FEATURE

Information, Privacy, and Just War Theory

Jack McDonald[*]

Just war theory has a privacy problem. That is, in order for individuals to act in a morally permissible manner in war, it is likely that they will need to rely upon information obtained by others, often in a manner that would be considered a violation of privacy. As unwarranted privacy violations are now widely conceived of as harmful actions, this creates a functional problem for each and every participant: conducting morally permissible physical action requires the commission of prior informational harms, either by the individual or by the institution of which they are a part. At the same time, privacy, and the notion of privacy rights in war, is underexamined in contemporary just war theory. This presents something of a puzzle: why does this remain the case, despite the rising consideration of privacy and privacy-related harms in the broader discourse?

Just war theory tacitly presumes that the sources of a combatant's knowledge are not a significant issue. Despite the fact that most ethical frameworks—including just war theory—imply that individuals have epistemic duties, epistemic questions are secondary issues in the normative debates of just war theory. Even though war and combat are constituted by epistemic uncertainty and unpredictability, the way that harm in such circumstances is usually analyzed is via discussion of the *expected* harm that will result from a given course of action.[1] Such expectation relies on the assumption that the probable harms of actions can be accurately computed. On this basis, the issue of epistemic uncertainty is limited to what combatants should do, where the outcome is unknown, or to a definable risk between two (or more) different outcomes, at least one of which is to be

[*]I would like to thank Mervyn Frost for his comments on this article, as well as the two peer reviewers and editorial team at *Ethics & International Affairs*. Previous versions were presented at the 2018 and 2019 ISA annual conferences, and I would like to thank Amy E. Eckert, Daniel R. Brunstetter, and Valerie Morkevičius for their comments on this work as it progressed.

Ethics & International Affairs, 34, no. 3 (2020), pp. 379–400.

doi:10.1017/S0892679420000477

avoided.[2] For this reason, there is a strong tendency in the literature to select situations in which theorists can at least agree upon a set of facts, or to the degree and character of uncertainty in a given situation. Debate in just war theory is therefore largely constituted by disagreements over the moral analysis of historical events and idealized thought experiments where "philosopher's cases usually presuppose omniscience."[3] When epistemic issues are examined in these thought experiments, standards of knowledge (and their moral implications) are deemed more important than sources of knowledge. This approach makes sense for conducting theoretical analysis, but it can have pernicious consequences for the character of discussion.[4]

Thus, the ongoing "renegotiation" of the tradition is primarily a debate over the relevant or correct moral principles that justify going to war, or activities therein, and not the harms caused by information collection or processing.[5] Most just war theorists are primarily concerned with ontological questions, such as whether or not social or functional categories such as "combatant" matter, and the normative questions related to harm in war, such as what actions or status render someone liable to attack.[6] But moral agency in war requires individuals to rely upon information and knowledge generated by social institutions, and these institutions routinely gather information by violating privacy either at the individual level or at the societal level. For this reason, we should not treat the information required for moral agency as morally neutral. Since the sources of a combatant's knowledge in war often rely on previous privacy harms, these harms should be considered in the context of war. Privacy harms pose a particular problem for revisionist views of war that reject the idea of war as a special sphere of activity (reductivism) and for the view that in war only individuals act or matter (descriptive and evaluative individualism).[7]

In this article, I argue that privacy harms cannot be evaluated without reference to social goods, and that in war and national security contexts, privacy violations by state agents and institutions should be explained in terms of balancing privacy and security. From a reductivist viewpoint, the existence of war should not change the method of moral calculus, nor the set of objects used to evaluate a given event. I argue that this often does not hold true in war, where privacy violations are generally ex parte, with no right of redress or challenge, and they often involve considering the security of one population over the privacy rights of another. Furthermore, there is a clear logic that leads to a total deprivation of privacy rights in war—suggesting that the injustice of killing noncombatants based upon poor

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

information availability outweighs the violations of privacy that might produce the information that would remedy this problem. Traditionalist nonreductive just war theory is better able to explain this moral problem and provide a practical guide for moral agency in war because it incorporates an analysis of social goods.

Individualist approaches to the ethics of war fail to explain the important features of privacy harms because privacy cannot be understood without its social context. Privacy is a social good, and one that a strict language of rights, duties, and obligations cannot accurately describe. Explaining the justice of privacy intrusions requires making reference to social goods, such as security, in balancing the social consequences of privacy harms against other social consequences, such as wrongful attacks due to lack of information. This, I argue, is a fundamental challenge for individualist views of war, which is left to explain not only speculative privacy violations but also individual reliance upon them.

Theorizing Privacy Harms in War

Moral agency and responsibility in war requires individuals to rely upon information and knowledge generated by social institutions. The worldviews of combatants are fundamentally shaped by the military institutions to which they belong. But individuals have epistemic duties, such as the duty to know. As Holly M. Smith notes: "If you are a military leader whose lieutenants recommend bombing a compound that might house enemy soldiers, you have an obligation to investigate—before bombing it—whether the compound really does house enemy soldiers, and whether it houses innocent civilians as well."[8] In this situation, the leader in question is likely to find it impossible to fulfill his or her duty to know this information without relying upon the larger military organization to which they belong. This demonstrates how information processing and knowledge generation in war is a social activity—no combatant has ever derived his or her entire knowledge in a war from only their perception or first principles. That said, there are some ways of fighting that reduce individuals' epistemic reliance upon information generated by their compatriots. For example, customs of pitched battle made enemy forces easy to identify, and therefore simplified many of the issues discussed in this article. Military uniforms and markings are, in effect, a means of self-identification to erase ambiguity in the eyes of the opposing force.[9] But wars are no longer fought in pitched battles, and many military forces refuse to wear identifying markings that enable their opponents to

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

recognize them as combatants. Moreover, guerrilla warfare and irregular warfare are often conducted in a manner where combatants disguise themselves among civilian populations. My aim here is not to retread well-articulated discussions regarding the ethics of guerrilla warfare,[10] or even terrorism, but to highlight that from an information-processing perspective, these changes in military practice have also given rise to ethical problems for those on the opposing side seeking to identify their adversary.

The sources of facts in war matter because combatants do not perceive the world from a neutral set of data. Institutional processes and procedures will largely determine the set of facts available to combatants at any key decision point.[11] Further, these processes and procedures are in a constant state of flux, and the knowledge that organizations generate serves to reshape the way they perceive their environment.[12] Military personnels' perceptions of operational environments are further shaped by their professional identity, itself informed by their membership in a wider transnational epistemic community of military professionals.[13] Knowledge generation by militaries is task oriented. For example, at the operational level, identification and targeting—generating facts as to who and what is or is not a permissible target—is a core element of what military institutions do.[14] Organizational-targeting processes draw upon collections of prior intelligence, as well as the corporate knowledge of militaries.[15] Antoine Bousquet defines this combination of military perceptual technologies, institutions, and mindset as the "martial gaze"[16]—a specific way that militaries perceive the world. These structural factors shape the availability of information to individual combatants. Changes to military structures can alter the information available to combatants in a significant way. For example, the networking of military forces, which allows "for an immense flexibility in terms of the location of decision-making" also involves a "radical altering of the nature of communication and responsibility."[17] This institutional worldview matters. As Neta Crawford notes, "The organization—the attitudes and beliefs of majority of its members, the standard operating procedures of the institution, and the resources and tools available for action—reduces the effectiveness of individual action unless it is in concert with the organization."[18]

The problem for the individual combatant is that, as noted above, the intelligence gathering and data processing necessary for action in war can also be harmful. Surveillance and war go hand in hand. Even during peacetime, modern states and state institutions rely upon surveillance in order to operate,[19] and their

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

militaries are no different. In order to wage war, military institutions are likely to perform intelligence-gathering actions that would be unconscionable at home. Although surveillance in war is intentionally underregulated, it nevertheless often violates the privacy rights of noncombatants. Here, the clearest examples relevant to contemporary conflict are instances where states use technology to conduct data collection at mass scale. Particularly in irregular conflicts, states and their militaries now turn to large data sets to identify their opponents,[20] and such techniques often require the processing of large sets of civilian data. "Person reidentification" refers to surveillance techniques that enable the tracking of individual persons through the analysis of otherwise anonymous video feeds and/or multiple data sets, infringing upon the privacy of large numbers of noncombatants. Here, the fact that information about a person exists in some form—even if it is anonymous—enables individuals or organizations to collate that information at a later date in order to track the person.[21] Since at least 2007, the U.S.-led coalition that toppled Saddam Hussein's Baathist government in Iraq has collected biometric information on individual Iraqi citizens in order to identify and track insurgents operating against coalition forces.[22] This type of control over populations through surveillance is not new—identity card systems were a key tool of counterinsurgency operations in the twentieth century[23]—but the scale of possible data collection, and the types of data that can be gathered, is now radically greater than before. In the case of Iraq, the revelation of this collection resulted in a group of NGOs writing to former U.S. defense secretary Robert Gates, alleging that this data collection violated international privacy standards.[24] The U.S. Army also recognized that this information could effectively be used as a "hit list" if belligerents in Iraq's sectarian conflict were to gain access to it.[25] Nonetheless, the United States retained possession of this data set after withdrawing its forces from Iraq, leading to a political dispute over the data's ownership.[26]

What this and other such examples demonstrate is that in cases where combatants require knowledge generated by privacy harms in order to make a moral choice, just war theory needs to integrate analysis of privacy harms into its analysis of individual actions. One difficulty in this regard is that privacy is both a relatively new social concept—one that only took shape in the late nineteenth century[27]—and an amorphous one, such that "no single model suffices to fully characterize all of the forms that privacy issues can take."[28] According to Daniel J. Solove, "We should understand privacy as a set of protections against a plurality of distinct but related problems."[29] Despite these differences, privacy

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

protection is often portrayed as necessary to protect core personal and social values against a variety of harms to both individuals and society.[30]

While most theorists agree that the violation of privacy protections generates harm, the definition of what privacy seeks to defend, how it defends it, and why can differ markedly between conceptualizations. Solove identifies six different and overlapping conceptions of privacy. He begins with Warren and Brandeis's theory of privacy as "the right to be let alone,"[31] and then identifies five others: limited access to the self; secrecy; control over personal information; personhood; and intimacy.[32] Some of these conceptualizations are likely familiar—the ideas that a person should have the right to a private space, that the state (or other people and corporations) should not be able to pry into a person's private thoughts, and that individuals should be able to keep secrets, free from unwarranted intrusion. Common to all of these conceptualizations, Solove identified four basic groups of harmful activities in relation to privacy: information collection, information processing, information dissemination, and invasion or "interference with one's personal life."[33] Solove's four-problem set can arguably be applied to other conceptual mappings of privacy as well, such as those supplied by Martin Kuhn and Helen Nissenbaum. This is because Solove's bottom-up taxonomy of privacy problems is a way of thinking about the kind of activities that can give rise to privacy harms without being dependent upon a specific conceptualization of privacy. Kuhn identifies three conceptualizations of privacy: privacy as (protected) space, privacy as secrecy, and privacy as information control.[34] Similarly, Nissenbaum identifies three privacy principles derived from social debates: limiting the surveillance of citizens, restricting access to personal or private information, and curtailing intrusions into private personal places.[35] Even though the taxonomies of Kuhn and Nissenbaum differ from that of Solove, the value of Solove's four-problem schema is that it covers the underlying privacy problems themselves.

Privacy violations and privacy harms cannot be explained without reference to social goods and values. The social good of privacy protections is intertwined with the social ills that privacy can also enable. In other words, "The value of privacy should be understood in terms of its contribution to society."[36] This is a social balancing act in the sense that privacy and national security are inextricably linked.[37] For example, the software encryption that enables online privacy and Internet banking also enables terrorists to remain anonymous and engage in money laundering. Governments must therefore weigh individual privacy rights

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

against their social consequences such that "when privacy protects the individual, it does so because it is in society's interest."[38] Privacy harms can be individual, but they can also be social. As Roger Clarke notes, "All users of electronic tools are subject to intensive surveillance,"[39] but to focus upon the surveillance of individual users misses the larger point. According to Clarke, there can be great harms inflicted at the societal level by "dataveillance"—a term he coined in 1988 to refer to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[40] The widespread use of digital devices, combined with what Clarke calls a "digital surveillance economy,"[41] is built upon monitoring individual behavior and is seen by some as a threat to informational privacy, or "the ability to control the acquisition or release of information about oneself."[42] The unprecedented volume and variety of information now available in near real time to companies has had a massive economic impact, with entire commercial sectors reordering themselves around the emergence of "big data." Though this data allows companies to track and target individual customers, we must evaluate the harm of these activities in the aggregate, not by focusing on the harms suffered by individuals on a case-by-case basis.

Much of the literature on privacy analyzes the balance of social goods and ills in terms of national, or single-society, concerns. This raises a further question: Should states treat those beyond their borders as equals? Most analyses of privacy harms privilege the privacy of the citizens of a home state at the expense of those abroad. More recently, however, some scholars have homed in on the privacy harms to individuals and societies arising from intelligence collection that states are undertaking in foreign countries.[43] Some argue that states should treat all individuals, whether citizen or foreigners, as equals; something Peter Margulies defines as the equivalency thesis: "A state must accord equivalent rights to persons within its own borders and persons located overseas with no ties to that state."[44] This highlights a key problem with privacy harms in war: Privacy balancing, such that it exists as a coherent process, is a unilateral endeavor, usually performed by a state in response to its society.[45] Extraterritorial privacy balancing may involve diplomacy between states, but in war it becomes a unilateral endeavor—an imposed balance, or a set of mutually imposed balances in the case of a civil war. Though human rights norms prohibit arbitrary intrusions of privacy, the law of war remains fundamentally silent on such matters.[46] Where the literature addresses the problem of privacy harms undertaken in order to forestall

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

extraterritorial threats, such harms are generally addressed within an analytical frame that focuses upon the costs and benefits to the privacy balance of the state inflicting the harms, and the consequences for the other states' populations are rarely considered in the same way. Moreover, whereas mechanisms often exist domestically to redress privacy harms, extraterritorial privacy harms (of the kind with which this article is primarily concerned) usually lack the kind of adversarial challenge processes found in domestic settings.[47]

So far, I have argued that just war theory should not view information processing as morally neutral, and that we can see moral harms attached to many kinds of information processing in war. If information processing can cause harms, then there will be conflicts where the moral evaluation of actions requires us to also consider the privacy harms committed in order to enable the action itself. As I have shown, the evaluation of privacy harms requires us to consider both social harms and social goods. The balancing of social goods and privacy harms usually takes place in a national context, but evaluating privacy harms in war requires us to consider how such balancing is performed, and who gets to dictate the balance. While there will be many situations where the privacy harms preceding action are of no relevance, there are plenty of privacy harms that are consequential. The second part of this article will focus on situations where privacy harms are relevant to the moral evaluation of war. Here I will argue that privacy harms challenge reductivist views of the morality of war, because the justification for privacy harms requires balancing social goods. This balance is fundamentally different during war than it is during peacetime, thus challenging reductivist views of war itself.

Privacy Harms as a Challenge to Reductivism

Given the traditionalist focus on social category and status, privacy harms pose much less of a problem for traditionalist conceptions of just war than revisionist ones. Whereas revisionist analysis of just war seeks to ground the morality of war in a coherent framework of analytical philosophy, traditionalist just war theory does not necessarily have, or seek, the same internal coherence. Michael Walzer's *Just and Unjust Wars* was, after all, the target of significant criticism by revisionists precisely because it lacked such theoretical coherence at its core. Conversely, if individuals have a right not to be harmed, and privacy is considered a similar sort of right, then it is hard to coherently argue that one right is important and should be retained, while another is not and should not be. There are, of

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

course, possible objections, since, as mentioned above, privacy norms are highly contested (in part due to their recent development) whereas physical and bodily integrity rights are more clearly defined.

Privacy harms pose a problem for reductivist theories of just war. From a reductivist perspective, the reasoning that makes an act morally justifiable in war must be the same reasoning that makes it morally justifiable in peacetime. Therefore, a reductivist approach to privacy harms in war would require that the explanations for privacy harms in war do not differ from the explanations for said actions outside war.[48] If violations of privacy rights are to be explained by the same set of factors both within and outside the context of war, where does that leave combatants? Do they have privacy rights, even in war? Reductivist approaches maintain that "people have fundamental rights to life and liberty that they don't simply lose once they enter a state of war."[49] But what of the right to privacy in this context? If individuals do not lose their rights at the onset of war, do both combatants and civilians retain the right to privacy (if such labels even matter)? After all, a core element of revisionist critiques of the notion of combatant equality is that combatants' fundamental rights, such as the right to life, cannot be surrendered simply because they pose a threat to others via membership in a fighting group.[50]

Even if combatants do not retain their privacy rights in war, what of civilians? Walzer's argument is that individuals ground their inalienable rights in their status, and that combatants, and only combatants, lose this right due to making themselves "dangerous" in the context of war.[51] However, this same logic does not necessarily apply to privacy harms inflicted upon civilians. Civilians are not dangerous—they are merely a source of information, a resource to be tapped. Moreover, reductivist theories will need to explain privacy harms in the same manner that they explain physical harms. Here, many of the moral theories associated with revisionist just war theory encounter problems. Since privacy harms are inflicted to inform agents needing to identify threats, such harms are not generally inflicted in response to obvious threats. Revisionist theories explain the loss of individual rights as due to the actions of individuals; they bear responsibility for posing a wrongful threat.[52] But the anticipatory nature of privacy harm means that this logic does not sufficiently explain the loss of privacy rights, or the liability to privacy harms, in the general circumstances of war. Further, it does not explain why forms of anticipatory privacy harm at a societal level may be necessary in war when they would be unnecessary in peacetime, nor does it explain why the

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

balancing of privacy harms against social goods in war may differ from similar balancing calculations in times of peace.

In my view, the key challenge the reductivist point of view encounters here is how to balance the harms of privacy violations against the social goods that such violations support. The balancing of social goods in war is profoundly difficult, and a key contemporary problem in both just war theory and the law of armed conflict is that the normative basis for action in war conflicts with other normative frameworks, such as human rights.[53] Reconciling such conflicting normative frameworks is a difficult task, and there is much disagreement among scholars and practitioners as to how these two frameworks in particular should interact during armed conflict.[54] In the context of ongoing theoretical debates within just war theory, this is closely aligned to wider debates over the retention of individual rights in armed conflict,[55] and whether the onset of armed conflict causes individual rights to change, or whether just war norms supersede individual rights.

For a reductivist, the onset of war should not change the evaluative framework. There are two problems with this belief. First, in extraterritorial conflicts, privacy balancing requires the consideration of the privacy goods of a separate society. Second, there is the issue, raised briefly above, of who gets to determine the balance. If all harm in war is justified in the same manner as harm in peacetime, how can reductivists account for the unilateral imposition of privacy balancing that occurs in war? While the method of examining the balance of privacy harms against social goods may not change, the underlying social, political, and moral relationships involved are profoundly different. Furthermore, as explained above, privacy rights differ from the rights with which just war theorists are primarily concerned. Unlike the right to life, privacy rights are to a significant degree socially contingent. In this regard, war has a generative force, producing new social relationships.[56] A reductivist account of rights, on the other hand, is essentially static: the onset of war does not remove preexisting rights. With privacy rights, we can see that this stasis works both ways, as it forecloses consideration of the generation of new relationships of rights in war.

As has been made clear, my view is that privacy harms are best accounted for from a nonreductive view. In the words of Seth Lazar, "An exclusively reductivist account of the morality of war would be incomplete."[57] Though nonreductivists (at least those who think that privacy rights exist in the first place) must still explain why the onset of war or armed conflict circumscribes these rights, they

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

are able to do so using a similar logic to that behind the justification for the use of violence in war. In other words, the commission of privacy harms is justified via the existence of war itself, as is the need to rebalance privacy concerns in the context of war (out of necessity), and further, the need to explain how the special status of war gives rise to new sets of rights relations between a state and an extraterritorial population.

There are still problems with a nonreductivist account. After all, privacy harms are often inflicted not only upon combatants but also upon noncombatant civilian populations as a whole. Following the examination of privacy above, I would argue that the most compelling nonreductivist explanation for privacy harms is that war inherently involves the unilateral balancing of individual rights and social goods by states, and that nonreductivists are able to accept that there are characteristics of this kind of unilateral balancing that are specific to the context of war. This view would likely rely upon a necessity claim (that intelligence collection in war is necessary for success) to justify significant privacy harms inflicted upon the civilian population at both an individual and a societal level. Privacy harm can be viewed as fitting the necessity claim in three ways: as a form of collateral damage; in terms of the doctrine of double effect; and, in an odd sense, that by taking refuge within a population, an opponent is effectively using noncombatants as informational human shields. Regardless of which view one takes, traditionalists are able to engage with the unilateral balancing of social goods by states in a way that reductivists cannot.

Privacy Harms as a Challenge to Individualism

Privacy harms are a problem for both descriptive and evaluative individualist approaches to just war theory. As noted above, traditionalist approaches to just war theory can make use of collective entities and social goods to make sense of and evaluate the moral problems associated with privacy harms in war. "Descriptive individualism" seeks to root the analysis of just war theory in a world of individuals, and the doctrine holds that "wars, or other complex human interactions, are wholly reducible to the individual actions of which they are composed."[58] This is closely related to "evaluative individualism," which maintains that only individual well-being has moral significance, and that "groups and collectives either lack wellbeing entirely, or their wellbeing is morally unimportant."[59] Neither descriptive nor evaluative individualist views

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

of just war theory can fully account for the necessary balancing of social goods during wartime. As such, a descriptive individualist view fails to describe the social goods in balance, and an evaluative individualist view fails to describe the social benefits of privacy goods, as well as the deleterious effects of some kinds of privacy harms.

Individualist approaches to just war theory place significant epistemic burdens upon individuals, which cannot be excused by reference to collective entities. Current epistemic debates among just war scholars center on whether or not individuals are required to know if the war in which they are fighting is just. Though collectivist theories, such as that presented by Walzer in *Just and Unjust Wars*, do place strong epistemic duties upon individual combatants, they do not consider that one's lack of knowledge regarding the justice or injustice of the cause he or she serves matters, so long as that person abides by the *in bello* constraints on combatant action. This is the principle of the moral equality of combatants (MEC), that questions of *jus ad bellum* are "logically independent" from *jus in bello* considerations,[60]and therefore that "Unjust combatants do not do wrong merely by participating in an unjust war."[61]

In contrast, revisionist just war theorists such as Jeff McMahan hold that individuals do wrong when fighting in unjust wars. For McMahan, lack of knowledge or epistemic limitations may provide a subjective justification for wrongful action, but gives no objective permission for unjust combatants to kill, as such action is objectively wrong.[62] In McMahan's view, this has significant consequences: an individual "becomes a legitimate target in war by being to some degree morally responsible for an unjust threat, or for a wrong that provides a just cause for war."[63]

A key argument against McMahan's point about the epistemic duty of individuals is that these duties may be too burdensome for individuals or impossible for them to fulfill in practice.[64] As Walzer argues, McMahan provides "a careful and precise account of what individual responsibility in war would be like if war were a peacetime activity."[65] In Walzer's view, the inability of individuals to access such information forms part of a justification for collectivizing liability for harm, whereas McMahan argues that "soldiers must act on the basis of presumptions of liability. But these presumptions may vary from one context to another."[66]

Descriptive individualism cannot accurately account for privacy harms in war. This view seeks to provide a general account of morality in war, but holds that war

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

can be understood as a composite of individual actions. It therefore focuses attention on individuals to explain the morality of war without reference to collective phenomena. However, this focus comes at a cost. As Neta Crawford notes, the focus upon individual moral agency and responsibility blinds us to the importance of military organization in war, both as a corporate entity and as a means of structuring individual decision-making.[67] Privacy harms pose two further problems: First, it is likely to be practically impossible to connect individual privacy harms to a particular individual decision. The second issue is that descriptive individualism cannot readily account for social privacy harms. The kinds of social privacy harms inflicted through digital surveillance and data mining, for instance, cannot be reduced to the individual level of analysis. Commensurability is always an issue in moral theory, but here the problem is ontological: Descriptive individualism seeks to explain the morality of action in war through individual duties, rights, obligations, and harms. It is well equipped to analyze the actions of individual agents, but ill equipped to describe the agency of complex social systems, social processes, and social harms. For example, privacy harms can be caused by digital systems automatically capturing data,[68] and theorists argue that privacy harms can be inflicted even without active human agency.[69] Descriptive individualism, with its focus upon individual human agency, fails to describe these aspects of privacy harm.

Evaluative individualism holds that only individuals matter in war. As such, it cannot account for institutional responsibility for privacy violations, and neither can it readily incorporate the moral evaluation of social goods necessary for privacy balancing.[70] Because evaluative individualism is solely concerned with the well-being of individuals, privacy harms that are theorized to negatively affect communities or social groups fall outside its scope. Evaluative individualism is based on determining the rightfulness of individual acts, but to integrate the full sum of privacy harms into an act-centric analysis is, practically speaking, impossible due to the complexity of information processing itself. Since intelligence collection that is likely to generate privacy harms is an institutional process, an evaluative method that ignores institutional features cannot account for the context of war.[71] As Neta Crawford has noted in her criticism of approaches centered upon individual moral responsibility in war, these approaches ignore the fact that "military organizations both enable and constrain individual moral agency."[72] The importance of military institutions is that no individual agent in war is able to check the full process by which he or she is presented with a worldview prior to

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

each decision.[73] Individuals, therefore, are largely ignorant of the harms committed that permit them to act.

Further Problems with Privacy Harms in War

I have argued that reductivists and individualists cannot properly account for privacy violations and privacy harms in war. Any account of the morality of war that admits the importance of privacy harms must account for the idea that attitudes toward the social good of privacy vary between war and peace, as well as for the role of collective objects and goods in descriptive and evaluative terms. Privacy violations are part and parcel of war and warfare. But given that war involves the deliberate infliction of physical harm and death, should privacy harms be seen as lesser, or second-order, considerations? This section will explore the importance of privacy harms in practical terms.

What is clear from the analysis of war in both moral and practical terms is that information is generally regarded as an unbridled good. The more information available to those making lethal decisions, the better. There appears to be no rational case for choosing to remain uncertain or refusing to acquire more information about a situation should the opportunity arise. This attitude, which I will refer to as the "maximal" preference, conflicts with that found in the moral analysis of information in other circumstances.

The maximal attitude toward information collection is composed of two moral attitudes: One is that an agent has a duty to determine the likely outcome of an action prior to making a decision that has potentially harmful consequences. The second is that an agent has a duty to reduce the scope of uncertainty to the greatest extent possible prior to carrying out a potentially harmful action. Without consideration of privacy harms, it could seem that there is no harm that arises from collecting information and thus no reason to stop collecting information on moral grounds. This misleadingly permits us to discuss the moral rights and wrongs of warfare without addressing a key problem in contemporary war and warfare: the set of activities required to generate the information needed to conduct just military operations can often be inherently harmful. The maximal preference for information in wartime contrasts with privacy concerns in most other peacetime contexts. In times of peace, privacy concerns are paramount and discussion often centers upon the "minimal" preference of hewing to the smallest amount of information collection necessary to achieve a given aim in

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

order to minimize intrusions of privacy. Even the balancing of privacy goods against security goods in domestic settings trends toward restricting privacy violations to the minimum degree necessary.

Is unrestricted maximal information collection better than militaries balancing their intelligence collection, with respect to the potential harm to individual privacy rights? In other words, does a "privacy/targeting trade-off" make sense in the framework of just war theory? By this, I mean that by reducing harmful intelligence collection and information-processing activities, agents might increase the risk of wrongful uses of lethal force by misidentifying their targets, identifying civilians as combatants, or increasing risks to members of their own fighting forces. In practical terms, this means that even a traditionalist account of just war is likely to permit a wide range of privacy violations and privacy harms—both individual and social—as the cost of waging war in a just manner. But this harm can only be explained, at least by nonreductivists and institutionalists, with reference to a combatant's needs, and the needs of military institutions. If we think again of the Iraqi biometric data held by the U.S. military, when wars end, are militaries acting unethically if they retain data generated during those conflicts that constitutes an ongoing privacy harm?

Militaries are not the only institutions to encounter privacy problems during armed conflict. Humanitarian groups, among others, also collect large volumes of data; something that has become known as "surveillance humanitarianism," whereby individuals must submit to the collection of biometric data in order to receive humanitarian aid.[74] The humanitarian imperative is fundamentally different from just war theory, but we can see that a shared concern with privacy is a fast-emerging problem in both ways of evaluating the morality of action during war. Complicating matters is the fact that data gathered and generated for humanitarian purposes can be repurposed for military uses, and vice versa. For example, humanitarian organizations can draw data from military platforms such as drones to assess resource distribution,[75] and militaries can use humanitarian biometric data for targeting purposes. In a recent example, the Syrian government, in coordination with Russia, requested the coordinates of healthcare facilities in Syria, ostensibly in order to avoid harming healthcare workers. The UN obliged.[76] Both states had previously been accused, on good grounds, of deliberately targeting the healthcare infrastructure located in rebel areas.[77] Although voluntary, relief groups reported significant pressure from donors and UN officials to take part in the UN's deconfliction mechanism.[78] Significant numbers of healthcare facilities

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

were attacked, and a recent UN report found it "highly probable" that the government of Syria or its allies had carried out air strikes on some of the facilities.[79]

Information processing is a key frame for understanding the ethical relationships inherent in war and has clear ethical implications beyond the scope of this article, notably concerning what it means to participate in war and render oneself liable to attack. For example, one element of the ethical analysis of cyberattacks relevant to our present problem is the manner in which civilians are integrated, through private military companies or as contractors, into military or intelligence units conducting potentially harmful cyberattacks,[80] further blurring the line between combatant and noncombatant.[81] These civilians may then contribute to military operations via informational activity that can potentially justify physical violence in response.[82] We typically assess the contribution of civilians to a war effort through their physical work and activities, and there is, of course, considerable debate regarding the appropriate set of circumstances or factors that make a civilian liable for direct attack.[83] But a civilian's contribution to armed conflict can also be entirely informational in nature. Civilians who inform combatants or military forces of the positioning of other combatants can easily enable effective violence. This involvement can be intentional, or, as Stephen Deakin has explored, entirely unintentional, since civilians may stumble upon covert military forces, thus attaining knowledge that is inherently dangerous for said forces.[84] Intelligence collection and knowledge generation may be a state-centric activity, but digital information and communications technologies are enabling private individuals to perform activities loosely described as "open-source investigations," or open-source intelligence,[85] and are producing information that identifies war crimes and attributes responsibility to belligerents in contemporary armed conflict.[86] New techniques, such as using social media platforms to gather intelligence,[87] can also be used by researchers and private individuals. In short, the possibility of privacy harms is increasing across all aspects of daily life, and the context of war is no different.

The value of considering privacy in war lies not only in identifying new harms but also in bringing perspectives to bear that benefit just war theory. Just war theory's tripartite division into *jus ad bellum*, *jus in bello*, and *jus post bellum* serves as a good framework to evaluate the retention of data by militaries. As just war theory examines justice in the resort to war, its conduct, and the establishment of a just peace, so too we might consider explanations for privacy violations in the anticipation of conflict, during conflict, and following from

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

conflict. However, perspectives from work on privacy can highlight and account for specific harms within these contexts, such as those inherent in the reuse of humanitarian data for military purposes. Here, Nissenbaum's observation that "there are no arenas of life *not* governed by *norms of information flow*" highlights the role that normative ideas play in defining the privacy problems of reusable data.[88] The author's concept of "contextual integrity" can guide our understanding of why militaries should be wary of repurposing humanitarian data for targeting, and can also explain the way in which military necessity justifies the violation of contextual integrity in war. As she describes it, contextual integrity requires that two sets of informational norms are followed: "norms of appropriateness, and norms of flow or distribution."[89] For Nissenbaum, what is appropriate and how information should be shared or distributed are fundamentally related to social context. When either is violated, contextual integrity is destroyed. Thus, the appropriateness of data collection in war is defined by the social context of war itself. When war ends, the necessity for violation fades, and thus the harm of retaining data may outweigh the social benefit of retention. Equally, the sharing of information originally gathered for humanitarian ends with agents who seek to repurpose it for military targeting clearly violates both norms from a humanitarian perspective, even if it does not do so from a military perspective. In this sense, intelligence agencies and military institutions are serial context corruptors—their information-processing practices place little weight on the contextual integrity of information. At the same time, we can see that these organizations process information according to their own (security-focused) context. Blacklists,[90] terrorist watch lists,[91] and so-called kill lists[92] each have their own unique security context, even though they share an underlying method of information processing and evaluation. As such, an examination of privacy may better enable us to evaluate the information-processing interactions of combatants, militaries, and noncombatants in war.

Epistemic approaches to just war theory can also connect theoretical debates. For example, they connect debates about standards of required knowledge to the institutional processes that generate knowledge in war, and the technologies used in these processes. This is relevant to traditional discussions of command responsibility[93] and joint criminal enterprise,[94] which hinge upon information available to commanders. Key novel research areas regarding epistemology and war contend with the production of knowledge by computational methods, since digital information and communications technologies can produce knowledge that would otherwise be unavailable to human beings, but with the caveat

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

that this knowledge is inherently probabilistic.[95] The computational production of knowledge, and the way it is shaping human conceptual frameworks, is a central issue within the ongoing debate related to "meaningful human control" and the ethical challenges associated with autonomous weapons in armed conflict.[96] In almost any area of just war theory, asking how knowledge enables justifiable action in war poses important challenges that need to be addressed.

Conclusion

Just war theory has largely moved beyond the central question posed by James Turner Johnson in his book *Can Modern War Be Just?*,[97] since, aside from pacifists, the field as a whole seeks to interrogate how and why contemporary warfare can be waged in a just manner. Many of the issues raised in this article are features of modern wars and warfare. In wars where distinction is largely obvious, the kinds of intelligence collection described here is unnecessary. Similarly, when wars were fought by massed armies, individuals needed to rely less upon information provided by others, whereas individuals in contemporary military forces must trust in their peers and institutions for most of the knowledge that constitutes their worldview. The twin rise of privacy rights and war, understood in terms of the rights of individuals, means that just war theory must take account of privacy harms, particularly where they are necessary for the conduct of military operations in the first place.

NOTES

[1] Seth Lazar, "Just War Theory: Revisionists versus Traditionalists," *Annual Review of Political Science* 20, no. 1 (May 2017), pp. 37–54, at pp. 43–44, www.annualreviews.org/doi/10.1146/annurev-polisci-060314-112706.

[2] See, for example, Walzer's discussion of the morality of soldiers tossing grenades into cellars to clear them of potential threats. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 5th ed. (New York: Basic Books, 2015), pp. 135-136.

[3] Lazar, "Just War Theory," p. 39.

[4] See David Luban, "Liberalism, Torture, and the Ticking Bomb," *Virginia Law Review* 91, no. 6 (October 2005), pp. 1425–61.

[5] Cian O'Driscoll, *The Renegotiation of the Just War Tradition and the Right to War in the Twenty-First Century* (New York: Palgrave MacMillan US, 2008).

[6] See, for example, Cécile Fabre, "Guns, Food, and Liability to Attack in War," *Ethics* 120, no. 1 (October 2009), pp. 36–63, www.journals.uchicago.edu/doi/10.1086/649218.

[7] Here I use Lazar's typology for the state of the field. See Lazar, "Just War Theory."

[8] Holly M. Smith, "The Subjective Moral Duty to Inform Oneself before Acting," *Ethics* 125, no. 1 (October 2014), pp. 11–38, at p. 13.

[9] Toni Pfanner, "Military Uniforms and the Law of War," *International Review of the Red Cross* 86, no. 853 (March 2004), pp. 93–130, www.cambridge.org/core/journals/international-review-of-the-red-cross/article/military-uniforms-and-the-law-of-war/FD791E3767A799582919AE709E1E136D.

[10] See, for example, Matthias Gross and Linsey McGoey, eds., *Routledge International Handbook of Ignorance Studies* (London: Routledge, 2015).

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

[11] Neta C. Crawford, *Accountability for Killing: Moral Responsibility for Collateral Damage in America's Post-9/11 Wars* (Oxford: Oxford University Press, 2013), pp. 314–17.

[12] Ikujiro Nonaka and Ryoko Toyama, "The Knowledge-Creating Theory Revisited: Knowledge Creation as a Synthesizing Process," in John S. Edwards, ed., *The Essentials of Knowledge Management* (London: Palgrave MacMillan, 2015), pp. 95–110.

[13] Mai'a K. Davis Cross, "Rethinking Epistemic Communities Twenty Years Later," *Review of International Studies* 39, no. 1 (January 2013), pp. 137–60, www.cambridge.org/core/journals/review-of-international-studies/article/rethinking-epistemic-communities-twenty-years-later-/C7057E942EAFAED773470752746F8454.

[14] Jack McDonald, *Enemies Known and Unknown: Targeted Killings in America's Transnational Wars* (New York: Oxford University Press, 2017).

[15] Astrid H. M. Nordin and Dan Öberg, "Targeting the Ontology of War: From Clausewitz to Baudrillard," *Millennium* 43, no. 2 (January 2015), pp. 392–410, journals.sagepub.com/doi/10.1177/0305829814552435.

[16] Antoine Bousquet, *The Eye of War: Military Perception from the Telescope to the Drone* (Minneapolis: University of Minnesota Press, 2018).

[17] Anya Topolski, "Relationality: An Ethical Response to the Tensions of Network-Enabled Operations in the Kunduz Air Strikes," *Journal of Military Ethics* 13, no. 2 (April 2014), pp. 158–73, at p. 162, www.tandfonline.com/doi/abs/10.1080/15027570.2014.944360.

[18] Crawford, *Accountability for Killing*, p. 315.

[19] Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Cambridge, U.K.: Polity, 1990).

[20] Eli Berman, Joseph H. Felter, Jacob N. Shapiro, and Vestal McIntyre, *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton, N.J.: Princeton University Press, 2018).

[21] Roberto Vezzani, Davide Baltieri, and Rita Cucchiara, "People Reidentification in Surveillance and Forensics: A Survey," *ACM Computing Surveys* 46, no. 2 (December 2013), pp. 29:1–37, dl.acm.org/doi/10.1145/2543581.2543596.

[22] Noah Schachtman, "Iraq Diary: Fallujah's Biometric Gates (Updated)," *WIRED*, August 31, 2007, www.wired.com/2007/08/fallujah-pics/.

[23] David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, Conn.: Greenwood, 2006).

[24] Marc Rotenberg, Simon Davies, and Ken Roth to Robert M. Gates, July 27, 2007, Electronic Privacy Information Center, epic.org/privacy/biometrics/epic_iraq_dtbs.pdf.

[25] Noah Schachtman, "Iraq's Biometric Database Could Become 'Hit List': Army," *WIRED*, August 15, 2007, www.wired.com/2007/08/also-two-thirds/.

[26] Spencer Ackerman, "US Holds on to Biometric Database of 3 Million Iraqis," "Danger Room" blog, *WIRED*, December 21, 2011.

[27] Dorothy J. Glancy, "The Invention of the Right to Privacy," *Arizona Law Review* 21, no. 1 (January 1979), p. 1.

[28] Philip E. Agre, "Surveillance and Capture: Two Models of Privacy," *Information Society* 10, no. 2 (1994), pp. 101–27, at p. 101, www.tandfonline.com/doi/abs/10.1080/01972243.1994.9960162.

[29] Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), p. 171.

[30] Ibid., p. 174; and Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (May 2004), pp. 119–58, at p. 417.

[31] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 1890), pp. 193–220, at p. 193, www.jstor.org/stable/1321160.

[32] Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (February 2005), pp. 477–560.

[33] Solove, *Understanding Privacy*, p. 172.

[34] Martin Kuhn, *Federal Dataveillance: Implications for Constitutional Privacy Protections* (LFB Scholarly Publishing, 2007), pp. 11–23.

[35] Nissenbaum, "Privacy as Contextual Integrity," p. 125.

[36] Solove, *Understanding Privacy*, p. 173.

[37] Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," *Harvard Civil Rights-Civil Liberties Law Review* 43, no. 2 (June 2008), pp. 435–89, at p. 484.

[38] Solove, *Understanding Privacy*, pp. 173–74.

[39] Roger Clarke, "Risks Inherent in the Digital Surveillance Economy: A Research Agenda," *Journal of Information Technology* 34, no. 1 (March 2019), pp. 59–80, at p. 67, journals.sagepub.com/doi/10.1177/0268396218815559.

[40] Roger Clarke, "Information Technology and Dataveillance," *Communications of the ACM* 31, no. 5 (May 1988), pp. 498–512, at p. 499, dl.acm.org/doi/10.1145/42411.42413.

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

[41] Clarke, "Risks Inherent in the Digital Surveillance Economy."

[42] A. Michael Froomkin, "The Death of Privacy?," *Stanford Law Review* 52(5) May 2000, pp. 1461–1543, at p. 1464.

[43] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age," *Harvard International Law Journal* 56, no. 1 (Winter 2015), pp. 81–146.

[44] Peter Margulies, "Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights," *Florida Law Review* 68, no. 4 (July 2016), pp. 1045–1117, at p. 1082.

[45] Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 2000).

[46] Margulies, "Surveillance by Algorithm," pp. 1090–91.

[47] Daniel J. Steinbock, "Designating the Dangerous: From Blacklists to Watch Lists," *Seattle University Law Review* 30, no. 1 (2006), pp. 65–118, at p. 67.

[48] Lazar, "Just War Theory," p. 40.

[49] Ibid., p. 40.

[50] Seth Lazar, "Evaluating the Revisionist Critique of Just War Theory," *Daedalus* 146, no. 1 (Winter 2017), pp. 113–24.

[51] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 5th ed. (New York: Basic Books, 2015), pp. 42–43.

[52] Lazar, "Just War Theory," p. 47.

[53] Kenneth Watkin, "Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict," *American Journal of International Law* 98, no. 1 (January 2004), pp. 1–34, www.jstor.org/stable/3139252.

[54] Anja Lindroos, "Addressing Norm Conflicts in a Fragmented Legal System: The Doctrine of Lex Specialis," *Nordic Journal of International Law* 74, no. 1 (January 2005), pp. 27–66, brill.com/view/journals/nord/74/1/article-p27_3.xml.

[55] In international law, this relates to the interaction between international humanitarian law and international human rights law. See Cordula Droege, "The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict," *Israel Law Review* 40, no. 2 (Summer 2007), pp. 310–55, www.cambridge.org/core/journals/israel-law-review/article/interplay-between-international-humanitarian-law-and-international-human-rights-law-in-situations-of-armed-conflict/05B4E379B7FD1F8B2BFC57958FB901EE.

[56] Tarak Barkawi and Shane Brighton, "Powers of War: Fighting, Knowledge, and Critique," *International Political Sociology* 5, no. 2 (June 2011), pp. 126–43, at p. 137, academic.oup.com/ips/article-abstract/5/2/126/1941280?redirectedFrom=fulltext.

[57] Lazar, "Just War Theory," p. 40.

[58] Seth Lazar, "Method in the Morality of War," in Helen Frowe and Seth Lazar, eds., *The Oxford Handbook of Ethics of War* (Oxford University Press, 2018), p. 33.

[59] Ibid., p. 33.

[60] Walzer, *Just and Unjust Wars*, p. 21.

[61] Jeff McMahan, "The Ethics of Killing in War," *Philosophia* 34, no. 1 (January 2006), pp. 23–41, at p. 24, link.springer.com/article/10.1007/s11406-006-9007-y.

[62] Jeff McMahan, *Killing in War* (New York: Oxford University Press, 2009), pp. 60–70.

[63] Jeff McMahan, "The Ethics of Killing in War," p. 34.

[64] Seth Lazar, "The Responsibility Dilemma for *Killing in War*: A Review Essay," *Philosophy & Public Affairs* 38, no. 2 (Spring 2010), pp. 180–213, at pp. 193–96.

[65] Michael Walzer, "Response to McMahan's Paper," *Philosophia* 34, no. 1 (January 2006), pp. 43–45, at p. 43, link.springer.com/article/10.1007/s11406-006-9008-x.

[66] Jeff McMahan, "Killing in War: A Reply to Walzer," *Philosophia* 34, no. 1 (January 2006), pp. 47–51, at p. 48, link.springer.com/article/10.1007%2Fs11406-006-9009-9.

[67] Crawford, *Accountability for Killing*, pp. 6–10.

[68] Agre, "Surveillance and Capture."

[69] M. Ryan Calo, "The Boundaries of Privacy Harm," *Indiana Law Journal* 86, no. 3 (2011), pp. 1131–62.

[70] Lazar, "Just War Theory," p. 40.

[71] Crawford, *Accountability for Killing*, p. 246.

[72] Ibid., p. 467.

[73] Henry Shue, "Laws of War, Morality, and International Politics: Compliance, Stringency, and Limits," *Leiden Journal of International Law* 26, no. 2 (June 2013), pp. 271–92, at p. 275, www.cambridge.org/core/journals/leiden-journal-of-international-law/article/laws-of-war-morality-and-international-politics-compliance-stringency-and-limits/D947C80157BDC7E4B44FDA5B098D9B72.

[74] Mark Latonero, "Stop Surveillance Humanitarianism: Requiring Biometric Data, like Iris and Facial Scans, Sets a Dangerous Precedent for Vital Aid," Opinion, *New York Times*, July 11, 2019, www.

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html; and Gus Hosein and Carly Nyst, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries* (London: Privacy International, October 2013), www.privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf

[75] John R. Emery, "The Possibilities and Pitfalls of Humanitarian Drones," *Ethics & International Affairs* 30, no. 2 (Summer 2016), pp. 153–65, www.cambridge.org/core/journals/ethics-and-international-affairs/article/possibilities-and-pitfalls-of-humanitarian-drones/1509D6D202FCAE3EAFDEE68B7811F86C.

[76] Josie Ensor, "UN Under Fire for Giving Russia Coordinates of Syrian Hospitals in 'High-Risk' Strategy to Stop Attacks," *Telegraph*, March 24, 2018, www.telegraph.co.uk/news/2018/03/24/un-fire-giving-russia-coordinates-syrian-hospitals-high-risk/.

[77] Samer Jabbour, Fouad M. Fouad, Jennifer Leaning, Donna McKay, Rabie Nasser, Leonard S. Rubenstein, Annie Sparrow, et al., "Death and Suffering in Eastern Ghouta, Syria: A Call for Action to Protect Civilians and Health Care," *Lancet* 391, no. 10123 (March 2018), pp. 815–17, www.thelancet.com/journals/lancet/article/PIIS0140-6736(18)30527-0/fulltext.

[78] Evan Hill and Whitney Hurst, "The U.N. Tried to Save Hospitals in Syria. It Didn't Work," *New York Times*, December 29, 2019, www.nytimes.com/2019/12/29/world/middleeast/united-nations-syria-russia.html.

[79] UN Board of Inquiry, quoted in "Syria: Warring Parties Failed to Abide by International Law over Hospital Attacks," UN News, United Nations, April 6, 2020, news.un.org/en/story/2020/04/1061192.

[80] Ross W. Bellaby, "Justifying Cyber-Intelligence?," *Journal of Military Ethics* 15, no. 4 (2016), pp. 299–319, www.tandfonline.com/doi/full/10.1080/15027570.2017.1284463.

[81] Edward T. Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," *Journal of Military Ethics* 12, no. 1 (2013), pp. 4–17, www.tandfonline.com/doi/abs/10.1080/15027570.2013.782633.

[82] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010), pp. 384–410, www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404.

[83] See, e.g., Fabre, "Guns, Food, and Liability to Attack in War"; and Helen Frowe, ch. 6 in *Defensive Killing* (Oxford: Oxford University Press, 2014).

[84] Stephen Deakin, "Wise Men and Shepherds: A Case for Taking Non-Lethal Action against Civilians Who Discover Hiding Soldiers," *Journal of Military Ethics* 10, no. 2 (June 2011), pp. 110–19, www.tandfonline.com/doi/abs/10.1080/15027570.2011.593713.

[85] Patrick Meier, "Crisis Mapping in Action: How Open Source Software and Global Volunteer Networks Are Changing the World, One Map at a Time," *Journal of Map & Geography Libraries* 8, no. 2 (May 2012), pp. 89–100, www.tandfonline.com/doi/abs/10.1080/15420353.2012.663739.

[86] Keith Hiatt, "Open Source Evidence on Trial," Forum, *Yale Law Journal* 125 (2016), pp. 323–30, www.yalelawjournal.org/forum/open-source-evidence-on-trial.

[87] Sir David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security* 27, no. 6 (December 2012), pp. 801–23, www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965.

[88] Nissenbaum, "Privacy as Contextual Integrity," p. 119.

[89] Ibid., p. 119.

[90] Steinbock, "Designating the Dangerous."

[91] Jeffrey Kahn, "Terrorist Watchlists," in David Gray and Stephen E. Henderson, eds., *The Cambridge Handbook of Surveillance Law* (Cambridge, U.K.: Cambridge University Press, 2017), pp. 71–100.

[92] Marieke de Goede and Gavin Sullivan, "The Politics of Security Lists," *Environment and Planning D: Society and Space* 34, no. 1 (February 2016), pp. 67–88, journals.sagepub.com/doi/10.1177/0263775815599309.

[93] Michael L. Smidt, "Yamashita, Medina, and Beyond: Command Responsibility in Contemporary Military Operations," *Military Law Review* 164 (June 2000), pp. 155–234.

[94] Allison Marston Danner and Jenny S. Martinez, "Guilty Associations: Joint Criminal Enterprise, Command Responsibility, and the Development of International Criminal Law," *California Law Review* 93, no. 1 (January 2005), pp. 75–169.

[95] Claudia Aradau and Tobias Blanke, "The (Big) Data-Security Assemblage: Knowledge and Critique," *Big Data & Society* 2, no. 2 (December 2015), journals.sagepub.com/doi/10.1177/2053951715609066.

[96] Heather M. Roff, "The Strategic Robot Problem: Lethal Autonomous Weapons in War," *Journal of Military Ethics* 13, no. 3 (2014), pp. 211–27, tandfonline.com/doi/abs/10.1080/15027570.2014.975010.

[97] James Turner Johnson, *Can Modern War Be Just?* (New Haven, Conn.: Yale University Press, 1986).

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press

Abstract: Are the sources of a combatant's knowledge in war morally relevant? This article argues that privacy is relevant to just war theory in that it draws attention to privacy harms associated with the conduct of war. Since we cannot assume that information is made available to combatants in a morally neutral manner, we must therefore interrogate the relationship between privacy harms and the acts that they enable in war. Here, I argue that there is ample evidence that we cannot discount the analysis of privacy harms in war, and that analysis of such harms requires us to examine social goods. I develop this point to demonstrate the problems that this poses for aspects of revisionist just war theory; namely, reductivism and individualism. In order to evaluate the moral consequences of privacy harms in war, we must understand the unilateral and adversarial character of balancing privacy harms against social goods in the context of war, which, in turn, requires that we consider social goods and social institutions as objects of moral evaluation. Further, concepts drawn from privacy scholarship, such as Helen Nissenbaum's concept of contextual integrity, enable us to identify a range of moral problems associated with contemporary war that deserve further attention from just war theorists.

Keywords: just war theory, privacy, ethics, surveillance, intelligence ethics, technology

https://doi.org/10.1017/S0892679420000477 Published online by Cambridge University Press