Show Us the Films: Transparency, National Security and Disclosure of Information Collected by Advanced Weapon Systems under International Law

Eliav Lieblich

Israel Law Review / Volume 45 / Issue 03 / November 2012, pp 459 - 491
DOI: 10.1017/S0021223712000155, Published online:

Link to this article: http://journals.cambridge.org/abstract_S0021223712000155

How to cite this article:

Request Permissions: Click here
SHOW US THE FILMS: TRANSPARENCY, NATIONAL SECURITY AND DISCLOSURE OF INFORMATION COLLECTED BY ADVANCED WEAPON SYSTEMS UNDER INTERNATIONAL LAW

Eliav Lieblich*

The advent of modern technology such as drones provides states with unique capabilities to acquire, with ease, high-quality information regarding acts performed by armed forces and agencies, such as (but not only) targeted killings. In some cases, this information can shed light on the facts of the case, when alleged violations of international humanitarian law or international human rights law have occurred and thus investigation is called for. However, although calls for disclosure are increasing, states are reluctant to disclose information relating to such activities. This article discusses potential sources for obligations of disclosure, whether to civil society or to certain international bodies such as the International Criminal Court. In essence, the article posits that disclosure obligations can derive from the principle of transparency, as it applies, inter alia, to investigations, augmented by an emerging positive right to receive information. These obligations must be balanced, in turn, with considerations of national security. The article suggests that this balance, across a wide spectrum of international contexts, should be conducted in light of standards of necessity, proportionality and specificity. Accordingly, blanket non-disclosure may constitute a violation of international law or result in factual inferences to the detriment of states or individuals.

Keywords: international humanitarian law, international human rights law, transparency, disclosure, drones

1. INTRODUCTION

Consider this scenario: a state conducts a transnational drone strike against an alleged militant, in a remote tribal area. Following the strike, local sources claim that the drone had directly hit a nearby wedding party, killing dozens of civilians. Clips of carnage are uploaded to YouTube, raising immense public outcry. The state argues, in its defence, that the wedding party was hit not by its drones, but rather by stray mortar rounds, launched by militants immediately after the strike in order to incriminate the state. The state does not initiate a criminal investigation, declaring instead that analysis of operational debriefing negates any wrongdoing by its forces. Furthermore, beyond issuing laconic statements, the state does not disclose any material in support of its version, stating concerns of national security (‘The Basic Scenario’).

However, since the attack was conducted by drones, the state is undoubtedly in possession of visual data collected by the drone’s instruments. I shall call this data ‘monitoring information’.

* Lecturer, Radzyner School of Law, Interdisciplinary Center (IDC) Herzliya, Israel; JSD Columbia Law School, LLM Columbia Law School, LLB Hebrew University, elieblich@idc.ac.il. I wish to thank Eyal Benvenisti, Yonatan Berman, Itamar Gelbfish, Maria Varaki, Lihi Yona and the participants in the 2011 international conference ‘New Technologies, Old Law’, organised by the Minerva Center for Human Rights of the Hebrew University in Jerusalem and the International Committee of the Red Cross. Last, but not least, I wish to thank the editorial team at the Israel Law Review for their meticulous analysis and comments. Of course, any error whatsoever, in fact or in law, remains my own.
Such data might have unique potential to impugn or exonerate the state and the individuals who took part in the operation. Accordingly, it can also serve to implicate or vindicate the state’s decision not to open an investigation. This article therefore asks a rather straightforward question: can states be obliged to disclose such information under existing international law norms? If so, what are the legal ramifications of refusal? As with many legal problems, while the question is simple, the answer is complex, and depends heavily on the terms we use. Thus, it should be emphasised that, while the term ‘obligation’, in plain language, refers to direct, positive duties to physically grant access to information, the use of the term in this article connotes a wider meaning. It refers also – and perhaps mainly – to situations in which refusal to disclose can result in adverse factual assumptions against the withholding state or an accused individual, even if, as will be discussed below, positive disclosure duties cannot be legally or practically imposed.

While the question of disclosure of monitoring information in international law as such has yet to be addressed in full force, there are ample grounds to believe, when analysing current trends regarding disclosure in general, that the question might require international legal attention in the near future. Accordingly, a normative, forward-looking discussion of the issue can be of substantial value. By no means pretending to exhaust the many dilemmas spawned by this problem, this article can hopefully outline the boundaries of – or set the stage for – further and detailed debate on the question.

In recent years, much controversy has arisen concerning acts of armed forces (and intelligence agencies) operating in relatively closed or remote environments, in which they are able, to a large extent, to control information – whether by deploying means of electronic warfare, exercising unique physical control over the operational environment (which allows them, inter alia, to confiscate video devices held by individuals), or by conducting swift surprise attacks by unmanned aerial vehicles (drones).1 Perhaps paradoxically, the same technologies that enable states to conduct operations in such environments, place them also in unique positions – not available in the past – to acquire and maintain high-quality monitoring information regarding all stages of the operation.2 Such information, collected by systems such as drones and other advanced instruments, can greatly shed light – at least in some cases – on the factual circumstances when investigation is needed.3 This aspect of the recent technological leap has not been widely debated, although states are under increasing pressure to disclose the legal and factual basis for their actions.

It is beyond question that advanced capabilities possessed almost uniquely by states allow them to collect high-quality information bearing significant evidentiary value, thereby granting

1 Two noteworthy examples could be the May 2010 Israeli interception of a Gaza-bound flotilla, and the US killing of Osama bin Laden in March 2011.
3 This potential can be also utilised by states to implicate others: for instance, according to media reports, the data-collecting capabilities of drones were employed by the US over Syria, to monitor the regime actions against the opposition: Zvi Bar’el, ‘Report: US Drones Flying over Syria to Monitor Crackdown’ (Ha’aretz, February 2012), http://www.haaretz.com/news/middle-east/report-u-s-drones-flying-over-syria-to-monitor-crackdown-1.413348. We shall address this issue briefly in the context of Israel and Egypt, in Section 4.1.
them a de facto monopoly over the control of evidence in specific instances. Moreover, it is certain that once the decision is made to use such systems, states automatically acquire this evidence without the need for further substantial effort. The ease of the production of this evidence, combined with the unique capabilities of states in this respect, augmented by the potential benefits of their disclosure in the promotion of accountability, undoubtedly gives rise to a general interest in disclosure.⁴ As argued polemically by William Schabas, in the context of the bin Laden operation:⁵

The United States government is the only body in possession of the facts. It has a duty to make things clear. There can be no doubt … that the soldiers involved had video-cameras on their helmets. Possibly, they were acting in self-defence. But in any court of law, he or she who invokes self-defence as a justification for killing another human being has a burden of proof to demonstrate that the action was proportional … But who knows? So show us the films and we can all decide.

The legality of the bin Laden operation, or of any other, is not the concern of this article. The article focuses, in a forward-looking manner, on the normative question of disclosure, and in particular, with regard to information acquired through advanced monitoring systems. Of course, the public interest in disclosure might conflict with legitimate concerns of national security. However, such concerns, as we shall see, cannot be absolute and must be reasonably balanced with other interests.

The first question one must ask is ‘disclosure to whom?’ In other words, who are the potential beneficiaries of disclosure obligations? When we say ‘disclosure’ we can refer to obligations towards a variety of actors, ranging from individuals in victim participation frameworks to states involved in adversarial international litigation or arbitration. This article, however, analyses disclosure obligations in terms of two extremes: on one side of the spectrum, it discusses disclosure to the general public; and on the other, disclosure to international courts. It focuses on the former owing to the central role of civil society in the disclosure debate as part of the increasing role of non-governmental organisations (NGOs) in the international system at large. It addresses disclosure to international courts, since they represent more structured and tangible bodies, operating under relatively traditional concepts of law. Between these extremes, the normative balance between the competing interests is remarkably similar; however, the results of the balance may be affected by the nature of the beneficiary body.

Within this distinction, another sub-categorisation is merited: between different types of disclosure. One type of disclosure is of the kind that might be required from a state in relation to suspected violations of international law, whether in the context of international adjudication or otherwise. Such obligations, spawning from the principles of accountability and transparency, can be supplemented by the right to access or receive information, as part of the right to freedom

⁴ See Beard (n 2) 421 (‘The introduction of virtual surveillance capabilities dramatically increases the pressure on states to deploy information to rebut accusations of misconduct on the part of their military forces’).
of expression. They might arise, furthermore, in conjunction with the state’s duty to investigate alleged violations. A second type of disclosure refers to general, procedural obligations, which may be accrued in litigation in various instances. The former aspect, as we shall elaborate below, is the main concern of this article, since it is in these situations where public interest in disclosure would be the strongest. The latter aspect, conversely, is a considerably wider subject, which is closer to questions of adversarial due process than to general public interests and, as such, is less relevant in our context.

The structure of the argument is as follows. Section 2 lays down the basic normative environment for our discussion, and the general competing interests at stake. It discusses the principle of transparency and its different aspects, the duty to investigate violations of international humanitarian law (IHL) and international human rights law (IHRL), and the complex interaction between these notions. It thereafter addresses the question of disclosure and national security. Section 3 demonstrates that the current debate regarding technological advances largely disregards the transparency enhancing potential inherent in such technologies, and specifically in their data-collecting capabilities. Taking into consideration this potential, Section 4 addresses the increasing calls for disclosure of information in the context of targeted killing operations. It should be noted that the focus on targeted killing is not a principled one: indeed, similar calls can be made in the context of any state act. However, the article devotes special attention to targeted killings because it is in this context that the nexus between high technology and lethality is most prevalent, and therefore might give rise to increased disclosure interests. In Section 5 the article addresses the question of disclosure to civil society, demonstrating that domestic freedom of information legislation – mainly in the US, where the issue has been heavily debated – is unlikely to be effective, in relevant contexts, in promoting disclosure – including, of course, of monitoring information. The section then discusses the emerging positive international right to access information.

Thereafter, the article moves to address potential disclosure obligations in relation to certain international bodies. Since there is a plethora of such bodies – the discussion of all being well beyond the scope of this article – I have chosen to survey the relevant mechanisms in selected universal, or almost-universal, bodies with forward-looking jurisdiction, such as the International Criminal Court (ICC) and the International Court of Justice (ICJ). However, the gist of the argument would probably be applicable to other international bodies. Thus, Section 6 deals with disclosure of monitoring information in international criminal proceedings, both in the context of the principle of complementarity and with regard to the inference of facts in cases of non-disclosure. Finally, Section 7 briefly addresses how disclosure of monitoring information can affect the burden of proof in international litigation. I shall also make a preliminary argument regarding disclosure and international fact-finding missions.

In general, as we shall see, while the mechanisms addressed in this article vary in terms of structure, purpose and powers, it seems that the principles of necessity, proportionality and specificity – meaning, the duty to give reasons for withholding information – universally govern the delicate balancing required between the public interest in disclosure of monitoring information, and the legitimate national security interests of states.
2. THE BASIC FRAMEWORK: THE PRINCIPLE OF TRANSPARENCY AND THE DUTY TO INVESTIGATE

2.1 THE VARIOUS ASPECTS OF THE PRINCIPLE OF TRANSPARENCY

In general, calls for disclosure of information concerning forcible acts can be based on the principles of accountability and transparency, as they can be deduced from IHL and IHRL.\(^6\) In parallel, and supplementing these calls, the principle of transparency can also be grounded in the positive right to access information, as part of the right to freedom of expression. It is worth clarifying the essence of these principles.

The duty of states, as set out under IHL and IHRL, comprises not only the duty to respect the obligations entrenched in the various conventions, but also to enforce them.\(^7\) It is in this context that the principle of accountability should be understood: it reflects, inter alia, the duty to investigate and prosecute serious violations and to provide, when applicable, effective remedies to victims.\(^8\)

The traditional normative justification for the principle of transparency in international law is found, first and foremost, in its being a cardinal condition for the effective public and institutional scrutiny of states’ adherence to their international obligations.\(^9\) Such scrutiny is paramount to the legitimacy of any legal regime,\(^10\) and is a crucial factor for compliance in the decentralised international system, in which enforcement mechanisms are notably weak. In the context of IHL and IHRL, an important aspect of transparency is found in that it promotes accountability: it allows individuals, NGOs and the international community at large to monitor the implementation of the duty to investigate (and to prosecute, where required) breaches of applicable international law, where there are sufficient prima facie suspicions that violations have occurred. It enables them to determine whether an investigation – if not initiated – is required and, if undertaken, whether it is conducted in a prompt, thorough and impartial manner.\(^11\) Thus, transparency is mainly

---


\(^8\) The term accountability can refer to individuals as well as states. For an in depth discussion of the term, see Yarwood (n 6) 9–34.

\(^9\) See, eg, Human Rights Committee, General Comment 34, Art 19: Freedoms of Opinion and Expression (2011) UN Doc CCPR/C/64/3 para 2 (GC 34).

\(^10\) On transparency (and other procedural obligations) and the legitimacy of international law, see John Tasioulas, ‘The Legitimacy of International Law’ in Samantha Besson and John Tasioulas (eds), *The Philosophy of International Law* (Oxford University Press 2010) 97, 114–15.

\(^11\) The Basic Principles and Guidelines on the Right to Remedy and Reparations for Victims of Violations of International Human Rights and Serious Violations of International Humanitarian Law, UNGA 60/147, 16
perceived as an instrumental, perhaps ‘secondary’, obligation – facilitating the enforcement of duties, including the duty to investigate and to prosecute violations (investigative transparency). However, investigative transparency is by no means a simple concept; we shall touch upon a few of its complexities in the next section.

The principle of transparency can nonetheless serve a large range of ends, beyond the investigative aspect. As we shall see, it might be emerging also as a primary international obligation in itself, viewed as an integral part of the right to freedom of expression (expressive transparency), and manifested, inter alia, in the positive right to receive information. The rationale underlying the notion of expressive transparency is that, absent access to information, public debate is inhibited. The latter understanding of the principle of transparency, when taken into account in the context of the duty to investigate, can serve to enrich and solidify it, and place it within a wider framework of IHRL jurisprudence. Expressive transparency can also be understood as part of a general administrative, or deliberative, notion of the principle, meant to promote greater public participation in policy making.

2.2 THE DUTY TO INVESTIGATE AND TRANSPARENCY: A COMPLEX RELATIONSHIP

Duties to investigate alleged violations can be found in both IHRL and IHL. In IHRL this duty is particularly developed. In fact, failure to investigate gross violations could itself give rise to a separate violation of human rights law. However, there is a difference between the scope, character and ‘triggers’ of the duties to investigate under IHL and IHRL – the latter being obviously wider, as expounded in important decisions of the European Court of Human Rights.

---

12 See, eg, McKerr v United Kingdom ECHR 2001-111 475, para 141, 154; Amichai Cohen and Yuval Shany, ‘Beyond the Grave Breaches Regime: The Duty to Investigate Alleged Violations of International Law Governing Armed Conflict’ (2012) Research Paper No 02-12, International Law Forum, The Hebrew University of Jerusalem, 24–25; Seibert-Fohr (n 11) 137. A close concept to investigative transparency is the issue of victim participation. The latter, however, is more concerned with the promotion of ‘restorative’ justice vis-à-vis the victim than with scrutinising the duty to investigate, and thus I will not elaborate on this issue.


Under IHL, the duty to investigate – regarded by the International Committee of the Red Cross (ICRC) as an obligation entrenched in customary international law\(^{17}\) – can be deduced from several sources.\(^{18}\) Chief among them is the *grave breaches regime* as set out in the four Geneva Conventions. As provided, for instance, in Article 146 of the Fourth Convention, the grave breaches regime obligates states to enact effective penal sanctions for any grave breach of the Convention as enumerated in Article 147,\(^{19}\) to search for suspects, to prosecute them regardless of their nationality or to extradite them.\(^{20}\) The obligation to actively ‘search for’ suspects effectively imposes upon states the duty of investigation, as a necessary condition for the fulfilment of the grave breaches regime.\(^{21}\) In addition, Article 146 requires contracting parties to take ‘measures necessary’ for the ‘suppression’ of all violations of the Convention other than grave breaches. It is obvious that any duty of ‘suppression’ – whatever its exact content, and whether it relates to criminal procedures or otherwise – requires *at least* previous investigation, in some form, since any suppression must rely on some determination of the factual premise regarding the alleged prohibited acts.\(^{22}\)

However, the scope and nature of the obligation to investigate under IHL – as well as its interaction with corresponding duties under IHRL – remains disputed. Significant disagreement encompasses a wide variety of questions, including those relating to the nature of or types of violation that must be investigated; the ‘triggers’ for the duty to investigate; and the identity and characteristics of the competent investigating organs. These questions are addressed thoroughly elsewhere, and are beyond the scope of this article.\(^{23}\) For our purposes, the article presumes the existence of circumstances in which a duty to investigate has indeed arisen, whether under IHL or IHRL; and moreover – as is widely accepted in contemporary literature and international adjudication\(^{24}\) – that both IHL and IHRL apply, in some form, during armed conflict.\(^{25}\)


\(^{18}\) See Cohen and Shany (n 12) 4–11.

\(^{19}\) The list of ‘grave breaches’ is supplemented in art 85 of Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), (entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I).


\(^{22}\) cf Cohen and Shany (n 12) 4–7 with Schmitt (n 15) 39.


\(^{25}\) Cohen and Shany (n 12) 11–13; Tomuschat Report (n 16) paras 29–34.
Be that as it may, it seems correct that the duty to investigate – and any respective transparency requirements – is more onerous in relation to actions closer to law enforcement activities, such as those taking place in situations of occupation, and narrower during ‘pure’ combat operations. Nevertheless, armed conflict and transparency are not always mutually excluding. For instance, even if in practice it is more difficult to conduct transparent investigations under intensive combat, this might be less true in asymmetric conflicts, in which states are often not under the same systemic duress that occurs in traditional, wide-scale wars. Also, in the latter cases, there is, in general, no inherent difficulty to fulfil the principle of transparency post bellum.

In any case, what is the exact role of transparency within the duty to investigate? In other words, to what extent is transparency required for an investigation to be considered as having been conducted in accordance with international standards? Indeed, the relationship between these concepts is a complex one, making it difficult to pinpoint just when lack of transparency indicates deficient investigatory practice. This is because transparency can relate to procedure (whether the process of investigation is transparent), or to substance (whether the decision making and discretion of the investigating authorities is transparent). It can refer to public access to information regarding the investigation (through freedom of information rights or, if the matter is brought before a court, in open proceedings), or to institutional oversight (manifested, for instance, in supervision by parliamentary subcommittees). As such, transparency is more of a spectrum than an absolute term: the effects of its existence or absence over the assessment of investigatory practices are highly contextual.

Moreover, the significance of transparency, in relation to investigatory duties, should be assessed in the light of three types of situation in a descending rate of acuteness. The most acute need for transparency arises when the state does not commence an investigation at all, claiming that there is no prima facie evidence of wrongdoing. The second situation arises when a state investigates but decides not to prosecute. The third occurs where prosecution does indeed take place, but the accused is exonerated (and here I set aside the issue of ne bis in idem which, being related to the rights of the accused, should be analysed, in most instances, separately from the obligations of the prosecuting state). It could therefore be argued that, in each of these situations, non-transparent practices might give rise to an attendant presumption against the state, its robustness in line with their descending acuteness.

Nevertheless, when analysing the situations above, transparency expectations can also be affected by the general characteristics of the relevant system; in other words, they can be informed by the level of independence and impartiality attributed to the investigating or adjudicating authorities. I shall touch upon this issue when discussing, in Section 6.1, the relations between transparency and the principle of complementarity. In sum, even if one adopts a narrow view of the obligation to investigate, the complex relations between the latter obligation and the principle of transparency make it unlikely that it could justify a blanket policy of non-transparency, applicable in all cases.

26 Tomuschat Report, ibid para 32.
27 ibid.
2.3 Disclosure and National Security

As with other public interests, transparency is not absolute, and must be frequently balanced with competing interests.\(^2^9\) When discussing issues pertaining to armed conflict and forcible acts at large, a competing interest of foremost importance is national security; indeed, complete disclosure of monitoring information can reveal classified capabilities and methods of warfare. In this context, while the investigative, expressive and administrative-deliberative aspects of transparency intertwine, they remain distinct: it seems reasonable that when disclosure claims are not only based on general administrative grounds or on those relating to the freedom of expression, but are made also in conjunction with the duty to investigate – that is, where there is sufficient suspicion that violations of law which require investigation have occurred – the transparency principle will have more weight when balanced against other valid interests, such as national security.\(^3^0\)

Any discussion of disclosure obligations and national security gives rise to three main challenges: substantive, practical and procedural. The substantive challenge posits that the power to assess national security concerns, if given to or appropriated by international bodies, impinges excessively on the notion of state sovereignty, of which the capacity to independently determine national security needs is a central pillar. However, this claim should be analysed in the light of wider trends in international law. While deference to national security claims, both generally and specifically regarding disclosure, is still dominant in certain international regimes – such as WTO law\(^3^1\) – this is not entirely the case with regard to fields of law that deal, at large, with the protection of basic rights.

Particularly, this is a result of the shift, in recent decades, in the understanding of the concept of sovereignty, from its traditional ‘black box’ view as territorial effective control,\(^3^2\) to a more substantive understanding of sovereignty as ‘responsibility’. The latter perception is an amalgamation of various processes, in which some traditional elements of sovereignty have been reformulated in a manner that could allow external actors to pass some judgment, to varying effects in different contexts, also on questions related to states’ national security.\(^3^3\) These processes can be

\(^{2^9}\) Fisher (n 13) 280–81.

\(^{3^0}\) cf Cohen and Shany (n 12) para 3.4.1.2.4.

\(^{3^1}\) General Agreement on Tariffs and Trade (GATT 1947), art XXI(a); see Petros Mavroidis, Trade in Goods (Oxford University Press 2007) 322–31; and even in this context states have been careful in invoking the national security exception: see Roger P Alford, ‘The Self-Judging WTO Security Exception’ (2011) 3 Utah Law Review 697.

\(^{3^2}\) See, eg, Lassa Oppenheim and Ronald Roxburgh, International Law (vol 1, 2nd edn, Longmans 1912), arts 123–24 (defining sovereignty as comprising independence, territorial and personal supremacy); see also Hersch Lauterpacht, Recognition in International Law (Cambridge University Press 1947) 103.

identified, inter alia, in the growing emphasis on the protection of civilians in IHL;\textsuperscript{34} in the increasing predominance of human rights instruments that limit derogation from certain rights, even when claimed to be justified on grounds of national security;\textsuperscript{35} in the understanding that some violations of international law operate \textit{erga omnes};\textsuperscript{36} and in mechanisms of international criminal law, which delegate to international institutions powers to assess the validity of domestic criminal proceedings,\textsuperscript{37} or to pass judgments or make inferences regarding their national security claims.\textsuperscript{38}

For instance, as was recognised by the ICTY, when investigating or adjudicating upon violations relating to the use of military force, access to military documents – among them, potentially, those that constitute monitoring information – can be of acute importance, since such material might comprise a substantial part of the evidence.\textsuperscript{39} Therefore, granting states an unfettered, blanket right to withhold such information, simply by citing national security concerns, can undermine the very purpose that international tribunals set out to achieve. This can only mean, in practice, that some international organs must have the power to substantively assess the national security concerns of states.\textsuperscript{40} The question, thus, is one of reasonable balance, and as such, national security cannot be a ‘magic word’ that trumps all.

Related to these sovereignty-based concerns, is the \textit{practical} argument, asserting that in any case, it is unlikely that sovereign states will comply with disclosure obligations, even if such obligations are generally merited. This is indeed a valid claim, considering the well-known weaknesses of international law.\textsuperscript{41} For this reason, we stop short of suggesting that in the current international system, absent substantial coercion, states can be effectively obliged, whether by human rights treaty bodies, by most international courts,\textsuperscript{42} or through any other mechanism short of a binding Security Council resolution,\textsuperscript{43} to hand over monitoring information. Instead, our approach is more modest – arguing that in most relevant cases refusal to disclose might result in adverse factual inferences rather than in direct disclosure obligations \textit{sensu stricto}. This


\textsuperscript{35} ICCPR (n 7) art 4.

\textsuperscript{36} \textit{Case Concerning the Barcelona Traction, Light and Power Company Ltd (Belgium v Spain) [1970] ICJ Rep 3, [33]–[34].}

\textsuperscript{37} Through the notion of ‘complementarity’, see discussion in Section 6.2.

\textsuperscript{38} Rome Statute of the International Criminal Court (entered into force 1 July 2002) 2187 UNTS 90 (ICC Statute), art 72, discussed in Section 5.


\textsuperscript{40} Ibid (‘To admit that a State holding such documents may unilaterally assert national security claims and refuse to surrender those documents could lead to the stultification of international criminal proceedings: those documents might prove crucial for deciding whether the accused is innocent or guilty. The very \textit{raison d’être} of the International Tribunal would then be undermined’).


\textsuperscript{42} Regarding the enhanced power of the ICTY to order disclosure, cf Blaskić (n 39) [61]–[69].

\textsuperscript{43} See, eg, UNSC Res 827, UN Doc S/RES/827, 25 May 1993, para 4 (deciding, under Chapter VII of the UN Charter, that all states shall cooperate fully with the ICTY); ICTY Rules of Procedure and Evidence, UN Doc IT/32/Rev.36, 20 October 2011, art 7bis(A) (providing that when a state fails to comply with obligations provided for in the ICTY Statute, the President shall report the matter to the Security Council).
balanced ‘sanction’ is reminiscent, to some extent, of domestic criminal discovery mechanisms, in which the prosecution, if choosing to rely on national security privileges, might pay a cost by suffering the dismissal of the case.\textsuperscript{44} Arrangements of such order can assure, to the extent possible in the international system, that blanket national security claims, as justifications for withholding of monitoring information, would be less hastily made.

A third prong of this sceptical challenge concerns \textit{procedural} aspects – questioning the manner in which refusals of disclosure would be assessed, or the methods of determination that non-disclosure might give rise to adverse inferences (namely, the question of ‘who will see’ the information). Since we are here concerned with the general normative aspects of the question – and across a broad spectrum of institutions – an in-depth discussion of procedure is beyond this article. Nonetheless, it is worthwhile to delineate the outlines of such future analysis. In essence, a distinction should be made between the rare instances in which a state is obliged (or consents) to \textit{positively} disclose information. In such cases, flexible \textit{ex parte} or \textit{in camera} arrangements can be made. Of course, this option is relevant to adjudicatory bodies, and has no bearing, in general, over public disclosure obligations. Conversely, in cases where failure to disclose merely results in factual inferences, procedural challenges of this type are less significant, since the question of whether adverse inferences are merited is chiefly decided in the light of circumstances \textit{external} to the withheld material – namely, the general legal and factual context of the case. At large, the more the monitoring information might be instrumental in the exposure of the legal truth in the specific instance – and the more the withholding of information is sweeping – the more a party’s refusal to disclose can give rise to inferences against it. The latter logic applies equally in international tribunals and in other, less formal arrangements, such as assessments by NGOs, treaty bodies or fact-finding missions.

3. \textsc{Advanced Technology as an Agent of Transparency}

Having discussed the interaction between transparency, investigations and national security, it is important to note a significant, though frequently overlooked, characteristic of advanced technology: its inherent potential to \textit{promote} transparency, and thus facilitate accountability.\textsuperscript{45} Interestingly, this by-product of the use of high technology is largely absent from recent arguments of both the critics and supporters of the deployment of such measures.

\textsuperscript{44} In the US, see, eg, \textit{Classified Information Procedures Act}, 18 USC App III, s 6(e)(2)(A)–(C); see Alexandra AE Shapiro and Nathan H Seltzer, ‘Litigating Under the \textit{Classified Information Procedures Act}’ (2009) 45 Criminal Law Bulletin 920 (‘[The law] recognizes that the defendant’s right to present his defense and the government’s desire to prevent the disclosure of classified information cannot always be accommodated, and in those circumstances, the defendant’s constitutional rights must prevail, and the government may choose to forego a prosecution rather than disclose classified information’).

\textsuperscript{45} For a comparable argument see Beard (n 2) 418–22 (‘the ubiquitous information flowing from persistent surveillance brings with it new expectations, together with unprecedented levels of transparency’).
In this context, extensive attention has been given to the transparency deficit that might occur when advanced weaponry is utilised by civilian intelligence agencies, and in particular the CIA.\(^{46}\) However, these critiques are aimed mainly towards the non-transparent way in which these agencies operate – or to the lack of public oversight of their actions – and should not be confused with an ostensible transparency deficit inherent in the weapons they use. This confusion is often made in the public discourse: for instance, when a recent New York Times op-ed asked ‘Do Drones Undermine Democracy?’\(^{47}\) it would have been more precise to ask whether the way in which drones are used undermines democracy.

Accordingly, an analysis of much of the critique concerning the deployment of drones reveals that, in actuality, it mainly amounts to procedural-institutional concerns regarding the operation of such weapons by the CIA.\(^{48}\) Although some of these critiques touch upon transparency issues, the problems they raise are, at large, not inherent in drones themselves;\(^{49}\) in any case, even if drones can indeed contribute to some transparency deficits in certain cases, these can be offset by the transparency potential embodied in the data collection capacities of the same technology.

For instance, one critic claims that high technology inhibits the fulfilment of the principle of transparency because of its capacity to enhance secrecy. Indeed, it is true that advanced weaponry can facilitate the secrecy of an operation. Drone operations are swift, can take place in remote areas, and are exposed only to very few people.\(^{50}\) Accordingly, states can deny or otherwise refuse to confirm that a drone attack has even taken place, or that it was actually carried out by their forces. These transparency deficits are enhanced when drone attacks are conducted by secret civilian agencies, with obscure control mechanisms and an undisclosed command structure.\(^{51}\)


\(^{49}\) For instance, one institutional critique asks whether CIA agents are allowed at all to use force under international law, or rather should they be considered ‘unlawful combatants’ as they are not members of a state’s armed forces. Not surprisingly, the supporters of the use of drones by the CIA are quick to rebuff such concerns: they find no special objection to the operation of such systems by persons who are not members of armed forces, and proceed to place the CIA’s involvement in such operations within the familiar paradigm of non-combatant direct participation in hostilities: see, eg, Anderson Testimony I, ibid paras 22–24 (quoting Mary Ellen O’Connell and Gary Solis); Michael N Schmitt, ‘Drone Attacks Under the Jus ad Bellum and Jus in Bello: Clearing the “Fog of Law”’ (2010) 13 Yearbook of International Humanitarian Law 311, 324–25; see discussion in Henderson (n 48) 142–59 (analysing the possible status of civilian intelligence agents using force in international and non-international armed conflicts).

\(^{50}\) Alston (n 46) 325–26.

\(^{51}\) For an extensive overview of transparency and accountability problems associated with CIA operations see Alston, ibid 352–406.
Of course, the enhanced capacity to deny the very occurrence of an attack entails grim consequences for the principle of accountability. However, it is reasonable that, in the vast majority of cases, since attacks do not usually take place outside a widely known political context, it would be rather easy to make a prima facie case for the attribution of an attack to a certain state. Moreover, critiques of this order still do not address inherent characteristics of drones themselves, but rather the potential for abuse that emanate from their use. While this is indeed a valid transparency challenge, the argument fails to note that – as mentioned above – this transparency deficit can be offset by the transparency advantages that advanced technology might bring, if properly harnessed for the purpose of increasing accountability.

The lack of attention to the transparency potential of advanced technology is easily exemplified also in discussions that go beyond institutional concerns. Indeed, the increasing use of drones for targeting individuals has been criticised on both the *jus ad bellum* and *jus in bello* levels. In the latter context, most of the discussion concerns the effects such weapons may have over the application of the IHL principles of distinction and proportionality, and the right to life under IHRL. Thus, it has been claimed that drone attacks result in indiscriminate killings of civilians; that they make killing without risk too easy, thereby leading to trigger-happy behaviour; that their ease of deployment can result in the targeting of protected persons not directly participating in hostilities at the time, rather than capturing them; that, regardless of their high-tech nature, they still require human intelligence, which is often unverifiable and can lead to tragic results; and that they might induce a ‘video game’ mentality to killing, which erodes the considerations of humanity that lie in the core of IHL.

Similarly – and this is perhaps more surprising – proponents of the use of drones also seldom mention their potential transparency-enhancing capabilities. They highlight, for instance, the enhanced precision of drones and their intelligence-enhancing surveillance capacities; the ability of operators to avoid hasty decisions, relieved from the stress of combat; and their overall potential to minimise erroneous targeting and collateral damage, which results from all of the above. In general, supporters deny that drones present significant and independent challenges to the application of the basic principles of IHL – challenges that do not arise from the operation of other, traditional, weapon systems.

---


53 For a discussion on both realms, see Schmitt (n 49).

54 Alston (n 6) para 79.

55 ibid para 80.

56 See Anderson Testimony I (n 48) para 21 (presenting this critique as one which has to be addressed by the US).

57 Alston (n 6) paras 81–83.

58 ibid para 84.

59 Intelligence, as distinguished from transparency, although these capabilities go hand in hand.


61 Schmitt (n 49) 321–23.
The fact is, however, that the use of high-tech weapons can serve to increase transparency and accountability, chiefly because they create evidence. Indeed, the monitoring capabilities possessed by modern military forces and intelligence agencies are staggering. Drones, for instance, whether armed or unarmed, collect high-quality information through their intelligence, surveillance and reconnaissance functions. They provide real-time, visual information regarding the target area and the targeted individuals before, during and after the attack – information that is undoubtedly kept and filed by the attacking state. While attack drones have been in the forefront of the discussion, other advanced capacities are also available to states, whether on the micro-tactical or strategic levels. For instance, micro-drones, some even launched by hand, can be used by ground forces for tactical intelligence purposes. Moreover, some tactical land systems integrate individual soldiers into an information network, allowing them to send and receive real-time data and transmit images.

On the other side of the spectrum, modern satellites can provide high-resolution imaging day and night and in any weather. These capabilities, and others, mean that states possess imagery not only regarding targeted killing operations conducted through drones, but also regarding other operations – including, but not limited to – so-called kill/capture operations conducted by land forces. The killing of Osama bin Laden, viewed ‘live’ in Washington by American officials, is just one noteworthy example.

However, two qualifications should be addressed. First, and notwithstanding their transparency-enhancing potential, any linkage between the availability of high-technology weapons and transparency obligations might give rise to various disincentives. Indeed, it is arguable that increased obligations could inhibit states from developing or using advanced weapons – including of the type that can otherwise minimise collateral damage, or, in our context, from acquiring and keeping monitoring information recorded by such capabilities. Nevertheless, upon closer look, these concerns do not seem to pose a substantial challenge. Since they reap significant operational benefits from their use – benefits that greatly overshadow any potential increased legal liability – it is highly unlikely that states will cease the production or deployment of advanced weapons. The same logic implies that states will also not be quick to destroy monitoring information that they possess, as such information serves to form a valuable intelligence

---

\[\text{62 ibid 313–15.} \]
\[\text{65 For instance, synthetic aperture radars (SAR) satellites, such as Israel’s TecSar, are based on radar rather than optical imaging: see Israel Aerospace Industries, ‘TecSar’, http://www.iai.co.il/35083-39439-en/BusinessAreas_SpaceSystems_ObservationSatellites.aspx?btl=1.} \]
\[\text{66 On kill/capture missions, see Alston (n 46) 333–41.} \]
\[\text{68 For an in-depth discussion of the possibility of increased obligations imposed on ‘stronger’ states in IHL – such as, perhaps, those in possession of monitoring information – see Gabriella Blum, ‘On a Differential Law of War’ (2011) 52 Harvard Journal of International Law 164.} \]
\[\text{69 cf Jean-François Quéguiner, ‘Precautions Under the Law Governing the Conduct of Hostilities’ (2008) 88 International Review of the Red Cross 796, 802.} \]
and operational database. Without exhausting this interesting question, there are ample grounds
to argue that if in a given instance a state chooses to do so nonetheless, it could be liable, in what-
ever forum, under some notion of evidential damage.70

Second, it is arguable that nowadays, as a result of the proliferation of popular technology
such as smartphones, states will never be in unique control of high-quality information.
Indeed, a blogger with an iPhone can create, record and disseminate information in a manner
unimaginable in the past. Thus, except in extremely closed environments, current technology
also allows individuals to accrue monitoring information. However, such information will rarely
match the quality, completeness, coherence and relevancy of monitoring information held by
states, especially when the latter have the initiative, as will frequently be the case in asymmetric
warfare. Therefore, the unique collection capacities of states still stand out.

We should bear this new reality in mind when discussing the increasing pressure on states to
disclose information.

4. INCREASING CALLS FOR DISCLOSURE OF INFORMATION: THE CASE OF
TARGETED KILLINGS

4.1 LEGAL AND FACTUAL DISCLOSURE AND NATIONAL SECURITY INTERESTS

Demands for disclosure can consist of calls to disclose the general or specific legal basis for the
operation, the factual circumstances of specific events, or both. While disclosure of a legal basis
is required in order to effectively challenge or justify policies or actions, the disclosure of factual
information is a precondition for the assessment of the application of the legal framework in a
specific instance. The duty of legal disclosure is not our main concern, although it raises interest-
ing jurisprudential questions regarding the obligations of states as lawmakers in the inter-
national system.

However, the discussion of legal disclosure in a relatively thorough manner is still of impor-
tance in our context. First, while the two types of disclosure are distinct, they might, in certain
respects, intertwine. For instance, there is little benefit in the disclosure of factual information
without any corresponding legal basis, especially when addressing hard cases such as alleged
violations of proportionality in IHL. In such cases, it is difficult to determine, for example,
whether an expected military advantage, to be balanced against incidental harm to civilians, is
part of the legal or factual framework of the case. Second, the issue of legal disclosure exempli-
fies the increasing disclosure expectations of various actors, from which we can draw conclusions
concerning their future demands. And third, as we shall see, significant disclosure gaps exist not
only concerning disclosure of the factual basis, but also regarding the legal basis for actions.
From the reluctance of states to release the legal basis for actions we can reasonably infer, a

70 See Ariel Porat and Alex Stein, ‘Liability for Uncertainty: Making Evidential Damage Actionable’ (1997) 18
Cardozo Law Review 1891, 1895. I am grateful to Eyal Benvenisti for pointing out this possibility.
fortiori, the barriers that exist regarding factual disclosure as well – including the disclosure of monitoring information.

In any case, while disclosure of the legal basis does not seem to conflict significantly with core considerations of national security – and therefore refusal to disclose is harder to justify\(^{71}\) – factual disclosure, as we have seen, might indeed give rise to weightier national security concerns, and thus any respective disclosure obligations should be balanced accordingly. However, it must be stressed that not every factual disclosure – even pertaining to monitoring data – gives rise to substantial security concerns, especially when balanced against the potential benefits of disclosure; otherwise, states would have refrained from releasing monitoring information even when it served their public relations interests, which is evidently not the case.\(^{72}\) Since the fact that states possess monitoring capabilities is widely known in the public sphere – indeed, states themselves admit it – a claim that any disclosure will expose classified capabilities should be taken with a grain of salt.\(^{73}\)

4.2 INCREASING CALLS FOR DISCLOSURE

With the increase in US drone operations since 2008, states have come under growing pressure to disclose legal and factual information regarding their actions. While these demands – which generally stem from concerns of transparency and accountability – have so far referred to monitoring information rather peripherally, they invoke similar concerns and interact with the same normative structure that would be featured in any future robust debate regarding the disclosure of monitoring information. As such, they are of much value to our analysis.

Thus, the issue of legal disclosure was predominant in the 2010 House of Representatives hearings on drone attacks, even in the statements of those who in general support US policy in this regard. Kenneth Anderson, in his testimony, placed major emphasis on the lack of legal disclosure regarding the use of drones,\(^{74}\) labelling the US administration’s silence in this context a ‘breath-taking’ failure.\(^{75}\) Similarly, many of the conclusions of the 2010 Study on Targeted Killings, conducted by UN Rapporteur Philip Alston, concerned disclosure. The study alleged that the failure of several states\(^{76}\) to disclose both their legal basis for targeted killings at large, as well as the legal and factual basis for specific operations, amounted to a breach of the principles of transparency and accountability as entrenched in IHL and IHRL.\(^{77}\) It noted that

72 See Beard (n 2), at 420–21 (exemplifying this practice); for a contemporary example, see Israel Defense Forces, ‘Terrorists Launch Grad Missiles into Israel’ (YouTube, 23 August 2011), http://www.youtube.com/watch?v=uMUVWjoAzR4.
73 Of course, states could always claim that, while monitoring capabilities are admitted in general, these capabilities are constantly improving and thus cannot be exposed. However, this seems a rather weak argument when posed in the face of allegations of serious violations.
74 Anderson Testimony I (n 48) paras 3, 27–30.
75 ibid para 28.
76 Alston (n 6) paras 13–26.
77 ibid paras 87–91.
absent disclosure, ‘[i]t is not possible for the international community to verify the legality of a killing’. The study emphasised also the role of civil society in making such assessments. The Rapporteur concluded, thus, that states should publicly identify, inter alia, the legal basis for targeted killings, the legal basis for a specific operation, and the measures taken after every such killing to ensure that the legal and factual analyses pertaining to the operation were accurate.

Furthermore, following specific operations – for instance, with regard to the killing of bin Laden – leading human rights groups have called for the disclosure of information. Human Rights Watch demanded that the US administration ‘provide all the relevant facts about Osama bin Laden’s death to clarify whether it was justified under international law’. Similarly, Amnesty International requested that the US and Pakistan ‘clarify aspects of the operation in Abbottabad in which Osama bin Laden was killed’. Similar demands for disclosure of legal and factual bases were made by Amnesty International following a rare public confirmation by President Obama, in early 2012, that drones were indeed being used to target suspected militants in Pakistan. As we shall see, the American Civil Liberties Union and other groups initiated domestic legal proceedings to that effect.

Perhaps attempting to address these claims, the US took some steps towards legal disclosure in a series of speeches delivered by senior officials in 2010–12. The most detailed of these, as of June 2012, were the remarks of counterterrorism assistant John Brennan, in which the Administration first formally admitted the existence of a drone-based targeted killings programme. Without delving into their nuances, all speeches gave assurances that the US adheres to international law, that its targetting operations are conducted within some framework of the law of armed conflict, and that decisions are subjected to meticulous review. However, while clarifying to some extent the jus ad bellum rationale behind US actions, and emphasising the

78 ibid para 92.  
79 ibid para 91.  
80 ibid para 93.  
85 Albeit not mentioning the CIA: Brennan (n 60).  
implementation of the principles of distinction, proportionality and humanity, the speeches refrained from setting out comprehensive theories with regard to these terms or the principle of accountability. Nor did the speeches provide substantial factual information regarding the strikes. As such, they are unlikely to satisfy the proponents of increased disclosure and international scrutiny, who are in turn poised to continue to challenge governments on this issue. Should relevant circumstances arise, it is reasonable that such challenges – based on the same rationales – will also be brought, with increased vigour, with regard to the disclosure of monitoring information.

5. DISCLOSURE TO CIVIL SOCIETY

5.1 DOMESTIC FREEDOM OF INFORMATION ACTS AND INTERNAL BARRIERS

As illustrated above, among those calling for disclosure, NGOs are playing a central part, in line with their increasing role in the promotion of state compliance. In most cases, when NGOs, as agents of civil society, demand disclosure of the legal or factual basis of operations, they are demanding public disclosure.

A source of growing importance for such obligations can be found in domestic rights of freedom of information (FOI). FOI often gives rise to positive rights to receive information held by public authorities, implemented through freedom of information acts (FOIAs). Specific rights to receive certain kinds of information can be entrenched in specialised legislation – such as, for instance, in the case of crime victims’ rights to participation. In other cases, such rights can be constructed by courts as inherent in certain contexts. FOIAs, however, are the most accessible method available to national and international NGOs seeking disclosure – since they usually constitute a general and relatively simple instrument for disclosure, and do not impose strict standing limitations.

Indeed, here we are venturing into questions of domestic law; however, discussing the competing interests at stake in domestic FOIA proceedings – and especially in those states in which the use of advanced weapons has been most pertinent – can inform also our analysis of international problems associated with the issue. It can further serve to delineate the balance required in the formulation of any emerging international positive FOI right. Importantly, the discussion

87 cf Alston (n 6) para 22.
90 Alston (n 46) 402.
91 In Canada, for instance, see Corrections and Conditional Release Act (1992) (Canada), s 142(1).
92 For instance, in Israel, non-statutory, internal administrative instructions that have a bearing over individuals’ rights are required by the courts to be effectively publicised: see HCJ 3930/94 Jazmawi v Minister of Health 1994 PD 48(4) 778.
demonstrates the general disclosure-inhibiting characteristics that are prevalent in domestic legislation, which may give rise to increased interest in international regulation, in cases where suspected violations of international law are concerned.

As we shall see, domestic FOI rights have not been, so far, extremely effective in the promotion of disclosure regarding all aspects of the use of high-technology weapons, and notably in the context of targeted killings. Some states lack FOIAs to begin with.\textsuperscript{93} Some have FOIAs, the effectiveness of which is yet unproven. In other states, such as Israel and the UK, FOIAs exclude certain security agencies.\textsuperscript{94} The American FOIA,\textsuperscript{95} conversely, does not manifestly exempt security agencies as such; however, it still allows wide leeway for withholding information. Several US FOIA proceedings, concerning targeted killings, exemplify this trend and might hint at the outcome of future monitoring information disclosure proceedings.

In January 2010, the American Civil Liberties Union (ACLU) submitted a request to several federal agencies, pursuant to the federal FOIA, seeking the disclosure of records pertaining to the use of drones in targeted killing operations.\textsuperscript{96} The request stressed\textsuperscript{97} that

the parameters of the program and the legal basis for using drones to execute targeted killings remain almost entirely obscure. It is unclear who may be targeted … how targets are selected … how civilian casualties are minimized … The public also has little information about any internal accountability mechanisms … Nor does the public have reliable information about who has been killed, how many civilians have been killed, and how this information is verified, if at all.

In March 2010, after having its FOIA request denied, the ACLU sought injunctive relief.\textsuperscript{98} The CIA,\textsuperscript{99} in particular, asserted that the \textit{existence or nonexistence} of the requested records is classified, relying thus on a wide interpretation of the national security exemptions provided for in the FOIA.\textsuperscript{100} This means that, not only were the requested records themselves deemed to be classified, but also the \textit{very fact} of their existence or non-existence.

This type of response to FOIA requests – known as the ‘Glomar response’ after a 1976 case involving a ship of that name\textsuperscript{101} – has been invoked by the CIA with increasing

\textsuperscript{94} Freedom of Information Act, 1998 (Israel), s 14(a) (Israeli FOIA); Freedom of Information Act 2000 (UK), s 23.
\textsuperscript{95} 5 USC § 552.
\textsuperscript{97} ibid 5.
\textsuperscript{98} ACLU, ‘Complaint for Injunctive Relief’ (16 March 2010), http://www.aclu.org/national-security/aclu-v-doj-et-al-complaint (ACLU Complaint II).
\textsuperscript{99} Added later as a defendant: \textit{ACLU v Department of Justice}, Civil Action No 10-0436 (RMC) 2011 WL 4005324 (DDC) 1.
\textsuperscript{100} ACLU Complaint II (n 98) para 25. Exemption b(1) excludes the disclosure of matters established by an Executive order to be kept secret in the interest of national defense or foreign policy; b(3) refers to exemptions provided by specific legislation.
\textsuperscript{101} \textit{Phillippi v CIA} 546 F2d 1009 (DC 1976). For a discussion of the origins of the Glomar response see Nathan Freed Wessler, “We Can Neither Confirm Nor Deny the Existence or Nonexistence of Records Responsive to
frequency,\textsuperscript{102} while enjoying significant judicial deference.\textsuperscript{103} This has been particularly the case in recent FOIA proceedings relating to targeted killings.\textsuperscript{104} Glomar responses, while at times necessary, effectively block further public and legal debate, since they do not allow the substantive critique of a decision to disclose or to withhold a specific record, or type of records, after the latter are acknowledged to exist. Their overuse can curtail the constructive development of a forward-looking balance between disclosure and national security concerns, by practically giving the latter interest an absolute, peremptory value.\textsuperscript{105} They are especially problematic when available information raises the preliminary concern that a government agency has acted in contravention of domestic or international law.\textsuperscript{106}

Glomar responses have some merit where even the involvement of a government or a specific agency in certain actions cannot be confirmed or denied without harming security interests\textsuperscript{107} – that is, in cases where the answer to the FOIA inquiry would itself ‘cause harm cognizable under an FOIA exception’.\textsuperscript{108} However, they make little sense where there is no serious denial regarding the existence of certain activities, such as American drone operations, conducted by the CIA or otherwise.\textsuperscript{109} Yet, US case law requires that, in order to negate the possibility of a Glomar response, such previous acknowledgement must be specific and official.\textsuperscript{110}

To a large extent, then, the question of previous acknowledgement was at the core of the ACLU’s FOIA action. In its September 2011 ruling, the DC District Court upheld the CIA’s Glomar response, and rejected the ACLU’s claim that the involvement of the CIA in drone attacks had previously been admitted. It decided, therefore, that even confirmation or denial of the existence of records could jeopardise national security.\textsuperscript{111} However, the court went a step further, in a manner that could have had a direct bearing over the question of disclosing

\textsuperscript{102} Alston (n 46) 403.
\textsuperscript{103} Wessler (n 101) 1394–95.
\textsuperscript{104} As of the date of writing this article, at least two other major disclosure requests have received the Glomar response. In December 2011, \textit{The New York Times} filed an FOIA-based lawsuit against the US Department of Justice (DoJ), after having its FOIA requests denied by the DoJ. The lawsuit demands the disclosure of the legal memoranda that serves the basis for targeted killing operations, and particularly the targeting of US citizens in such operations. In this case, too, the DoJ claimed, concerning parts of the request, that the material is classified and privileged, and issued a Glomar response towards other aspects of the request: See ‘Complaint Against United States Department of Justice’ (\textit{The New York Times}, 20 December 2011, paras 39–40, 46), http://www.medialaw.org/Content/NavigationMenu/ Publications1/MLRC_MediaLawDaily/Attachments3/times_v_state_dept_complaint.pdf. The ACLU, in further litigation pursued after the targeting of US citizens, filed another FOIA lawsuit, in February 2012. It explicitly demanded the disclosure of the legal and factual basis of the targeted killing programme, and specifically regarding the targeting of US citizens. The CIA and DoJ issued, once again, a Glomar response: see ACLU, ‘Complaint for Injunctive Relief’ (1 February 2012, paras 30–46), http://www.aclu.org/ files/assets/tk_foia_complaint.pdf.
\textsuperscript{105} cf Wessler (n 101) 1397–98, 1403–06.
\textsuperscript{106} ibid 1408.
\textsuperscript{107} See example in Wessler, ibid 1389–90.
\textsuperscript{108} \textit{Gardels v CIA} 689 F2d 1100, 1103 (DC 1982); see also \textit{ACLU v DoJ} (n 99) 5–6.
\textsuperscript{109} For a similar claim, see Wessler (n 101) 1396–98.
\textsuperscript{110} \textit{ACLU v DoJ} (n 99) 13.
\textsuperscript{111} ibid 9–14.
monitoring information: it held, in obiter dictum, that even if it had recognised that the CIA officially admitted that it had been involved in drone attacks, the CIA could still have issued a Glomar response, unless it had also previously and officially admitted that records on drone strikes existed. This dictum is rather perplexing, since it is certain that agencies indeed keep records of their actions; this is particularly true when drones are used, since the relevant agencies record each operation and it is highly reasonable that these records are kept. Thus, once the involvement of an agency in targeted killings is not under serious dispute, the lack of disclosure regarding the existence of records – including monitoring information – seems curious. Accordingly, it makes sense that if the CIA involvement had been deemed to have been publicly admitted, the existence of at least some monitoring information must be understood to have been implied in such an admission.

Indeed, it would be inconceivable to issue a Glomar response regarding the existence of records in circumstances such as those, for instance, of the bin Laden operation, when pictures of officials following the operation in real time have already been disseminated in the media. It seems that it was for these reasons that the CIA refrained from issuing a Glomar response when requested by a US NGO to disclose factual information – including monitoring information – regarding the operation. The CIA located 52 relevant records which it refused to disclose under FOIA exemptions. Since it could not reasonably issue a Glomar response, the CIA had to substantively justify its decision to withhold the requested information. It thus argued that the records pertained to military plans, systems or operations, intelligence sources and methods, and foreign relations or activities, and that their disclosure would inflame tensions and lead to retaliatory attacks. In an April 2012 memorandum opinion, the DC District Court reiterated the ‘low hurdles’ of reasonableness, good faith, specificity and plausibility required in order to justify national security exemptions, and thus deferred to the CIA’s discretion. In doing so, the Court refrained from analysing each record’s specific implication for national security, but concluded generally that all records might have such effects.

FOIA battles over facts pertaining to alleged violations of international law are not unique to the US context or to the question of targeted killings. Moreover, they can sometimes involve the interests of third states. It is worth mentioning one Israeli case which, although not concerned with an armed conflict, deals directly with monitoring information in contentious international circumstances, with a bearing on issues of IHRL. In August 2007, an Israeli television channel reported – according to information it received from IDF reservists – that Israeli soldiers had spotted three persons, perhaps asylum seekers, attempting to cross the border between Egypt

---

112 ibid 13.
113 *Judicial Watch v DoD* CA11-980 (DC 2012) 1.
114 ibid 1–2, 5 (the CIA relied on FOIA exemptions 1 and 3).
115 ibid 21 (pursuant to § 1.4 of Executive Order 13526, classification of material must pertain to one of eight categories of information; in addition, it is required that disclosure could be reasonably expected to result in describable damage to national security).
116 ibid.
117 ibid 35.
118 ibid 35–36.
and Israel under cover of darkness. Following the launch of illumination rounds from the Israeli side, Egyptian forces rushed to the scene and, according to the Israeli troops, lethally shot one of the persons and injured another. The third managed to reach the border fence, where Israeli soldiers apparently attempted to pull him into Israel as Egyptian officers managed to pull him back onto Egyptian territory. The Israeli soldiers alleged that thereafter Egyptian officers proceeded to kill the individuals.\footnote{119} If found true, the allegations would undoubtedly constitute breaches of IHRL.

Israeli NGOs learned that the dramatic scene was filmed by military video cameras deployed on the border, and accordingly – after having their disclosure requests refused – filed an FOIA petition against the relevant authorities. While the authorities did not deny that the video existed, they refused disclosure, relying on the Israeli FOIA’s national security and foreign relations exemptions.\footnote{120} Interestingly, the authorities argued that ‘Egypt might regard the disclosure of such materials as taking a diplomatic stance against it’.\footnote{121} The Tel-Aviv Administrative Court accepted the state’s national security claims after reviewing them in camera, without ruling on the foreign relations claims.\footnote{122} The Israeli authorities’ justifications were thus based, to a large extent, not on ‘direct’ Israeli interests but rather on the reluctance to embarrass Egypt, which could in turn indirectly affect Israel, in view of the complex relations between the two states. While such concerns cannot be downplayed, there is danger in expanding the term ‘national security’ to encompass ambiguous threats, which essentially amount to indirect political interests.

From an international perspective, this is especially true where suspected violations of international law occur. The question whether states can be expected to act otherwise, when the issue is debated strictly on the bilateral level – and thus spawns considerable inter-state pressure – is indeed worthy of serious consideration. International regulation of the issue can perhaps alleviate this pressure, in similar circumstances, by extracting the question from the bilateral realm.

In sum, whatever will be ruled in ongoing FOIA litigation,\footnote{123} the discussion above exemplifies the existing barriers not only to disclosure of factual details regarding specific operations, but also regarding the general legal basis for state action. Bearing this in mind, it seems highly unlikely that the domestic FOIA route will actually bring about the disclosure of the factual basis of a specific action, much less the disclosure of monitoring information – even, should the case arise, when violations of international law are concerned.\footnote{124}

\footnote{119} AdminC (TA) 2320/07 The Movement for Freedom of Information and Another v Chief of Staff of the IDF and Others, Petition under the Freedom of Information Act, 1998 (undated 2007) (in Hebrew, on file with author) (FOIA Petition).
\footnote{120} ibid paras 14–15; Israeli FOIA (n 94) s 9(a)(1).
\footnote{121} FOIA Petition (n 119) para 14.
\footnote{123} Wessler (n 101) 1394–95.
\footnote{124} See also Alston (n 46) 404 (‘The bottom line is that civil society groups, confronted with the systematic application of such freedom of information restrictions … have little prospect of being able to obtain meaningful information about extraterritorial targeted killings activities’).
5.2 TOWARDS AN INTERNATIONAL POSITIVE RIGHT TO RECEIVE INFORMATION: HUMAN RIGHTS LAW AND GLOBAL ADMINISTRATIVE LAW

As demonstrated above, domestic FOIAs are not likely to be effective in relation to the disclosure of monitoring information. Practices such as the Glomar response may allow states to curtail, through domestic law, the principle of transparency – with regard to both legal and factual information – and thus, in turn, also the assessment of the fulfilment of their international obligations, including the duty to investigate alleged violations. Since the consequences of forcible acts are at the core of international concern, it seems that the question of disclosure cannot be confined strictly to the domestic sphere. It only makes sense, therefore, that the question of freedom of information should be addressed also at the international level.125

The right to ‘seek, receive and impart information’ is entrenched in Article 19(2) of the ICCPR, as part of the right of freedom of expression, and can be restricted only by law when such restrictions are necessary, inter alia, for the protection of national security.126 A parallel right to ‘receive and impart information and ideas without interference by public authority’ is entrenched in the European Convention on Human Rights (ECHR).127 As is evident from the text of the ECHR (‘without interference’), the right to information in international law was traditionally understood as relating to negative aspects such as freedom of the press, including the ‘right to listen’ to transnational broadcasting.128 Accordingly, in its first General Comment on Article 19, the Human Rights Committee did not elaborate on the positive aspect of freedom of expression.129

Recently, however, in its September 2011 General Comment 34 (GC 34), the Committee clarified that the right to receive information, as entrenched in Article 19(2) of the ICCPR, applies positively to public bodies, regardless of its form or source. Furthermore, the Committee called upon states, for the first time, to enact freedom of information legislation in order to ensure ‘easy, prompt, effective and practical access’ to information.130 The Committee thereby opened the door for substantive international scrutiny of domestic FOIA balancing.

GC 34 recognises that the right to receive information is not absolute; however, the Committee stressed that restriction of the right must fulfil the necessity condition, and that ‘the relation between right and restriction and between norm and exception must not be

125 ibid 318, 432.
126 ICCPR (n 7) art 19(2)–(3).
130 GC 34 (n 9) paras 18–19; see also United Nations Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media and OAS Special Rapporteur on Freedom of Expression, ‘International Mechanisms for Promoting Freedom of Expression, Joint Declaration’ (6 December 2004), http://www.osce.org/fom/38632 (declaring that the right to access information is a ‘fundamental human right’ and setting forth principles for its implementation).
reversed’\textsuperscript{131} by withholding from the public ‘information of legitimate public interest that does not harm national security’.\textsuperscript{132} Furthermore, it stressed that any legal restriction of access to information must be \textit{proportional}: that is, it must be (i) appropriate to achieve the restriction’s protective function; (ii) the least intrusive instrument capable of achieving that function; and (iii) proportionate to the protected interest. Importantly, the Committee posited that the restricting state bears the burden of demonstrating in a specific fashion the nature of the threat, the necessity and proportionality of the restriction, and the direct and immediate connection between the restriction and the threat (\textit{specificity}).\textsuperscript{133} The Committee thus outlined a general international framework for balancing between the positive right to receive information and national security interests, centred on the concepts of necessity, proportionality and specificity.

From GC 34 four main conclusions can be drawn. First, in the near future states will be expected by ICCPR treaty bodies to report on their FOIA practices – a fact that can be used by NGOs to increase disclosure pressures, through the submission of ‘shadow’ reports to IHRL bodies.\textsuperscript{134} Second, it is reasonable that the emerging positive right to receive information will trickle to other human rights bodies, when facing potential disclosure claims. Third – and significant in our context – the approach of GC 34 can arguably influence the transparency standard required in investigations under IHRL, and also – considering the increasing convergence of these bodies – under IHL. In fact, when the issue is alleged violations of law, it seems that the public interest in disclosure will be much stronger. Fourth, it is possible that current FOIA disclosure practices, as surveyed in the previous section, might not satisfy the emerging understanding of the right to access information under IHRL, especially when a duty to investigate materialises.

For instance, blanket exclusions of security agencies from FOIAs may be considered to be too broad and, instead, states could be required to analyse each request according to its merits. Moreover, it is doubtful whether broad use of the Glomar response would satisfy the necessity, proportionality and specificity conditions as set out in GC 34. With regard to the disclosure of factual information – including monitoring information – this seems to be particularly true when three conditions materialise: (i) when there is sufficient public knowledge, at a reasonable level, that the state or its agencies were involved in the action; (ii) when the disclosure is requested with regard to monitoring capabilities that are already widely known to be possessed by the state; and (iii) these conditions are fortified where suspected violations of international law are at hand. In such cases, the mere possession of monitoring information cannot be denied; and, accordingly, the request for disclosure should be assessed on its merits – again, according to the aforementioned principles of necessity, proportionality and specificity. For instance, if a particular piece of media has the potential to reveal sensitive information, selective or partial

\textsuperscript{131} GC 34 (n 9) para 21.
\textsuperscript{132} ibid para 30.
\textsuperscript{133} ibid paras 34–35.
non-disclosure would be more in conformity with the proportionality principle than complete non-disclosure.

On the theoretical level, the emerging international positive right to freedom of information can be informed, perhaps, with principles derived from the sphere of global administrative law (GAL). While not a unified body of law, GAL condones the application of traditional principles of domestic administrative law – such as reasonableness, proportionality, reasoned decisions and transparency – also to global governance.\textsuperscript{135} Importantly, since GAL is a general concept, not tied to a single body of treaties, it can serve as a general guideline to assess state behaviour in many instances. GAL thus attributes administrative characteristics – and corresponding obligations – to a wide range of bodies, including ‘national regulatory bodies operating with reference to an international intergovernmental regime’.\textsuperscript{136} Broadly within this category one can include national authorities that are obliged to investigate violations of international norms, especially when their actions – such as withholding information – adversely affect others, whether states, organisations or individuals.\textsuperscript{137} Furthermore, balancing competing interests is an integral part of administrative law thinking.\textsuperscript{138} The GAL standard of proportionality,\textsuperscript{139} for instance, can enhance and interact with the corresponding standards in the context of disclosure, as set out in GC 34.

As we shall see, these emerging principles can perhaps guide us in analysing disclosure obligations – or rather the implications of non-disclosure – in relation to other mechanisms of international law, such as international tribunals.

6. Monitoring Information and International Criminal Proceedings

6.1 Complementarity, Transparency and Superior Access

Until now, I have discussed potential sources for disclosure to the public. In the following sections, the question of disclosure with regard to select international bodies will be addressed. Among these, I will focus on the disclosure of monitoring information in international criminal proceedings, since in this context the emerging positive right to receive information can perhaps play a significant role.\textsuperscript{140} In general, as with regard to FOI, exemptions from disclosure to international bodies may be justified on grounds of national security; accordingly, our treatment of such exemptions can be informed by corresponding IHRL or GAL standards.

\textsuperscript{135} See Kingsbury, Krisch and Stewart (n 14); see also Eyal Benvenisti, ‘The Interplay Between Actors as a Determinant of the Evolution of Administrative Law in International Institutions’ (2005) 68 Law and Contemporary Problems 319, 319 (2005).

\textsuperscript{136} Kingsbury, Krisch and Stewart (n 14) 17.

\textsuperscript{137} ibid 16–17, 21–22.

\textsuperscript{138} ibid 17.

\textsuperscript{139} ibid 40–41.

\textsuperscript{140} The discussion in this section should not be understood as applying specifically to states or cases mentioned in earlier sections. This is partly because some of these states are not parties to the ICC Statute, but mostly because our discussion here is forward-looking and normative.
Can refusal to disclose monitoring information affect international criminal proceedings? On the face of it, the answer is negative. Since criminal proceedings concern individuals, they involve the presumption of innocence.\textsuperscript{141} In the ICC, as in any criminal court, the onus is on the prosecutor to prove the guilt of the accused.\textsuperscript{142} In addition, the ICC Statute precludes any reversal of the burden of proof or onus of rebuttal.\textsuperscript{143} Thus, even if the accused has access to monitoring information acquired by the state – in itself not an obvious possibility – he or she will not be required to disclose it.

However, since in international criminal proceedings state parties are indirect ‘third’ actors,\textsuperscript{144} disclosure obligations can still play a part. One aspect refers to the admissibility of the case – through the principle of complementarity. The principle, as entrenched in Article 17(1)(a)–(b) of the ICC Statute, provides that if a state investigates or prosecutes a case (or investigates and decides not to prosecute) the case will be inadmissible before the ICC, unless the state is unwilling or unable to genuinely investigate the case.\textsuperscript{145} The complementarity principle thus serves to encourage states to fulfil their primary responsibility to investigate and prosecute alleged crimes, while reaffirming their sovereignty.\textsuperscript{146} While states enjoy a presumption, in this context, in favour of their domestic procedure, the presumption can be reversed where there are indications that the national process is not genuine\textsuperscript{147} – the general question being whether domestic procedure was used in order to unjustly exonerate the accused.\textsuperscript{148}

Let us return to the Basic Scenario (in Section 1 above). Assume that the state maintains its refusal to disclose the monitoring information, while not initiating an investigation, and the case finds its way to the ICC. Can the refusal contribute to the conclusion that the state is unwilling to genuinely investigate or prosecute the case? While a straightforward positive reply may very well be contentious, such a conclusion is still worth considering, at least in certain instances. To be sure, such a determination will require a complex analysis, which can perhaps be conducted only on a flexible case-by-case basis.\textsuperscript{149} In any such consideration, the exploration of the interaction between the principles of transparency and complementarity must play a key part.

Indeed, withholding monitoring information, in certain instances, can significantly reduce the transparency of the domestic procedure. Transparency is implied in Article 17(2)(c) of the ICC Statute, since absent at least some preliminary degree of transparency – and at least before the

\textsuperscript{141} ICC Statute (n 38).
\textsuperscript{142} ibid art 66(2).
\textsuperscript{143} ibid art 67(1)(i).
\textsuperscript{145} ICC Statute (n 38) art 17(1)(a).
\textsuperscript{147} The Principle of Complementarity, ibid para 3.
\textsuperscript{148} Benzing (n 146) 598.
\textsuperscript{149} The Principle of Complementarity (n 146) paras 33–42, 44–47, 51–52.
Court’s organs – it is impossible to verify that the domestic proceedings are being conducted ‘independently’ and ‘impartially,’ and with the genuine intent to bring the person to justice. Thereby, lack of transparency can affect, to varying extents, the scope of presumption in favour of the domestic procedure.\textsuperscript{150} This conclusion might be especially true when monitoring information is withheld, given that in such cases the state has ‘exclusive or superior access to the necessary information, and therefore is in the best position to know the state of affairs and provide evidence’.\textsuperscript{151}

In any case, the determination whether withholding monitoring information can affect ICC admissibility requires us to specify exactly what ‘type’ of transparency we are looking for. As discussed in Section 2.2, a difficult question concerns the level of investigative transparency required of the state, and whether these obligations are imposed in relation to the general public or rather only to national investigating authorities. There is a wide spectrum of possibilities and combinations in this context. Thus, a common, generally accepted practice of states is to conduct an investigation in which the investigating authorities have full access to all relevant information, but the source material – such as monitoring information – is not accessible to the public.\textsuperscript{152}

While, at large, complementarity determinations should be limited to the handling of a specific case,\textsuperscript{153} it seems that in such instances cautious inferences regarding the genuineness of the investigation can be made from the general context of the relevant domestic system, and whether it is deemed largely to be independent and impartial.\textsuperscript{154} When the system is generally so deemed, the absence of public disclosure cannot be expected to inform the complementarity assessment. Of course, when a generally non-independent system is involved, lack of public disclosure can perhaps be of more significance, notwithstanding the fact that the state claims that domestic investigating authorities had full access to source material.\textsuperscript{155}

‘Hybrid’ cases are also possible. For example, a system with generally independent institutions can conduct an investigation but, for some reason, decide to restrict the investigating entity, either through encroachment upon its independence, or through the placing of ad hoc limitations on its powers – inter alia, with respect to access to information. For instance, the mandate of the commission, nominated by the Israeli government to investigate the 2010 Gaza

\textsuperscript{150} cf ibid para 55 (addressing the shifting of the burden concerning questions of admissibility). Arguably, lack of transparency can be remedied, to some extent, during the preliminary process as outlined in the ICC Statute (n 38) art 18. See Benzing (n 146) 624–25.

\textsuperscript{151} The Principle of Complementarity (n 146) para 56 (referring to exclusive or superior access to information as a basis for shifting the burden of proof regarding the determination whether domestic procedures were ‘genuine’.)

\textsuperscript{152} This is possible, for instance, when independent Humanitarian Law Commissions are established, in a manner that balances between public scrutiny and required military secrecy. See Cohen and Shany (n 12) para 5.2. In some continental legal systems, notably in France, investigations are generally secret by default: Act No 2000-415 of 15 June 2000, Code of Criminal Procedure, art 11 (‘Except where the law provides otherwise and subject to the defendant’s rights, the inquiry and investigation proceedings are secret’).

\textsuperscript{153} cf Benzing (n 146) 603 (‘according to the wording of Article 17, the Court will always assess the situation in a state merely in relation to a specific case, rather than make a general and all-embracing examination of the system as such. Nevertheless … the Court will not simply notarise the exercise of jurisdiction by a state. They [the terms in the article] require a certain degree of scrutiny of the quality and standard of national proceedings’).

\textsuperscript{154} See The Principle of Complementarity (n 146) para 35.

\textsuperscript{155} ibid.
Flotilla incident, empowered it to receive all information – including monitoring information – that it saw fit from any governmental authority. However, the commission was not authorised to summon IDF troops that took part in the operation.\(^{156}\) Perhaps in such cases a judgment can be made with regard to the potential importance of the undisclosed material for the investigative process.\(^{157}\)

Be that as it may, the balance encompassed in the emerging international positive right to receive information can inform also the analysis of complementarity. For instance, the requirements of necessity, proportionality and specificity concerning legitimate restrictions of disclosure can influence the determination whether a state is willing to conduct a genuine investigation – in light, of course, of the general context of the specific legal system. These similarities notwithstanding, while non-disclosure to the general public, as discussed above – and assuming it corresponds with the aforementioned requirements – can be more easily justified in terms of national security, it seems less plausible that restrictions on access to information imposed on investigating authorities can survive the requirement of independence and impartiality as set out in the ICC Statute – assuming the withheld information is of significant importance for the effectiveness of the investigation.

### 6.2 Inference of Facts

The previous section discussed the issue of disclosure in the context of ICC admissibility. However, the issue can surface also during the ICC’s criminal proceedings and investigations themselves. The ICC Statute imposes a general obligation on states parties to cooperate with the Court in the investigation and prosecution of crimes.\(^{158}\) Accordingly, the Court is authorised to request the cooperation of states parties in general,\(^{159}\) and specifically regarding the provision of records and documents.\(^{160}\) Returning to our Basic Scenario, the Court can request the state to disclose the monitoring information that can vindicate or implicate those behind the drone attack. As provided for in Articles 72 and 93 of the ICC Statute, a state may deny such a request only on grounds of national security, and after it has considered whether acceptable conditional disclosure is possible.\(^{161}\)

Thus, embedded in the ICC Statute are the necessity and proportionality standards for the restriction of disclosure, reminiscent of those that are emerging under IHRL. Indeed, international criminal law and human rights law are increasingly perceived as seeking to defend similar values,\(^ {162}\) and it is therefore reasonable to interpret these requirements, as contained in both

---

\(^{156}\) Although it was authorised to hear the testimonies of top IDF commanders: see State of Israel, Government Decision No 1796, 14 June 2010 (in Hebrew), http://turkel-committee.gov.il/content-50.html.

\(^{157}\) Note that I refer to the Israeli commission only by way of example of an investigatory body with somewhat diminished powers, and do not otherwise pass judgment regarding its specific merits.

\(^{158}\) ICC Statute (n 38) art 86.

\(^{159}\) ibid art 87.

\(^{160}\) ibid art 93(i).

\(^{161}\) ibid arts 72, 93(4)–(5). For a survey of these articles, see Susan Rose-Ackerman and Benjamin Billa, ‘Treaties and National Security’ (2008) 40 New York University Journal of International Law and Politics 437, 475–79.

\(^{162}\) Seibert-Fohr (n 11) 3.
bodies of law, in a like manner. However, since the ICC Statute concerns disclosure during criminal proceedings, national security concerns might carry less weight than they do in relation to disclosure to the public: this is especially true since the ICC Statute provides special conditions for disclosure of sensitive data by, for instance, conducting *in camera* and *ex parte* proceedings.163

Nevertheless, if a state denies the Court’s request, and cooperative means of resolving the matter fail – means that are designed essentially to bring the refusal to disclose into conformity with proportionality and some requirement of specificity164 – the Court is authorised, inter alia, to conclude, in the circumstances of the case, that the state has violated its obligations under the Statute.165 Granted, the Court has no authority to order direct disclosure, as states were especially wary of granting it such power,166 available, for instance, to the ICTY.167 However, and significantly, as provided for in Article 72(7)(a)(iii), in such a case the Court is authorised to ‘make such inference in the trial of the accused as to the existence or non-existence of a fact, as may be appropriate in the circumstances’.168

While Article 72 is rather ambiguous,169 its plain language implies that a refusal by a state to disclose information can lead, potentially, to the inference of facts not only for the benefit, but also to the detriment of the accused individual.170 This power can serve as an incentive (or disincentive) for the state to disclose, depending on its interest in the specific case. When refusals by states pertain to high-quality, objective factual material that is found in monitoring information, and if a state vehemently refuses to any conditioned disclosure, the Court could be more inclined to use its powers under Article 72(7)(a)(iii). This outcome is not unproblematic, since it places accused persons at the mercy of states which may not regard their interests as a top priority. Essentially, then, the inherent weakness of the ICC in terms of its capacity to order states to disclose information171 shifts the risk of non-disclosure to the accused. Therefore, any factual

---

163 ICC Statute (n 38) art 72(5)(d). Experience shows that the Court will not be too reluctant to conduct such proceedings: see Alex Little, ‘Secrecy at the International Criminal Court’ (2010) 103 American Society of International Law Proceedings 232.

164 ICC Statute (n 38) art 72(6). However, specificity is not required if a ‘specific description of the reasons would itself necessarily result in such prejudice’ to national security.

165 ICC Statute (n 38) art 72(7)(a)(ii). In doing so, perhaps the Court will follow the balance between disclosure and national security concerns as set out by the ICTY in *Blaskić* (n 39) [61]–[69]; it should be noted, however, that the ICTY has power to positively order disclosure, which is largely lacking in the ICC Statute. See Knoops and Amsterdam (n 144) 276–77. For an in-depth analysis of national security concerns and the ICTY, see Laura Moranchek, ‘Protecting National Security Evidence while Prosecuting War Crimes: Problems and Lessons for International Justice from the ICTY’ (2006) 31 Yale Journal of International Law 477.


167 *Blaskić* (n 39) [61]–[69].

168 ICC Statute (n 38) art 72(7)(a)(iii).


171 See Knoops and Amsterdam (n 144) 276–77.
inference must be carefully tailored as to not impinge too gravely upon the rights of the accused, and has to take into consideration the specific constellation of interests between the accused and the withholding state.\footnote{On this dilemma, see Behrens (n 170) 125.}

7. **Monitoring Information and the Burden of Proof in International Litigation and Fact-Finding**

Finally, the question of disclosure can arise also in inter-state litigation. Just as in most domestic jurisdictions, it is a ‘well settled’ principle of international law that a party seeking to establish a fact bears the burden of proof.\footnote{Case Concerning Avena and Other Mexican Nationals (Mexico v United States of America) [2004] ICJ Rep 12 (Avena), [55]; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US), Jurisdiction and Admissibility, Judgment [1984] ICJ Rep 437, [101].} This burden is especially heavy when the claims are of ‘exceptional gravity’,\footnote{Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Yugoslavia (Serbia and Montenegro), Provisional Measures, Order of 13 September 1993 [1993] ICJ Rep 325, Separate Opinion of Judge Lauterpacht, [67].} such as can be expected when violations of IHL or IHLR are alleged. Article 49 of the ICJ Statute grants the Court the power to ‘call upon’ contesting states to ‘produce any document,’ and provides that ‘formal note shall be taken of any refusal’.\footnote{ibid [205].} Accordingly, Article 62(1) of the Rules of Court confers on the ICJ wide discretion to call upon parties to produce evidence.\footnote{ibid.} Should a party refuse to produce evidence requested by the Court, the latter may draw inferences from the party’s abstention.\footnote{ibid.} Moreover, in certain instances, a shift of the entire burden of proof is possible.\footnote{ibid [206].} However, the basic documents of the ICJ do not expressly address the question of disclosure and national security.

This issue arose in the **Bosnia Genocide** case, in which Serbia disclosed documents with blacked-out text, citing national security interests. Bosnia requested the Court to instruct Serbia to disclose ‘unredacted’ versions of the documents, and to draw conclusions from any refusal to do so.\footnote{ibid [206].} The Court denied the request to order full disclosure, but hinted that it is nevertheless ‘free to draw its own conclusions’.\footnote{ibid.} The Court seems to have based its decision on the fact that Bosnia had already ‘extensive documentation and other evidence available to it’ from previous ICTY proceedings.\footnote{ibid [206].} Such a case must be distinguished from situations
where the withholding state is in *exclusive* possession of high-quality evidence, such as can be found in monitoring information, and refuses even partial disclosure. Indeed, in the *Corfu Channel* case, the Court ruled that ‘exclusive control’ over evidence can give rise to ‘liberal recourse to inferences of fact’.

In light of the above, there is ample space to argue at least for an evidentiary rule, according to which, once a prima facie case has been made regarding alleged violations, a state might acquire the burden of producing monitoring information in its possession, in order to prove that it has acted lawfully. While this issue is rather underdeveloped in ICJ jurisprudence, it seems reasonable that when national security concerns are raised, they should be subject to the same necessity, proportionality and specificity requirements emerging in other contexts. Thus, a blanket refusal to disclose monitoring information – in light of its potential weight in the resolution of the case and the exclusive control of the state over the information – can result in the shifting of the burden of proof and to a resulting adverse inference to the detriment of the withholding state.

Without exhausting this issue, it is arguable that the same dynamics of factual inferences can develop also in international fact-finding. First, it should be noted that international fact-finding missions mandated to inquire into matters of state responsibility are not bound by the same standards of proof as are required under international criminal law, but rather with the more flexible standard of ‘balance of probabilities’.

Thus, even when a state cooperates, in general, with international commissions of inquiry, it can still incur obligations of proof. For instance, when forcible actions by states result in deaths of civilians, the burden of proof could shift to the detriment of the relevant state. Such dynamics are implied in the Report of the UN Secretary General’s Panel of Inquiry on the Gaza Flotilla Incident (the Palmer Report), commissioned to investigate, inter alia, the nine deaths in the course of the Israeli interception of the *Mavi Marmara*. The Panel, while finding lawful the maritime blockade imposed by Israel, concluded that ‘no satisfactory explanation has been provided to the Panel [by Israel] for how the individual deaths occurred’. The Panel thereby alluded to a heavy burden of proof incurred by states in such instances. Whether or not this was, in fact, the case concerning the Palmer Report, it makes sense that when states are in possession of monitoring information that can potentially vindicate them, and yet they refuse to disclose it to panels of inquiry without making a national security

---

182 *Corfu Channel (United Kingdom v Albania)*, Judgment [1949] ICJ Rep 18 (the Court here referred to exclusive control that is a product of ‘exclusive territorial control’ but the reasoning must apply to any case of such control). In *Avena* (n 173), the US claimed that the burden of *production* under international law should be on the party in exclusive control of the evidence; this claim was based on the distinction between burdens of proof and production. See, eg, Charles T McCormick, *Handbook on the Law of Evidence* (5th edn, West Publishing 1999) 342; *Microsoft v i4i*, 131 SCt 2238, 2245, n 4, (2011) (on this distinction). This distinction was not accepted as such by the ICJ, but this fact should be understood in light of the Court’s general authority to order parties to disclose evidence, which makes the question of the burden of production less acute: *Avena* (n 173) [56]–[57]. Thus, the logic of inference of facts when states refuse to disclose material under their exclusive control still stands.


claim that corresponds with the principles of necessity, proportionality and specificity, they can be deemed to have failed to lift this burden, and accordingly suffer adverse factual inferences.

8. CONCLUSION

The ever-increasing technological advances undoubtedly have the potential to augment the accountability of individuals and states in the face of alleged violations of IHL and IHRL, namely through transparency-enhancing data-collecting capabilities. These capabilities place states in unique positions to possess material of high-quality evidentiary value. In parallel, pressure to disclose information has been mounting, and will probably not cease in the near future. When states have faced such demands they have invoked, and will continue to do so, national security concerns. These concerns are legitimate. However, considering the public interest in disclosure that could arise where serious violations of IHL and IHRL are alleged, a blanket rule of non-disclosure seems to result in an unbalanced result in which security interests trump all others.

Domestic FOIAs do not seem to provide an effective remedy, since their provisions – and, perhaps more so, the interpretation of their exemptions – might not always result in a proper balance. For instance, they allow practices such as the Glomar response, not only concerning disclosure of factual information, but also regarding the legal basis for operations. This seems to be a skewed situation, considering the notion that questions of international import should not be quashed strictly by domestic mechanisms. Thus, as we have seen, an international positive right to receive information is emerging, which recognises restrictions on disclosure only if they adhere to standards of necessity, proportionality and specificity. This development can extract the question of disclosure from the domestic to the international level, and influence also our perception of the requirement of transparency in the context of the duty to investigate violations.

The question of disclosure of monitoring information can arise also in international criminal proceedings – in the context of both admissibility (complementarity) and inference of facts. With respect to complementarity, it is arguable that non-disclosure may, in certain situations, affect the perception of the domestic system as willing (or unwilling) to genuinely investigate offences. It might also result in the inference of facts in the proceedings themselves, giving due regard, however, to the rights of the accused.

Finally, the article has briefly touched upon the same dilemma that arises in inter-state litigation and fact-finding mechanisms, where inference of facts against the non-disclosing state is also possible, arguing that the same balancing principles should apply in this context.

At the end of the day, the issue of disclosure of monitoring information boils down to common sense, manifested in the reasonable balancing of the competing interests. It makes sense, for instance, that when states widely admit to be in possession of certain capabilities – and even

185 cf Alston (n 46) 318 (‘national insistence on the adequacy of domestic procedures can never be considered a substitute for the degree of transparency required to enable the international community to discharge its separate monitoring obligations’).
disclose monitoring information when it fits their interests – they cannot hide behind blanket national security claims when disclosure is requested by public or international bodies. This is especially so where suspicions of violations of international law have arisen. It is equally reasonable that instruments of international law – if the pursuit of the legal truth is of any relevance – cannot be completely barred from access to material of such potential significance, without any costs to the withholding state. These costs can be reflected at least in adverse inferences.

The duty to conduct effective investigation of alleged violations, enhanced by the emerging positive right to receive information – and the balancing standards it sets out – can thus be an important framework in which to discuss obligations to disclose monitoring information. In turn, these emerging norms can and should affect similar dilemmas that arise across a wide variety of international mechanisms.