notwithstanding Security Council Resolution 276 (1970)*, ICJ Rep 16, 21 June 1971.
Kasikili/Sedudu Island (Botswana v. Namibia)	*Kasikili/Sedudu Island (Botswana/Namibia)*, Judgment, ICJ Rep 1045, 13 December 1999.
Legality of the Threat or Use of Nuclear Weapons	*Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Rep 226, 8 July 1996.

Maritime Delimitation (Somalia v. Kenya)	*Maritime Delimitations in the Indian Ocean (Somalia v. Kenya)*, Judgment, ICJ Rep 3, 2 February 2017.
Navigational Rights (Costa Rica v. Nicaragua)	*Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)*, Judgment, ICJ Rep 213, 13 July 2009.
Palestinian Wall Advisory Opinion	*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ Rep 2004, 9 July 2004.

International Criminal Tribunal for the former Yugoslavia (ICTY)

Prosecutor v. Anto Furundzija	*Prosecutor v. Anto Furundzija*, Trial Judgement, IT-95-17/1-T, International Criminal Tribunal for the former Yugoslavia, 10 December 1998.
Prosecutor v. Kupreškić	*Prosecutor v. Kupreškić et al.*, Trial Judgement, IT-95-16-T, International Criminal Tribunal for the former Yugoslavia, 14 January 2000.
Prosecutor v. Tadić	*Prosecutor v. Duško Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-AR72, International Criminal Tribunal for the former Yugoslavia, 2 October 1995.

Permanent Court of Arbitration (PCA)

Mauritius v. United Kingdom	*Mauritius v. United Kingdom (Chagos Marine Protected Area Arbitration)*, Final Award, ICGJ 486, Permanent Court of Arbitration 8, 18 March 2015.

Domestic Courts

Lafarge, Paris Court of Appeal	*Lafarge*, Paris Court of Appeal, France, 22 May 2022.

State Practice

Australian Military Manual (2006)	Australia, *The Manual of the Law of Armed Conflict*, Australian Defence Doctrine Publication 06.4, Australian Defence Headquarters, 5 November 2006.
Danish Military Manual (2016)	Denmark, Ministry of Defence, *Military Manual on international law relevant to Danish armed forces in international operations*, September 2016.
German Military Manual (2013)	Germany, Bundesministerium der Verteidigung, *Law of Armed Conflict Manual*, May 2013.
German Position Paper (2021)	Germany, Federal Government, *On the Application of International Law in Cyberspace*, Position Paper, March 2021.
ICRC (2022a)	ICRC, *Regional Consultation of Central and Eastern European States, 8 December 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts*, ICRC, Geneva, December 2022.
ICRC (2022b)	ICRC, *Regional Consultation of Latin American States, 9-10 November 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts*, ICRC, Geneva, June 2022.
Ministère des Armèes de France (2019)	Ministère des Armèes de France, *Droit International Appliquè Auc Opèrations Dans le Cyberspace* (Ministry of the Armed Forces of France, International Law Applied to Operations in Cyberspace), 2019.
New Zealand Military Manual (2017)	New Zealand, Defence Force, *Manual of Armed Forces Law*, Volume 4 (2 ed), DM69, 7 August 2017.

New Zealand Statement (2020) — New Zealand, Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace*, 1 December 2020, available at: https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace/ [read 11.10.2023].

Norwegian Military Manual (2013) — Norway, Forsvarssjefen, *Manual i krigens folkerett*, 2013.

United Kingdom Military Manual (2010) — United Kingdom, Ministry of Defence, *The joint service manual of the law of armed conflict*, JSP 383, September 2010.

United Kingdom Attorney General (2021) — Wright, Jeremy, *Cyber and International Law in the 21st Century*, United Kingdom Attorney General's Office, 2 May 2018, available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [read 11.10.2023].

United States Military Manual (2023) — United States, Department of Defense (DoD), *Law of War Manual*, July 2023.

UNODA (2021) — UNODA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, UN Doc A/76/136, 13 July 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

Books and Articles

Arato (2010) — Arato, Julian, "Subsequent practice and evolutive interpretation: techniques of treaty interpretation over time and their diverse consequences," *Law & Practice of*

International Courts and Tribunals, 9(3), 2010, 443-494.

Backer (2015) — Backer, Larry Catá, "Moving Forward the UN Guiding Principles for Business and Human Rights: Between Enterprise Social Norm, State Domestic Legal Orders, and the Treaty Law That Might Bind Them All," *Fordham Int'l LJ* 38(2) 2015, 457-542.

Blank and Jensen (2022) — Blank, Laurie R., & Eric Talbot Jensen, "LOAC and the Protection and Use of Digital Property in Armed Conflict" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 50-66.

Borelli (2015) — Borelli, Silvia, "The (mis)-use of general principles of law: lex specialis and the relationship between international human rights law and the laws of armed conflict" in Laura Pineschi (ed.), *General Principles of Law and the Judiciary: The Role of the Judiciary*, Cham: Springer International Publishing, 2015, 265-293.

Carrillo (2022) — Carrillo, Arturo J., "Between a Rock and a Hard Place? ICT Companies, Armed Conflict, and International Law," *Fordham Int'l LJ*, 2022, 46, 57-123.

Čertanec (2019) — Čertanec, Ann, "The connection between corporate social responsibility and corporate respect for human rights," *Law Economics and Social Issues Review* 10(2), 2019, 103-127.

Cooper (2021) — Cooper, Camilla G., «Cyberoperasjoner og krigens folkerett» in Camilla G. Cooper and

Emilie Aasheim (eds.) *Folkerettskonferansen 2021: Hybride trusler og cyberoperasjoner*, Forsvarets Høgskole, 2021, 22-34.

Davenport (2022) — Davenport, Tara, "The Use of Cable Infrastructure for Intelligence Collection During Armed Conflict: Legality and Limits" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 181-205.

Dinstein (2016) — Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed., Cambridge University Press, 2016.

Fleck (2007) — Fleck, Dieter, "Individual and State Responsibility for Intelligence Gathering," *Michigan Journal of International Law* 29(3), 2007, 687-709.

Fortin (2022) — Fortin, Katharine, "The relationship between international human rights law and international humanitarian law: Taking stock at the end of 2022," *Netherlands Quarterly of Human Rights* 40(4), 2022, 343-353

Geiß and Lahmann (2021) — Geiß, Robin and Henning Lahmann, "Protection of Data in Armed Conflict", *International Law Studies* 97(1), 556-572.

Gill et. al. (2017) — Gill, Terry, et. al, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare International Law Association Study Group on the Conduct of Hostilities in the 21st Century," *International Law Studies* 93(322), 2017, 321-388.

Graboritz, Morford and Truax (2020) — Graboritz, Beth D., James W. Morford and Kelley M. Truax, "Why the Law

of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data," *The Cyber Defense Review* 5(3) 2020, 121-132.

Grote (2023) — Grote, Tatjana, "Best of Both World? The Interplay between International Human Rights and the Law of Armed Conflict in Cyberspace," *LSE Law Review* 8 2023, 2023, 179-226.

Harlem and Taylor (2022) — Harlem, Mads and Mark B. Taylor, *Folkeretten og næringsvirksomhet i konfliktområder*, 2. ed., 2022, available at: https://www.fagforbundet.no/globalassets/solidaritetsprosjekter/filer/rapport-folkeretten-og-naringsvirksomhet-i-konfliktomrader-2022.pdf.

Hellestveit and Nystuen (2020) — Hellestveit, Cecilie and Gro Nystuen, *Krigens Folkerett* (1st edition), Universitetsforlaget 2020.

Hellestveit and Wilhelmsen (2022) — Hellestveit, Cecilie and Mathilde Wilhelmsen, *Ny teknologi og menneskerettigheter*, NHRI Report, 2022, available at: https://www.nhri.no/wp-content/uploads/2022/03/Ny-teknologi-og-menneskerettigheter.pdf.

Henckaerts and Doswald-Beck (2005) — Henckaerts, Jean-Marie and Louise Doswald-Beck; International Committee of the Red Cross (ICRC), *Customary International Humanitarian Law*, Volume 1: Rules, Cambridge University Press, 2005.

Hill-Cawthorne (2023) — Hill-Cawthorne, Lawrence, "Common Article 1 of the Geneva Conventions and the Method of Treaty Interpretation," *International & Comparative Law Quarterly* 72(4), 2023, 869-908.

ICRC (1975) — International Committee of the Red Cross, Committee III Summary

Record of the 21st Meeting: Consideration of Draft Protocols I and II, Vol. XIV, CDDHI III/SR. 21, 17 February 1975.

ICRC (2012) — International Committee of the Red Cross, "Ten questions to Philip Spoerri, ICRC Director for International Law and Cooperation," *International Review of the Red Cross* 94(887), 1125-1134.

ICRC (2019) — International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, ICRC Position Paper, 28 November 2019.

ICRC (2022c) — International Committee of the Red Cross, *What is International Humanitarian Law?*, ICRC Report, March 2022, available at: https://www.icrc.org/en/document/what-international-humanitarian-law.

ICRC (2023) — International Committee of the Red Cross, *Protecting Civilians Against Digital Threats During Armed Conflict, Recommendations to States Belligerents, Tech Companies, and Humanitarian Organizations*, ICRC Report, September 2023, available at: https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict.

ICRC Commentary AP I (1987) — Pilloud, Claude, et.al. (eds.) *Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff Publishers, 1987.

ICRC Commentary GC IV (1958) — International Committee of the Red Cross, *Commentary on the Geneva Conventions of 12 August 1949, Volume IV*, 1958.

ICRC Updated Commentary GC I (2016) — ICRC, *Updated Commentary on the First Geneva Convention – a new tool for generating respect for international humanitarian law*, Cambridge University Press, 2016.

ICRC Updated Commentary GC II (2017) — ICRC, *Commentary on the Second Geneva Convention: Demystifying the law of armed conflict at sea*, Cambridge University Press, 2017.

ICRC Updated Commentary GC III (2020) — ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War*, 2nd ed., Cambridge University Press, 2020.

Ingvarsson and Sannem (2021) — Ingvarsson, Bödvar and Jo Andreas Sannem, *Innføring i militærrett*, Gyldendal Norsk Forlag, 2021.

International Law Commission (2018) — International Law Commission, "Draft Conclusions on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties," *Report of the International Law Commission*, UN Doc A/73/10, 2018.

Karp (2014) — Karp, David J., *Responsibility for Human Rights: Transnational Corporations in Imperfect States*, Cambridge University Press, 2014.

Kröger, Miceli and Müller (2021) — Kröger, Jacob L., Milagos Miceli, and Florian Müller, "How Data Can Be Used Against People: A Classification of Personal Data Misuses," [Preprint] 30 December 2021. Available at: https://ssrn.com/abstract=3887097.

Lubin (2022a) — Lubin, Asaf, "The Duty of Constant Care and Data Protection in War" in Laura A. Dickinson and Edward Berg (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*

[forthcoming 2024], 2022, available at: https://ssrn.com/abstract=4012023.

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

Mačák (2015) — Mačák, Kubo, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review* 48(55) 2015, 55-80.

Macchi and Bright (2020) — Macchi, Chiara and Claire Bright, "Hardening soft law: the implementation of human rights due diligence requirements in domestic legislation" in Martina Buscemi, Nicole Lazzerini, Laura Magi and Deborah Ruddo (eds.*) Legal Sources in Business and Human Rights*, Brill Nijhoff, 2020, 218-247.

McCormack (2018) — McCormack, Timothy, "International humanitarian law and the targeting of data," *International Law Studies* 94(1), 2018, 221-240.

McKenzie (2021) — McKenzie, Simon, "Cyber Operations against Civilian Data," *Journal of International Criminal Justice* 19, 2021, 1165-1192.

Melzer (2009) — Melzer, Nils, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC Report, 2009.

Milanovic (2022) — Milanovic, Marko, "Surveillance and Cyber Operations" in Mark Gibney et. al. (eds) *Routledge Handbook on Extraterritorial Human Rights Obligations*, Routledge, 2022.

O'Connell (2022) — O'Connell, Mary Ellen, "Data Privacy Rights: The Same in War and Peace" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 12-28.

OECD (2002) — The Organization for Economic Cooperation and Development, *Measuring the Information Economy Annex 1. The OECD Definition of the ICT Sector*, 2002, available at: https://www.oecd.org/digital/ieconomy/2771153.pdf.

OECD (2023) — The Organization for Economic Cooperation and Development, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD Publishing, Paris, 2023, available at: https://doi.org/10.1787/81f92357-en.

Pillai and Kohli (2017) — Pillai, Arvind and Raghav Kohl, "A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and Other State Practice," *Oxford U Comparative L Forum* 3, 2017.

Pomson (2023) — Pomson, Ori, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law," *Journal of Conflict and Security Law*, 28(2), 2023, 349-387.

Rengel (2013) — Rengel, Alexandra, *Privacy in the 21st Century* (Vol. 5) Martinus Nijhoff Publisher, 2013.

Ritter and Mayer (2017) — Ritter, Jeffrey and Anna Mayer, "Regulating data as property: a new construct for moving forward," *Duke Law and Technological Review* 16 2017, 220-277.

Rodenhäuser (2023) — Rodenhäuser, Tilman, "The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law," *International Law Studies*, 100(1), 541-573.

Sarfaty (2022) — Sarfaty, Galit A., "Corporate Data Responsibility" in Laura A. Dickinson and Edward Berg (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (forthcoming 2024), 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105916.

Schmitt (2011) — Schmitt, Michael N., "Cyber operations and the jus in bello: key issues," *Israel Yearbook on Human Rights* 41, 2011, 113-135.

Schmitt (2014) — Schmitt, Michael N., "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Review* 25 2014, 269-299.

Schmitt (2015) — Schmitt, Michael N., "The Notion of "Objects" During Operations: A Riposte in Defence of Interpretive and Applicative Precision," *Israel Law Review* 48(1), 2015, 81-109.

Schmitt (2019) — Schmitt, Michael N., "Wired warfare 3.0: Protecting the civilian population during cyber operations," *International Review of the Red Cross*, 101(1), 2019, 333-355.

Shehabi (2022) — Shehabi, Omar Yousef, "Emerging Technologies, Digital Privacy, and Data Protection in Military

Occupation" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 87-112.

Steenberghe (2022) — Steenberghe, Raphaël van, "The impacts of human rights law on the regulation of armed conflict: A coherency-based approach to dealing with both the "interpretation" and "application" processes," *International Review of the Red Cross* 104(919) 2022, 1345-1396.

Todeschini (2018) — Todeschini, Vito, "The Impact of International Humanitarian Law on the Principle of Systemic Integration," *Journal of Conflict & Security Law* 23(3), 2018, 359-382.

UNGP (2011) — UN General Assembly, *Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie*, UN Doc A/HRC/17/31, Annex, 21 March 2011.

UN Human Rights Office of the High Commissioner (2022) — United Nations Human Rights Office of the High Commissioner, *Update on the human rights situation in Ukraine*, Report, March 2022, available at: https://www.ohchr.org/sites/default/files/2022-03/HRMMU_Update_2022-03-26_EN.pdf.

US Federal Trade Commission (2021) — US Federal Trade Commission, *A Look at What ISPS Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, FTC Staff report, 21 October 2021, available at: https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-

providers/p195402_isp_6b_staff_report.pdf.

Uvarova (2023) — Uvarova, Olena, "Sustainability in Transition: Corporate Respect for Solidarity" *Kharkiv Forum-Wageningen Law Series* 1, 2023, 1-22.

Velde (2022) — Velde, Jacqueline Van De, "From Telegraphs to Terabytes: The Implications of the Law of Neutrality for Data Protection by "Third" States and the Corporations Within Them" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 67-86.

Watt (2022) — Watt, Eliza, "The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflict" in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 157-180.

West (2022a) — West, Leah, "Face Value: Precaution versus Privacy in Armed Conflict," in Asaf Lubin and Russell Buchan, *The Right to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, 2022, 132-156.

Blog Posts, Media Articles and Websites

ECCHR — European Center for Constitutional and Human Rights [ECHHR], "Lafarge in Syria: Accusations of complicity in grave human rights violations," 18 May 2022, available at: https://www.ecchr.eu/en/case/lafarge-in-syria-accusations-of-complicity-in-grave-human-rights-violations/#case_case [read 7.11.2023]

Gisel & Rodenhäuser (2020) — Gisel, Laurent, & Tilman Rodenhäuser. "Cyber operations and international humanitarian law: Five key points" *Humanitarian Law and Policy Blog*, 28 November 2019, available at: https://blogs.icrc.org/law-and-policy/2022/06/28/shielding-prisoners-of-war-from-public-curiosity/ [read 24.08.23].

GNI Principles (2008) — Global Network Initiative Principles, 29 October 2008, available at: https://globalnetworkinitiative.org/gni-principles/ [read 11.09.23].

ICRC (2009) — International Committee of the Red Cross, "Direct participation in hostilities: questions and answers," 2 June 2009, available at: https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm [read 20.09.23].

Mahnad (2022) — Mahnad, Ramin, "Shielding prisoners of war from public curiosity," *Humanitarian Law and Policy Blog*, 28 June 2022, available at: https://blogs.icrc.org/law-and-policy/2022/06/28/shielding-prisoners-of-war-from-public-curiosity/ [read 13.11.2023].

Millett (2023) — Millett, Ed, "Deploying OSINT in armed conflict settings: law, ethics, and the need for a new theory of harm", Humanitarian Law and Policy Blog, 5 December 2023, available at: https://blogs.icrc.org/law-and-policy/wp-content/uploads/sites/102/2023/12/Deploying-OSINT-in-armed-conflict-settings_-law-ethics-and-the-need-for-a-new-theory-of-harm.pdf [read 6.12.2023]

Pratt (2019) — Mary K. Pratt, "ICT (information and communications technology, or technologies)", *TechTarget*, July 2019, available at:

https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies [read 24.10.2023].

Satariano and Frenkel (2022) — Satariano, Adam and Sheera Frenkel, "Ukraine War Tests the Power of Tech Giants," *The New York Times*, 28 February 2022, available at: https://www.nytimes.com/2022/02/28/technology/ukraine-russia-social-media.html [read 30.10.2023].

Solinge (2019) — Solinge, Delphine van, "Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address", *Humanitarian Law & Policy Blog*, 12 June 2019, available at: https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/ [read 24.08.2023].

Stupp (2022) — Stupp, Catherine, "Ukraine War Shows Need for Global Data-Privacy Agreement, EU Officials Say," *WSJ*, 25 May 2022, available at: https://www.wsj.com/articles/ukraine-war-shows-need-for-global-data-privacy-agreement-eu-officials-say-11653471001 [read 10.10.23].

West (2022b) — West, Leah, "Privacy vs. Precaution in Future Armed Conflict," *Lieber Institute West Point Articles of War*, 21 January 2022, available at: https://lieber.westpoint.edu/privacy-vs-precaution-future-armed-conflict/ [read 24.08.23].