Book Section:

Bellaby, R. orcid.org/0000-0002-6975-0681 (2021) Intelligence and the just war tradition : the need for a flexible ethical framework. In: Miller, S., Regan, M. and Walsh, P.F., (eds.) National Security Intelligence and Ethics. Taylor & Francis (Routledge) , Abingdon, Oxon , pp. 7-20. ISBN 9780367758318

https://doi.org/10.4324/9781003164197

1 Intelligence and the just war tradition

The need for a flexible ethical framework

Ross Bellaby

Introduction

It is impossible to think of one "just war doctrine", with a single point of lineal development from a single idea. Rather, "just war" is better thought of as a set of "recurrent issues and themes in the discussion of warfare . . . reflecting a general philosophical orientation towards the subject" (Clark 1988, 31) – a collection of underlying ethical arguments that have evolved over time in response to security challenges. As a broad body of thought the just war tradition "remains one of the most popular frameworks for evaluating the morality of war and warfare" (Fitzsimmons 2015, 1069);[1] influencing and becoming reflected in political rhetoric and legal cannon.[2] Indeed, many theorists have adapted the just war tradition to tackle emerging ethical-security problems of the day, from acts of terrorism and counter-terrorism policy,[3] drone warfare,[4] biosecurity,[5] private military companies[6] and civil wars.[7]

For intelligence the ethical dilemma faced includes recognizing and reconciling that it necessarily includes practices that "unavoidably entail doing something that is seriously contrary to the moral rules accepted as governing most human activity" (Quinlan 2007, 2) with the argument that without secret intelligence states cannot "understand sufficiently the nature of some important threats" (Omand 2007, 116). That on the one hand it can be argued that over the last century intelligence has become one of the most vital tools a political community has in providing timely information designed to serve and protect its members and, as such, represents an ethical good. While on the other hand, it can also be argued that secret intelligence often necessarily involves violating people's vital interest in privacy and autonomy and so there should be limits on its use. There is a need, therefore, for an ethical framework that can evaluate and reconcile these two tensions, offering both a limitation on the harm that is caused by intelligence collection, while also outlining exactly when this harm is justified. By establishing the criteria of just cause, legitimate authority, right intention, last resort, proportionality and discrimination, it can be argued that the harm intelligence can cause is limited while also outlining if and when its use is justified.

There are, however, some key concerns levied at using the just war tradition as a basis for developing an ethical framework for intelligence. Key amongst

DOI: 10.4324/9781003164197-3

them is that intelligence is not a war. That is, a lot of what intelligence does focuses on domestic surveillance with activities closer to police work; it is not on a battlefield, weighing up the costs of killing the soldier in front of you, but rather involves extensive and systematic collection of data. Intelligence is not necessarily about examining the ethical cost of killing an individual in order to protect one's own or another's life. It is about data collection and analysis in order to prevent threats from actually causing significant harm to another. For some, therefore, it is better if intelligence was located within the political as compared to the security sphere, where questions on its activity should reflect existing domestic oversight structures. There are concerns that equating intelligence with war makes its activities too permissive; the supreme emergency often associated with war heightens the pressure to act and lowers the ethical threshold, making it an ill fit for a broad set of activities which are often carried out in times of peace and against one's own population.

However, while intelligence is not war, it is also not police work. Indeed, although it is actually difficult to place a clear set of boundaries around what intelligence is – as it ranges from data collection and analysis to more active forms of paramilitary operations – intelligence is quintessentially an activity that concerns itself with "national security", dealing with threats greater in their impact both in terms of areas of national importance and number of people affected. It is tasked with detecting threats that can represent a significant harm to a large number of individuals and works within the national security infrastructure to provide security to the community as a whole. The argument put forward here, therefore, is that by looking at the underlying tensions presented by intelligence activity and the justifications found within the just war tradition a set of specialized just intelligence principles can be established.

Indeed, on a theoretical level the just war tradition gives an important starting point in the need to understand the fundamental harm caused to the individual – that is, the impact it has on our most fundamental vital interests – and how this relates to the harm that the national security agenda is seeking to prevent. Just as the just war tradition recognizes a general presumption against killing to be justified within a set of given limits, the impacts of secret keeping on people's autonomy and other vital interests means there is also a general presumption against secrecy unless a direct justification is given (Calhoun 2001). The tradition then invites us to break down the justification into a set of ethical sub-questions and debates to be had that, in combination, provide an extensive understanding as to whether the act is just or not. These criteria are well versed in dealing with the types of ethical debates that are raised in the security sphere, drawing on both absolutist and utilitarian questions and concerns. For example, the principle of just cause asks us to consider the underlying reason given for why the harm is justified, drawing on wider ethical arguments on self-defence and the duty of the state to protect the political community, explored through hypotheticals and real-life or historical cases to understand what reasons are justifiable for different acts. The principle of legitimate authority places the political community at the centre, challenging both oversight internal to the intelligence community and those external structures that are pulled into the protective shield of secrecy to lose much of their potency. While the principle of proportionality delineates what costs and benefits should be included in the calculation and ensures that the overall benefit is in the positive, the principle of discrimination seeks to distinguish the rights and obligations the state has to different groups of people, outlining who is a legitimate target and who is protected. Not only does the just war tradition direct us to ask certain ethical questions that are relevant in the security world but it also establishes a body of thought to guide the types of debates we should be having, and the variety of answers available to us.

One important difference, however, between war and intelligence is that in the former there is a sharp distinction between the justice of going to war, *jus ad bellum*, and the justice of actions within war, *jus in bello*. This distinction does not work when we consider cyber-intelligence collection. There is not the same division between evaluating and sanctioning the general act of intelligence collection and the carrying out of the variety of acts under this authorization that is seen with war. There is no "time of war/time of peace" distinction for intelligence, but rather operations are running continuously. So, with intelligence, the evaluation must be done continuously, whereby each operation must fulfil all the just cyber-intelligence principles described later, with an operation being sanctioned according to who is being targeted, taking into account whether there is a specific just cause for the operation, ensuring that there is a right intention, and that the method chosen is proportionate the proposed gains.

Adapting just war for just intelligence

Reconceptualizing the idea of security

In order to create this new ethical framework how we conceive of "security" needs reconceptualizing. While Zedner is correct in that security is another "promiscuous concept" (Zedner 2009, 9) – ranging in content, referent object and means of provision[8] – the value of security, and from there the right or expectation to have security, for this chapter is directly linked to the value that an individual has in maintaining their vital interests.[9] That is, security is the condition by which one's vital interests are maintained and protected. This means contemplating security as the processes and protections designed to maintain people's vital interests. For example, at its core the vital interest in maintaining one's physical integrity gives rise to the understanding of security as personal safety, thus "usually understood to refer to the protection against physical or other harm" and to provide security therefore includes "the prevention of or resilience against deliberate attack" (Schneier 2006, 12).[10] Or, in terms of privacy, security refers to the protections one has, both physically and symbolically, that prevent outsiders from intruding on private spaces or accessing personal information without authorization.

Security is therefore not separate from people's interests, but an overarching formula by which they are ensured, and the role of the state is to negotiate the tensions between the various vital interests and seek to provide the necessary protections so that individuals can fulfil their own version of the good life. The provision of security means understanding the complex interrelation between an individual's vital interests and offering them the necessary protections, and that harming someone is the way and degree to which these vital interests are violated. What this understanding provides is a way of detailing the impact, or harm, that intelligence can have on individuals, which can then be reconciled with the threat the intelligence community is seeking to prevent. Importantly, this means that security and human rights are not opposing attributes to be "balanced" against each other but are different aspects of the same phenomenon. Indeed, narratives that portray security and liberties as opposing qualities that must be traded or balanced, while pervasive, are dangerous (Waldron 2003; Pozen 2015; McArthur 2001). By framing it as a trade-off between privacy and security, where you can have either security or privacy but not both and, importantly, where security is seen as a trump card (Thompson 2001; Dragu 2011; Bambauer 2013),[11] it is not surprising that "After 9/11 countries around the globe unhesitatingly adopted policies to enhance their government's capacity to prevent terrorism . . . at the expense of individual civil liberties" (Dragu 2011).[12] While Jeremy Waldron warns that even these framings are problematic in terms of unequal distribution of the trade-off, unclear returns for any given exchange and the problem of trading liberties at will (Waldron 2003), it is argued here that these framings fail to see how the matrix of vital interests should be taken as a whole, viewed holistically in order to provide an individual with enough of his vital interests that he can carry out his goals, and therefore be deemed secure. This means that "the overlapping or even isomorphic relationship between privacy and security is far more subtle than it might be imagined and cannot be glossed over by a rhetoric of 'opposed' rights or values of security and privacy" (Raab 2017).

Therefore, it is important to understand the harm that an intelligence activity represents through its aim of providing security to people so that this can be reconciled with the harm that it seeks to prevent by forestalling a threat from being realized. As a process this means, first, recognizing that while some vital interests such as physical and mental integrity might appear to take precedence over the other interests such as autonomy, liberty, self-worth or privacy, they should be taken together as a complex matrix that all need to be maintained.[13] That in maintaining the security of the individual an excess of one vital interest will not necessarily make up for the lacking of another interest: an excess of physical security cannot be used as a justification for undermining people's privacy; it cannot be argued that people are physically very safe in exchange for having no privacy (Feinberg 1984, 37; Rescher 1972, 5).

Secondly, in making this calculation, it is important to understand that these vital interests are not binary, whole one minute and utterly destroyed the next, but exist to varying degrees given the context. The negotiation therefore involves understanding which and to what extent both the state and a perpetrator are threatening vital interest(s). For example, privacy can be perceived as consisting of different levels where the more personal or intimate the information, the greater the expectation of privacy (Marx 2004, 234; Von Hirsch 2000). Therefore, there must be a greater threat to someone's other vital interests to justify the privacy intervention. Part of this negotiation is understanding whether the target has acted in some way so as to waive or forfeit their immediate vital interests, the potential threat to other people's vital interests represented by the aggressing actor and that the state is itself not representing the greater threat to our vital interests.

Proportional problems and proportional responses

I have spoken elsewhere about a metaphorical "ladder of escalation" which can be used to separate out different intelligence collection activities according to the harm they cause, which can be set against the level of threat they seek to prevent. This flexibility allows for a differentiation across the large range of intelligence activities and situations with a flexible set of just intelligence principles, each with their own series of internal spectrums or proportional calculations. For example, in terms of just cause and self-defence the type of defence one should muster should be proportional to the type of threat. That is, if the threat is of lesser magnitude than killing or severe suffering, while there might not be a justification to kill in self-defence there could be justification for a low-level physical response, loss of property and resources, or sanctions (Pattison 2018). For intelligence, this means the justified intelligence activity should reflect the potential threat represented. Equally, for authority then different measures need to be in place to offer flexible but increasing oversight as the harm caused goes up, whereby the level of blame is not diminished but more securely located with those in charge. While for discrimination this allows those tangentially involved with a threat to be included for low-level intelligence activities, while being protected from more intrusive forms lest evidence shows they have a greater involvement.

Temporal quality

One of the key differences between war and intelligence is that in the former the threat is relatively known, whereas intelligence activity can, and should, come long before the threat is known for it is the purpose of the intelligence operative to locate the threat in the first instance. Therefore, intelligence can involve targeting individuals before their threat status is known, which means decisions are being made on whether or not to use an intelligence activity before one is able to make an ethical calculation as to whether it is justified or not. In order to reconcile this it is necessary to think of intelligence as a form of pre-emptive or preventive self-defence. This is based on the argument that there is a distinction between "self-defence against present definite threats . . . definite future threats . . . as well as indefinite potential threats" (Lee 2018, 346; Walzer 2015). For example, pre-emptive self-defence counters threats that, while not realized, have a clear likelihood and close temporal quality, while preventive self-defence has a much broader temporal range, being years down the line or where it is unclear if the threat will materialize. By understanding intelligence as a flexible, proportional activity it is possible to use those activities which cause a lower level of harm to gather initial information on a situation and target, and then use this information to either escalate up through more harmful intelligence activities or by abandoning the target.

Developing and applying just intelligence principles

Following from these initial principles a set of “just intelligence principles” can be created. These principles reflect the underlying ethical arguments found within the just war tradition but are appropriately adapted for intelligence activity. These just intelligence principles are as follows (Bellaby 2014, 109):

- Just cause: there must be a sufficient threat to justify the harm that might be caused by the intelligence collection activity.
- Authority: there must be legitimate authority, representing the political community’s interests, sanctioning the activity.
- Intention: the means should be used for the intended purpose and not for other (political, economic, social) objectives.
- Proportionality: the harm that is perceived to be caused should be outweighed by the perceived gains.
- Last resort: less harmful acts should be attempted before more harmful ones are chosen.
- Discrimination: there should be discrimination between legitimate and illegitimate targets.

While a direct transfer of the just war tradition’s principles to just intelligence is both inaccurate and unhelpful, by following the underlying ethical arguments made they can be applied to different areas of intelligence activity.

Just cause

The criteria of “just cause” is often considered to be one of the most important of the just war principles as it outlines the main reason for going to war and the main argument for its ethical justification. Over the years, acting in self-defence has been defined as the main, acceptable just cause for going to war. In comparison, the just cause equivalent for intelligence collection could be interpreted as preventing the realization of a threat against the political community. This is because it is the role of the intelligence to firstly detect, provide information on and initiate some prevention of any and all threats that face the political community. In this way, depending on the nature of the threat, it can act as a just cause to justify the use of the intelligence activity and the harm it can cause. Therefore, by acting to detect and prevent these threats intelligence activity works as an act of a preventive self-defence, averting the actualization of threats against the political community (Bellaby 2014, 26).

However, protecting the political community is more than just protecting the state, and includes its ethical, moral, social and legal norms. The purpose of the just cause is not necessarily to balance these, but to highlight what they are and interrogate them.[14] Reconciling these different conceptions of security and determining if there is a suitable threat to the political community means understanding the threat from both other actors' and the state's own national security efforts if they excessively or unnecessarily violate people's vital interests. For example, when the National Security Agency (NSA) programmes to collect as much information as possible (through surveillance programs referred to as Upstream, Quantuminsert, Tempora) were revealed, by doing this the intelligence services were seen to be significantly violating the privacy of people *en masse* (Feinberg 1984, 35; Bellaby 2016). Therefore while there was not a just cause for such intelligence activity because there was no clear, direct threat to act as a justification, there is in fact a just cause for someone to reveal the information and blow the whistle given the harm being caused. What this means for intelligence is that there is actually a just cause for revealing the secret activity of the intelligence community when their activity itself represents a threat to the political community. When the state, or its representatives, is the source of an unjustified threat to the individual's and society's vital interests then there is a just cause to act.

Just authority

In the just war tradition the principle of legitimate authority determines that in order for a war to be considered morally permissible it must be authorized by the right (or legitimate) authority. That is, those who have the right to command by virtue of their position: "since the care of the common weal is committed to those who are in the right authority, it is their business to watch over the common weal" (Aquinas 2002, 214). This authorizing actor must have both the moral weight of representing and protecting the needs of the political community and ensuring practical considerations such as having the physical, intellectual and emotional ability to take into account the different factors involved while limiting personal costs or bias. While traditionally the legitimate authority rested with the state and its representatives as the most appropriate actor to fulfil these needs, this does not necessarily have to be the case. The state will often represent a good choice as it has extensive experience and a wide breadth of knowledge and in many instances is a manifestation of the political community's best form of protection and ability to represent the wishes of the people. However, at its core the just war tradition seeks to place authority within those who best represent and will act in the interests of the political community and its people. What this means is that when the state fails in this task or begins to represent the source of the problem then there is a need to rest the legitimate authority elsewhere.

Initially, therefore, this should (uncontentiously) mean bringing oversight out of the intelligence community's purview as those planning, performing or managing operations have heavily invested interests. However, while this oversight has traditionally been placed predominantly in the hands of the executive, with additional oversight through the legislature and judiciary, historically many administrations have covered up wrongdoing that would have resulted in individual repercussions for members of government and embarrassment for the administration as a whole (Wells 2004, 1203; Ambinder 2013, 6). Existing institutions have proven unable to act without bias and act outside their political objectives, and are therefore ill-suited for balancing the ethical and security concerns. Indeed, Rahul Sagar has shown that in the United States "Given the President's stronghold over the flow of national security information, there is little reason to believe that lawmakers will be able to *take the lead* in uncovering policies and actions" (Sagar 2016, 128).[15] Whereas in terms of the judiciary he argues that "judges are not trained, and the courts not equipped, to make politically charged decisions about what state secrets are appropriate" coupled with a "judicial deference towards the executive's claims about the harm likely to be caused by the disclosures" (Sagar 2016, 74). Moreover, in those courts where the whole proceedings are kept secret – the Foreign Intelligence Surveillance Court being a notable case – the secrecy limits opportunity for engaged reflection and debate on the legal interpretation as judicial peer review and the right to appeal is prevented.[16] What this highlights is that these existing political structures lack the physical power to keep the intelligence community in check, and are insufficient in manpower, intellectual mandate or drive to do so or cannot separate their own political interests from their role as overseer. The problem seen is that the secrecy necessarily attached to intelligence is extended over the political oversight mechanisms, which in turn insulates them from the piercing power of democratic observation and rather than these actors interrogating intelligence they become habitualized by a national security elitism that distorts their oversight role.

Rather, there needs to be a new, proactive and imbedded set of oversight mechanisms to systematically examine conduct and information collected to determine if it should be released or not.[17] In designing this new oversight actor several principles can be highlighted. First, at its core the principle of legitimate authority distils the idea that the review should be examined before rather than after the event. The wars must pass the initial criteria before any attack is deemed legitimate. This means that the review should be penetrative. The oversight actor should have the power and expectation to review operations, policies, practices and trends within the intelligence community in real time, including whether there are tendencies towards too much secret keeping as well as acting to review individual cases to determine if they should keep the information or not.

Secondly, since the authority should represent the political community, it does not have to be limited to state representatives nor do they necessarily have to be elected or subject to populous demands – as restricting it in this way can be more detrimental to the actual review. Therefore, alternative representative mechanisms can be utilized such as using legal, moral and societal experts or representatives, chosen because of their expertise rather than because of their elected status. In order to avoid the same popular pressures faced by elected officials they should not be subjected to direct democratic elections, but rather represent experts in the relevant fields of intelligence oversight, preferably legally trained, nominated and confirmed by the legislative in a public debate where their suitability is tested.

Thirdly, to limit the distortive effect of political interference the body should be able to determine for itself what information should be released free from political censure. If it detects intelligence activity that contravenes the principles outlined in the other criteria it should be free to determine for itself what to reveal according to the interests of the community and free from worries of political scandal.

Last resort

In the just war tradition the need that war only be undertaken as a last resort is an attempt to allow those means that can cause a lower level of harm, like diplomacy or economic pressure, to be given a chance to resolve the issue before the higher harms seen in war are permitted. This way the more harmful acts are avoided if possible. Based on this conception of last resort, one can argue for a similar rationale for the just intelligence principles. In order for an intelligence collection means to be just it must only be used once other less harmful means have been exhausted or are redundant. In this way, the principle of last resort ensures that the intelligence collection means with the lowest level harm is used first in an attempt to deal with the threat, and thus give the opportunity for more harmful activities to be avoided. While there is no rigid methodology or steps that must be worked through, it does require that some of the more harmful actions are not resorted to out of ease or expediency.

Proportionality

The idea of proportionality is one of the oldest principles not only of the just war tradition but also of moral theory and armed strategy in general. Leaders and individuals alike often weigh up the costs of an action against what can be gained from it. The notion of proportionality seeks to ensure that the harm caused in war is proportionate to the threat that it is meant to overcome, placing a limit on the amount of harm allowed for a given action. What is important is that all the harms are included in the calculation and only those benefits that are directly linked to the just cause should count (Hurka 2005; McKenna 1960; Regan 1996). For example, in terms of war while we would not consider the boost to the economy as a relevant good, the fact that it might hurt the economy would be counted as a negative. Therefore, while wider damages can be included when assessing the need to release the information only specific goods directly relating to the just cause can be included when arguing for information retention.

Similar to the consequentialist calculation one can argue that in order for the intelligence collection to be just the level of harm that one perceives to be caused by the collection should be outweighed by the perceived gains. As David Omand asks, "is the likely impact of the proposed intelligence gathering operation, taking account of the methods to be used, in proportion to the seriousness of the business at hand in terms of the harm it seeks to prevent?" (Omand 2007, 162). On the one hand the costs and gains can be examined in terms of Herman's "balance sheet" approach, where "knowledge and activities can be examined separately, and then can be integrated into an ethical balance sheet" (Herman 2002, 290). This moral accounting allows us to balance the overall good effect of intelligence knowledge against some of the less desirable methods. If it is discovered "at the bottom of the ledger that the benefits of intelligence knowledge is found to be in credit, then the means employed to gather intelligence can be morally justified by the positive impact of knowledge acquired" (Erskine 2004, 366).

In addition to these direct costs, however, we need to include wider costs such as the impact on individuals' autonomy, society, degradation to important social norms and practices and the cohesion of the political community. Richard Matthews argues that no individual is an island, but is a part of a complex set of social networks that are also damaged when someone is affected by intelligence practice: "its run-on effect is well documented and involves wide-ranging pain and suffering across the communities and contexts" (Matthews 2012, 466). For example, additional costs associated with intelligence collection activities can include degradation to social cohesion as minorities are over-represented and excessively targeted, marginalizing them from the greater social whole and reinforcing distorted criminal statistics, often with individuals unaware that their information is being used (Bennetto 2005, 5).

Discrimination

The requirement that an attack must discriminate between combatants and non-combatants is one of the most stridently codified just war rules and is reflected in the international law of war as such. Soldiers charged with the deployment of force and violence cannot do so indiscriminately. They have an obligation to exert a particular effort to discriminate between legitimate and illegitimate targets. The target has to have "something about them" to justify being a legitimate target (Nagel 1979, 124). That is, either the target represented a threat of some form and attacking him is justified as an act of self-defence, or that when the individual became a soldier he waived his normal protective rights in some way.

For intelligence one can argue that, just as soldiers are legitimate targets because they are a threat and they give up certain protective rights, arguably any individual can act in a way as to make themselves a threat or to forfeit certain protective rights. Holding a particular job; being in possession of important information and being a member of a state's infrastructure are all examples of how an individual can make himself liable for the threat or consent to the waiving or forfeiting of certain rights. For example, "consent to participate in the world of national security on all levels of a country's self-defence structure together with the quality of the information possessed" puts the individual liable to the threat and as such justifies them as targets (Pfaff and Tiel 2004, 6).

Notes

[1] For a summary of the various different historical thematic and contemporary intellectual developments see Johnson (2006).

[2] For political use, see Kelsay (2013). For the principle of discrimination, see Article 48, first additional protocol to the Geneva Conventions; for the principle of proportionality, see Article 51(4b), first additional protocol to the Geneva Conventions; for the principle of just cause, see Article 51 UN Charter.

[3] For example, see Lowe (2003), Walzer (2006), Crawford (2003), Sussmann (2013), Valls (2000) and Steinhoff (2004).

[4] For example, see Williams (2015).

[5] For example, see van der Bruggen (2013).

[6] For example, see Fitzsimmons (2015) and Pattison (2008).

[7] For example, see Meisels (2014) and Scheid (2012).

[8] For work on “security studies” and the changes in referent object, the construction of security threats and security actors, see Buzan, Wæver, and de Wilde (1997), Browning and McDonald (2011) and Katzenstein (1996).

[9] For more on there being a “right” to security, see Lazarus (2007), (2012).

[10] This is different from the instrumentalist arguments made by people such as Henry Shue whereby security is necessary for the enjoyment of other rights. See Lazarus (2012).

[11] For arguments against security necessarily trumping privacy, see Moore (2011). For arguments for security trumping privacy, see Himma (2007).

[12] Also see Ackerman (2006) and Hardin (2004).

[13] Isaiah Berlin declared that in much the same way that boots were more important than the words of Shakespeare, liberty and autonomy are not necessarily the total first needs of an individual (Berlin 1969, 124).

[14] For McMahan the principle of proportionality is therefore directly connected to the principle of just cause as it enables the balancing of the just cause against the various potential harm to be caused by the act of war (McMahan 2005).

[15] Also see Born (2003, 22).

[16] For the role of the right to appeal and the importance of multi-layered court systems, see Dalton (1985), Lennerfors (2007) and Nobles and Schiff (2002).

[17] This builds on Rahul Sagar’s discussion on the limits of retrospection as a form of oversight (Sagar 2007, 414–17).

References

Ackerman, Bruce. 2006. *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism: Emergency Powers in an Age of Terrorism*. New Haven: Yale University Press.

Ambinder, Marc. 2013. *Deep State: Inside the Government Secrecy Industry*. Hoboken, New Jersey: Wiley.

Aquinas, Thomas. 2002. “From Summa Theologiae”. In *International Relations in Political Thought: Texts from the Ancient Greeks to the First World War*, edited by Chris Brown, Terry Nardin, and Nicholas Rengger. Cambridge; New York: Cambridge University Press.

Bambauer, Derek E. 2013. “Privacy versus Security”. *Journal of Criminal Law and Criminology* 103 (3): 667–83.

Bellaby, Ross W. 2014. *The Ethics of Intelligence: A New Framework*. London; New York: Routledge.

———. 2016. “Justifying Cyber-Intelligence?” *Journal of Military Ethics* 15 (4): 299–319. https://doi.org/10.1080/15027570.2017.1284463.

Bennetto, Jason. 2005. *Police and Racism: What Has Been Achieved 10 Years after the Stephen Lawrence Inquiry Report?* London: Equality and Human Rights Commission. www.equalityhumanrights.com/en/file/6316/download?token=4QCFPaJj.

Berlin, Isaiah. 1969. *Four Essays on Liberty*. London; New York etc.: Oxford Paperbacks.

Born, Hans. 2003. *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices*. Edited by Philipp Fluri, Anders B. Johnsson, and Born Hans. Geneva: IPU-DCAF.

Browning, Christopher S., and Matt McDonald. 2011. "The Future of Critical Security Studies: Ethics and the Politics of Security". *European Journal of International Relations*, October. https://doi.org/10.1177/1354066111419538.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1997. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Calhoun, Laurie. 2001. "The Metaethical Paradox of Just War Theory". *Ethical Theory and Moral Practice* 4 (1): 41–58. https://doi.org/10.1023/A:1011440213213.

Clark, Ian. 1988. *Waging War: A Philosophical Introduction*. Oxford; New York: Clarendon Press.

Crawford, Neta C. 2003. "Just War Theory and the U.S. Counterterror War". *Perspectives on Politics* 1 (1): 5–25. https://doi.org/10.1017/S1537592703000021.

Dalton, Harlon. 1985. "Taking the Right to Appeal (More or Less) Seriously". *Yale Law Journal* 95 (1): 62–107.

Dragu, Tiberiu. 2011. "Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention". *American Political Science Review* 105 (1): 64–78. https://doi.org/10.1017/S0003055410000614.

Erskine, Toni. 2004. "'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering". *Intelligence and National Security* 19 (2): 359–81. https://doi.org/10.1080/0268452042000302047.

Feinberg, Joel. 1984. *The Moral Limits of the Criminal Law: Harm to Others v. 1*. New York: Oxford University Press Inc.

Fitzsimmons, Scott. 2015. "Just War Theory and Private Security Companies". *International Affairs* 91 (5): 1069–84. https://doi.org/10.1111/1468-2346.12398.

Hardin, Russell. 2004. "Civil Liberties in the Era of Mass Terrorism". *The Journal of Ethics* 8 (1): 77–95. https://doi.org/10.1023/B:JOET.0000012253.54321.05.

Herman, Michael. 2002. *Intelligence Services in the Information Age: Theory and Practice*. London: Frank Cass Publications.

Himma, Kenneth E. 2007. "Privacy versus Security: Why Privacy Is Not an Absolute Value or Right". *San Diego Law Review* 44: 857–920.

Hurka, Thomas. 2005. "Proportionality in the Morality of War". *Philosophy & Public Affairs* 33 (1): 34–66. https://doi.org/10.1111/j.1088-4963.2005.00024.x.

Johnson, James T. 2006. "The Just War Idea: The State of the Question". *Social Philosophy and Policy* 23 (1): 167–95. https://doi.org/10.1017/S0265052506060079.

Katzenstein, Peter. 1996. *The Culture of National Security: Norms and Identity in World Politics*. New York, NY: Columbia University Press.

Kelsay, John. 2013. "Just War Thinking as a Social Practice". *Ethics & International Affairs* 27 (1): 67–86. https://doi.org/10.1017/S0892679412000780.

Lazarus, Liora. 2007. "Mapping the Right to Security". In *Security and Human Rights*, edited by Benjamin Goold and Liora Lazarus, 1st edition. Oxford; Portland, OR: Hart Publishing.

———. 2012. "The Right to Security: Securing Rights or Securitising Rights". In *Examining Critical Perspectives on Human Rights*, edited by Rob Dickinson, Elena Katselli, Colin Murray, and Ole W. Pedersen. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139026291.

Lee, Hsin-Wen. 2018. "A New Societal Self-Defense Theory of Punishment: The Rights-Protection Theory". *Philosophia* 46 (2): 337–53. https://doi.org/10.1007/s11406-017-9931-z.

Lennerfors, Thomas Taro. 2007. "The Transformation of Transparency: On the Act on Public Procurement and the Right to Appeal in the Context of the War on Corruption". *Journal of Business Ethics* 73 (4): 381–90. https://doi.org/10.1007/s10551-006-9213-3.

Lowe, Scott. 2003. "Terrorism and Just War Theory". *Perspectives on Evil and Human Wickedness* 1 (2): 46–52.

Marx, Gary. 2004. "Some Concepts That May Be Useful in Understanding the Myriad Forms and Contexts of Surveillance". *Intelligence and National Security* 19 (2): 226–48. https://doi.org/10.1080/0268452042000302976.

Matthews, Richard. 2012. "An Empirical Critique of 'Interrogational' Torture". *Journal of Social Philosophy* 43 (4): 457–70. https://doi.org/10.1111/josp.12004.

McArthur, Robert L. 2001. "Reasonable Expectations of Privacy". *Ethics and Information Technology* 3 (2): 123–8. https://doi.org/10.1023/A:1011898010298.

McKenna, Joseph C. 1960. "Ethics and War: A Catholic View". *American Political Science Review* 54 (3): 647–58. https://doi.org/10.1017/S0003055400122609.

McMahan, Jeff. 2005. "Just Cause for War". *Ethics & International Affairs* 19 (3): 1–21. https://doi.org/10.1111/j.1747-7093.2005.tb00551.x.

Meisels, Tamar. 2014. "Fighting for Independence: What Can Just War Theory Learn from Civil Conflict?" *Social Theory and Practice* 40 (2): 304–26. https://doi.org/10.5840/soctheorpract201440218.

Moore, Adam D. 2011. "Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability". *Public Affairs Quarterly* 25 (2): 141–56.

Nagel, Thomas. 1979. *Mortal Questions*. Cambridge: Cambridge University Press.

Nobles, Richard, and David Schiff. 2002. "The Right to Appeal and Workable Systems of Justice". *The Modern Law Review* 65 (5): 676–701. https://doi.org/10.1111/1468-2230.00403.

Omand, David. 2007. "Reflections on Secret Intelligence". In *The New Protective State: Government, Intelligence and Terrorism*, edited by Peter Hennessy, 1st edition. London; New York: Continuum.

Pattison, James. 2008. "Just War Theory and the Privatization of Military Force". *Ethics & International Affairs* 22 (2): 143–62. https://doi.org/10.1111/j.1747-7093.2008.00140.x.

———. 2018. *The Alternatives to War: From Sanctions to Nonviolence*. Oxford, UK; New York: OUP Oxford.

Pfaff, Tony, and Jeffrey R. Tiel. 2004. "The Ethics of Espionage". *Journal of Military Ethics* 3 (1): 1–15. https://doi.org/10.1080/15027570310004447.

Pozen, David. 2015. "Privacy-Privacy Tradeoffs". *University of Chicago Law Review* 83 (1): 221–47.

Quinlan, Michael. 2007. "Just Intelligence: Prolegomena to an Ethical Theory". *Intelligence and National Security* 22 (1): 1–13. https://doi.org/10.1080/02684520701200715.

Raab, Charles D. 2017. "Security, Privacy and Oversight". In *Security in a Small Nation: Scotland, Democracy, Politics*, edited by Andrew W. Neal. Open Book Publishers. https://doi.org/10.11647/OBP.0078.

Regan, Richard J. 1996. *Just War: Principles and Cases*. Washington, DC: The Catholic University of America Press.

Rescher, Nicholas. 1972. *Welfare: The Social Issues in Philosophical Perspective*. 1st edition. Pittsburgh: University of Pittsburgh Press.

Sagar, Rahul. 2007. “On Combating the Abuse of State Secrecy”. *Journal of Political Philosophy* 15 (4): 404–27. https://doi.org/10.1111/j.1467-9760.2007.00283.x.

———. 2016. *Secrets and Leaks: The Dilemma of State Secrecy*. Revised edition. Princeton, NJ: Princeton University Press.

Scheid, Anna F. 2012. “Waging a Just Revolution: Just War Criteria in the Context of Oppression”. *Journal of the Society of Christian Ethics* 32 (2): 153–72. https://doi.org/10.1353/sce.2012.0035.

Schneier, Bruce. 2006. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. 2003. Corr. 2nd edition. New York: Springer-Verlag New York Inc.

Steinhoff, Uwe. 2004. “How Can Terrorism Be Justified?” In *Terrorism: The Philosophical Issues*, edited by Igor Primoratz, 97–109. UK: Palgrave Macmillan. https://doi.org/10.1057/9780230204546.

Sussmann, Naomi. 2013. “Can Just War Theory Delegitimate Terrorism?” *European Journal of Political Theory* 12 (4): 425–46. https://doi.org/10.1177/1474885112464478.

Thompson, Paul B. 2001. “Privacy, Secrecy and Security”. *Ethics and Information Technology* 3 (1): 13–9. https://doi.org/10.1023/A:1011423705643.

Valls, Andrew. 2000. “Can Terrorism Be Justified?” In *Ethics in International Affairs*, edited by Andrew Valls, 65–79. Lanham, Maryland: Rowman & Littlefield Publishers.

van der Bruggen, Koos. 2013. “Biosecurity and the Just-War Tradition”. In *On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects*, edited by Michael J. Selgelid and Brian Rappert. ANU E Press. https://research.monash.edu/en/publications/on-the-dual-uses-of-science-and-ethics-principles-practices-and-p.

Von Hirsch, Andrew. 2000. “The Ethics of Public Television Surveillance”. In *Ethical and Social Perspectives on Situational Crime Prevention*, edited by Andrew Von Hirsch, David Garland, and Alison Wakefield, 59–76. Studies in Penal Theory and Penal Ethics. Oxford: Hart.

Waldron, Jeremy. 2003. “Security and Liberty: The Image of Balance”. *Journal of Political Philosophy* 11 (2): 191–210. https://doi.org/10.1111/1467-9760.00174.

Walzer, Michael. 2006. “Terrorism and Just War”. *Philosophia* 34 (1): 3–12. https://doi.org/10.1007/s11406-006-9004-1.

———. 2015. *Just and Unjust Wars*. 5th edition. New York: Basic Books.

Wells, Christina E. 2004. “‘National Security’ Information and the Freedom of Information Act”. *Administrative Law Review* 56 (4): 1195–1221.

Williams, John. 2015. “Distant Intimacy: Space, Drones, and Just War”. *Ethics & International Affairs* 29 (1): 93–110. https://doi.org/10.1017/S0892679414000793.

Zedner, Lucia. 2009. *Security*. 1st edition. London; New York: Routledge.