Redefining the security paradigm to create an intelligence ethic

Ross W Bellaby

Published online: 15 May 2022.

Submit your article to this journal ⓒ

Article views: 498

View related articles ⓒ

View Crossmark data ⓒ

Routledge
Taylor & Francis Group

Redefining the security paradigm to create an intelligence ethic

Ross W Bellaby

ABSTRACT

This paper argues that before any detailed ethical framework can be created the conceptualisation of the relationship between fundamental human rights and the ethical purpose of intelligence needs to be reconceived. That is, rather than intelligence being considered to exist in opposition to our rights, where one is balanced or traded against the other, it is ethical when it is used as a process to protect and provide for all of our most vital interests, and not prioritising one at the cost of another.

Introduction

In the first instance, there can be some significant resistance to developing any overly explicit, and for some limiting, ethical expectations for intelligence. As Allen Dulles, once the head of the United States Central Intelligence Agency (CIA) and principal intelligence advisor to the President and the National Security Council, argued in 1963, 'The last thing we can afford to do today is to put our intelligence in chains'.[1] The concerns are that any ethical limits will automatically place undue restraints of an activity whose purpose is to provide timely information on threats to people's lives. There those who therefore argue that intelligence should not be subjected to an ethical framework that dictates what activities are acceptable for it would just hinder its practice. Or there are those that argue that any project that aims to apply ethics to intelligence is oxymoronic.[2] The job of intelligence in many instances is to collect information that other actors would wish to keep secret. Intelligence, by necessity, is an unsavoury business. Intelligence 'carries an ethical baggage with it or – to be more accurate – a baggage of unworthiness'.[3] The argument, therefore, is that it is both unhelpful and redundant to attempt to apply ethical considerations to a field such as this. As a *New York Times* reporter put it, 'is there such a thing as an ethical spy?'[4]

However, by claiming that intelligence is an activity that is inherently unethical and so should exist outside the realm of ethical discourse lest the activity be banned outright, it is to ignore the important role that ethics plays in the life of the individual and the political community, as well as the ethical role that intelligence itself can play. This means, first, recognising the fact that intelligence cannot exist outside the purview of ethical evaluation. No activity can. Moreover, it ignores that intelligence does play an important ethical role through its capacity to protect people from harm. Secret intelligence is still needed and depended upon, a dependency that is currently driven by the emergence of diverse and asymmetric threats from international terrorist networks and sub-state actors, as well as the various already established threats, including domestic crime and social unrest, state actors, foreign espionage and international instability. The challenge is how national security and intelligence are conceptualised and the implications this has for ethical evaluation.

Indeed, intelligence as a practice, culture and product instantly offers up some key challenges when it comes to establishing an ethical framework, the first of which is understanding how intelligence is conceptualised in its position in society. It is the role of state intelligence actors to safeguard and maintain the state's national security by detecting, locating and preventing threats,

CONTACT Ross W Bellaby ✉ r.bellaby@sheffield.ac.uk

including threats from 'espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means'.[5] Intelligence exists in the realm of preventing serious harm to the state's key interests in order to provide for the welfare of its political community. As a result, intelligence is very much seen as a key part of 'national security', existing in this prioritised realm and possessing a near supreme emergency culture where it constantly battles to prevent a catastrophic threat from being realised.[6]

As such intelligence is very much seen as quintessentially a topic of *realpolitik*,[7] a key area of security best left to the realm of 'high politics', where it is considered inherently vital to the survival of the state. As such, it represents a clear example of securitization where it is raised out of the political realm and placed in the extraordinary security sphere where normal political rules and limitations are not given the same consideration and weight. This positions intelligence within the realm where imminent threats and supreme emergencies heightens the pressure to act and lowers the ethical threshold; the language becomes one of division between an internal 'us' and the threatening 'them'; and it drives the state to present itself like it is providing an active form of security and returning results. On the one hand, this positioning of intelligence is not surprising or necessarily incorrect. Intelligence as a practice is charged with locating and preventing very dangerous threats to both individual lives and the interests of the community across their economic, political, and social needs. However, this extraordinary framing has important implications on how intelligence is understood as a practice and creates a reluctance to apply some forms of ethical oversight on its behaviour. This framing of intelligence as being in a constant state of emergency prevention is one that emerged throughout the Cold War and has continued under the War on Terror, and reflects a resurgence in Lasswell's 'garrison state' as the prioritisation of a security mind-set that privileges a militaristic culture and policy imperatives over other concerns.[8] Matched by Cass Sustein's growth in a risk culture, this distorts how threats such as terrorism are perceived, overemphasising their imminence, pervasiveness and likely destructive force.[9] This results in a society where the prevention of threats is prioritised over the provision of goods and can drive an escalation of security policy.[10] Such mentality perpetuates a feeling that any restrictions on intelligence – ethical, legal or a culture of transparency for example – are likely to limit its effectiveness and result in imminent harm to people.

This has shaped how we understand, approach and deal with intelligence, placing it above in terms of importance and precedence than those needs of the political sphere. The result of this is that it has limited the type of ethical debates and legal restrictions that are normally placed on both state and individual behaviour. This positioning of intelligence in society, however, is premised on security, as defined in the UK Security Service Act 1989, 'the protection of national security and in particular its protection against threats such as terrorism, espionage and sabotage, the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means'.[11] At its core of national security is the prioritisation of physical safety from violent threats. Therefore, before we can develop the necessary ethical tools to guide intelligence activity, this article will argue that we need to reframe security as the means by which of all an individual's most fundamental vital interests – often articulated through core human rights – are provided for and protected, and not just focusing on the physical interest one has in protecting their body and life.[12] This also means rather than intelligence and rights being placed in opposition to each other – where intelligence and security are balanced against rights and where one is lost for the benefit of the other – security should be conceived as the means by which these rights are protected. Security should concern itself with the overall complex relationship between our vital interests in terms of how it should provide and protect them. As a result, it should be recognised that intelligence can both violate and protect these vital interests and so can be both a threat to and provider of security. Ethical intelligence requires a flexible reconciliation process that examines the way our vital interests are impacted and interrelate to determine when intelligence should be limited or licenced.

Furthermore, intelligence as a term and concept covers a varied set of activities that makes examining it holistically and comparatively very difficult. For example, the often discussed 'collection' phase of intelligence ranges in its practices, from individual and *en masse* surveillance, to manipulating a source through bribery, blackmail or exploiting an individual's weaknesses, to data-mining and dataveillance. While the lesser seen parts of intelligence such as analysis, counter-intelligence, covert and paramilitary operations, and policy development, equally raise very different, and sometimes very specific, ethical questions and concerns which need to be addressed. This makes developing a single framework for evaluating 'intelligence' especially difficult.[13] In addition, there is the temporal challenge of not knowing if target is a legitimate one until you have carried out potentially unethical operations against them. This means that the ethical calculation one makes must recognise and compensate for the prospect of treating someone like a threat before they have shown themselves to be one.

To resolve these issues, this article will argue that by conceptualising security as the provision of our vital interests, it is possible to create an encompassing framework that can detail the harm intelligence activities can cause, and then spread the harms across a spectrum, so we can also develop an escalating and proportional set of responses. By taking this proportional evaluation route, the temporal challenges can be resolved as the less harmful activities can be utilised to justify the target as legitimate for the more harmful ones.

Reconceptualising security

At the centre of these problems is a narrow conceptualisation of security, one that prioritises securing our physical form from damage, pain or death, as well as a heightened fear around national security infrastructure and an obsessive need for secrecy. While security is another one of those 'promiscuous concepts'[14] – ranging in content, referent object and means of provision[15] – it will be argued that the value of security, and therefore the right or expectation to have security, is directly linked to the value that individuals have in maintaining their vital interests.[16] That is, security is the condition by which one's vital interests are maintained and protected, and so should be seen as the processes and protections designed to maintain all of a person's vital interests. These vital interests are those requirements that Joel Feinberg calls our 'welfare interests' and John Rawls refers to as 'primary goods': essential preconditions that are needed regardless of what conception of the good life the individual holds or what their life plans might be in detail.[17] These interests are the most important a person has and thus cry out for protection. These include the interest in physical and mental integrity, autonomy, liberty and privacy.

For example, at its core, the vital interest in maintaining one's physical integrity gives rise to the understanding of security as personal safety, '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'.[18] In addition to this, however, security should also include the vital interest people have in their privacy, creating the protections one needs, both physically and symbolically, that prevent outsiders (including the state) from intruding on private spaces or accessing personal information without authorisation. While the interest in autonomy creates the need for protections against manipulation and coercion and promotes the need for individuals to be free-thinking and sufficiently informed in both their personal and political life.

Security, therefore, is the condition by which all of one's vital interests are maintained and protected. Security is 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. This involves both limiting and licensing the power of the state, something expressed through the social contract that outlines the agreement of rational individuals to sacrifice some of their freedoms in return for the state's duty to protect their vital interests. Through public deliberation and debate these various vital interests are negotiated between people within

a political community, holding the state to account in both its own coercive power over the population as well as in terms of its obligation to provide the necessary security.[19] This relationship and the limit/licensing power of state can manifest in terms of human rights legislation, which enable individuals to hold the state to account and its duty to secure those conditions.

Importantly, this security conceptualisation alters the way in which the relationship between civil liberties and security is understood or discussed. For example, the narratives that surround intelligence are that liberties must be traded away in order to be successful; that you can either have security or you can have your civil liberties, but you cannot have both.[20] Such narratives are either framed as a balancing exercise, where a more perfect mid-point between levels of civil liberties and security powers are ever sought and moved, or as a trade-off where one must sacrifice one if we are to have the other.[21] The impact of such narratives is such 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'.[22] One trade-off often discussed is that between privacy and security, where the dichotomy presented is such that you can have either security or privacy and, importantly, where security is seen to be a trump card that overrides other concerns.[23] This is a particular framing that has always been part of the rhetoric that surrounds the debate on security and human rights, but came into stark contrast in the wake of the 9/11 attacks and was one that was propelled into the public narrative following the Snowden leaks.[24] While Jeremy Waldron warns that even if such a framing was correct, it would be problematic in terms of unequal distribution of the trade-off as the impact is often disproportionately felt by minorities within a community, with unclear returns for any given trade-off and the problem of trading liberties at will, even thinking about it in terms of a trade is incorrect. That is, this positions human rights and security as opposing entities. Rather, security should be reconceptualised as the means by which all the vital interests are provided for and so talk about providing security is to talk about how one is to provide the best conditions for ensuring these vital interests. Indeed, this is closer to the sentiment outlined in the President's Review Group on Intelligence and Communications Technologies, which noted that while the word 'security' often refers to national or homeland security, it should include those ethical norms vital for 'people to be secure in their persons'.[25] This means taking a much more holistic approach to security, recognising all the different vital interests, how they interact and the way in which protecting one can impact on the others.

What this means for national security is that it has value in terms of protecting the individual's vital interests as well as the health of the political community as an important means through which the individual enacts or realises both vital and further interests. As Adam Moore argues, 'we value national security, not because some specific political union is valuable in itself, but because it is a necessary part of protecting individual rights'.[26] The value of the state, and the need for national security, is therefore drawn from the value of those individuals it is charged with protecting: 'whatever rights and privileges states have, they have them only in so far as they thereby serve individuals' fundamental interests'.[27] Indeed, the ethical value found within intelligence activity comes from their role in protecting the individual and the political community and this end shapes what activities they can justly carry out.[28] Therefore, it is necessary to understand the impact that any intelligence practice or policy can have on our vital interests and determine if they are justified in light of the vital interests it seeks to protect. What this means for intelligence is that any ethical framework developed should take into account the various types and forms our vital interests can take and how they interact, working to reconcile the vital interests while not necessarily prioritising one over the other.

Secrets and secrecy

This conceptualisation of security is made more problematic by the inherent pervasive and obsessive need for secrecy found within the intelligence community. Indeed, intelligence comes with an inherent expectation of absolute secrecy across all it does.[29] This need for secrecy in turn creates

an internal culture that separates the intelligence community from the rest of the political sphere, and feeds upon itself to foster a need for hyper-secrecy. On the one hand, this is not only under-standable but also completely necessary in terms of maintaining the essential aspect of 'secret' intelligence. This is not a call for complete transparency. Secrecy does play an important role in facilitating the intelligence community's ability to protect both the individual and the political community. Without the intelligence community being able to keep tactics and the information it produces secret to some extent, intelligence would be dramatically weakened. However, it also needs recognising that overly secretive environments or cultures that are placed above or outside the normal political sphere isolate their members and their structures, separating them from those on the outside who are unaware and unable to engage, and so not able to act as a counter and reference point to the internal cultures and escalation. Those on the inside are subjected to a process of in-group/out-group differentiation that dehumanises 'others' and when coupled with a lack of outside input means there is no means of measuring one's moral compass.[30] As a result, officers learn to exclude those considered as outsiders from their universe of obligation.[31] Cognitive restructuring means violence or harm is redefined as honourable, for a greater abstract good, and becomes increasingly socially and morally acceptable to those inside.[32] Secretive environments normalise this process, feeding upon itself to reinforce both the need for greater secrecy and a lack of regard for the negative consequences for those on the outside. In such an environment internal criticism is limited as it is seen as a betrayal to the group and so restricts alternative analysis as group-mentality smothers dissenting points of view.[33]

The insular atmosphere skews one's ability to evaluate one's activity. Indeed, Hannah Arendt highlighted how the mandate to try and protect the political community from threats and to seek to fulfil that objective actually encourages them to move further from that ethical end.[34] It is not that those within the intelligence community and their authorising political actors are necessarily acting according to some private or nefarious agenda. But rather that the prioritising of a narrow con-ceptualisation of security coupled with a secretive and isolated culture can result in activities being disconnected from the actual interests or needs of those it seeks to protect. This can distort intelligence policy application, promoting distrust not only between individuals and the state but also between different social groups, having real repercussions for individuals in terms of social mobility and treatment.[35] The security misconception heightens the desire for secrecy as it creates a false binary where, as Dennis Thompson notes, you are essentially left with two options, 'abandon the [security] policy or sacrifice democratic accountability'[36]; and importantly a decision where national security is all important. In terms of intelligence, this can result in tactics far harsher than was originally planned, including escalating interrogation techniques, increasingly intrusive collec-tion methods, or unequal treatment based on race or ethnicity.

This is further compounded by a relatively passive set of oversight mechanisms.[37] In a system of checks and balances, there has developed an ethos of authorising or rejecting the activity at the point of asking for permission or at established times. For example, the legislative's power over the intelligence community is mainly limited to the power of the purse or carrying out investigations after the scandal has been revealed.[38] Or in terms of the executive or judiciary, intelligence actors are meant to approach them for authorisation, with surveillance warrant requests being the most notable example of this.[39] This has, however, proven highly problematic because it is wholly too passive for the intelligence community and its inherently closed-off nature. Waiting for intelligence actors to bring issues for authorisation means that there is virtually no investigation into what they are doing otherwise, meaning that too much power rests with them to decide what, if and when to bring it forward. Moreover, the executive oversight system is not positioned in opposition to the intelligence community, acting in a penetrating manner. But they are selectively brought into the exulted sphere of secrecy and placed within the same security mentality and culture. The sphere of secrecy is extended out to include those who are meant to be keeping an eye on the watchmen and in doing so they become habitualised.

The reconciliation process

By reconceptualising security as the means by which all our vital interests are provided for and protected, it is possible to better understand when intelligence is justified as a means of protection, as well as when it is prohibited as an unjustified violation. Making this reconciliation process means recognising that all our vital interests – whether physical integrity or privacy and autonomy – are important, but not absolute and can exist in different forms and with different levels of protection. Evaluations must be made on the type and level of violation represented in a set of intelligence activities with ethical judgements being carried out in relation to the surrounding circumstances and the type of threat predicted, its potential impact and the likelihood of it being realised. The security of the individual and the society they are in can be examined in terms of how infringements on vital interests such as liberty and privacy are justified in terms of protecting other vital interests, such as physical integrity; or how violating the privacy of a few specific targets can provide for greater autonomy of many others.

As a process, this means, first, recognising that while some vital interests such as physical and mental integrity might appear to take precedence over the other interests such as autonomy, liberty, or privacy, this is not necessarily always the case and they should be taken together as a complex matrix that all need to be maintained. Significantly, vital interests make a chain whereby the whole chain is no stronger than its weakest link.[40] Indeed, an excess of one will not necessarily make up for the lack of another interest: an excess of physical security cannot be used as a justification for undermining people's privacy; a general argument cannot be made that people are physically very safe in exchange for having no privacy.

Secondly, 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). That is, depending on the context the 'severity' of the violation needs to be taken into account. This can include the longevity of the violation, its level of impact, the number of people it impacts, whether there are secondary or additional side effects or harms caused, if it is systematic or a one off, and the ability of people to consent. All these factors need to be examined as a complex whole, both in terms of the harm caused by the intelligence activity and the harm it seeks to prevent. This means that a prick on the finger is not considered more harmful than being incarcerated just because it is a physical violation as compared to a violation of liberty.

Therefore, the severity of the violation helps us understand the specific level of harm caused. 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 and the greater the harm caused when violated.[41] Therefore, there must be a greater threat to someone's other vital interests to justify the privacy intervention. Finally, in making this negotiation it needs to be understood whether the target has acted in some way to waive or forfeit their immediate vital interest protects; if there is a threat to the vital interests of another to a greater degree or in a more fundamental way; and that people's vital interests being provided for to a minimum standard. For instance, people lose or waive their right to liberty when they represent a threat to another's vital interests or the integrity of the political community as a whole.

Spectrum, reflexivity and a temporal paradox

By understanding the different ways and levels that intelligence can both impact and protect people, and that it is not a trade-off between rights and security, nor even a balancing act, but a reconciliation process, it is possible to also resolve the temporal challenge of how to justify an intelligence activity before there is a sufficient known threat to act as the justification in the first instance. That is, it is possible to think of intelligence as a form of proportional 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'.[42] For example, pre-emptive self-defence counters threats that, while not realised, 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 materialise. By understanding these distinctions, self-defence can be conceived as a spectrum in terms of threat likelihood and temporal distance, which can justify different types of intelligence activities. That is, the more known the threat is, the closer it is or the more concrete the evidence on the threat, the greater the justification there is for a more impactful form of intelligence. This type of distinction is important because intelligence does not exist in the same temporal immediacy of defending oneself against an imminent blow. But 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 use this information to either escalate up through more harmful intelligence activities or by abandoning the target.

What this means is a proportional approach to intelligence needs to be taken, which includes using what is knowable through non-harmful means to detail the level of threat and the degree to which it is reasonable to assume the threat is real. That is, in order for intelligence agencies to collect information there first must be some evidence present so as to provide a justification for setting out to collect intelligence. So, there must be a spectrum or graduation in terms of a response. For example, for those activities that cause a low level of harm, there only has to be a low level of evidence to act as a justification, whereas for those activities that cause a high level of harm there must be a greater level of evidence. This notion of levels of evidence is itself nothing new. Various legal systems mark out levels of evidence, or 'burdens of proof', which are required when assessing whether certain actions are permissible or not. Legal canons mark a distinction between a *reasonable suspicion*, a *probable cause*, a *balance of probabilities, clear evidence*, and *beyond any reasonable doubt*, whereby depending on the circumstances, the level of proof required changes. For example, reasonable suspicion is a low standard of proof often required to determine whether a brief investigative stop or search by a police officer or any government agent is warranted. For anything that is more 'intrusive', to detain someone, for example, a higher burden of proof must be provided, for instance a probable cause. These different levels of probability provide, what Polyvious Polyviou calls, the 'best compromise' between two often opposing interests, 'the intrusions upon the individual and the security of the state'.[43] This notion is compatible with intelligence collection. Intelligence is essentially a calculation of probabilities and possibilities about activities that it is not meant to know about. Intelligence by its very nature is engaged with uncertainties: 'intelligence rarely tells you all you want to know. Often difficult decisions need to be made on the basis of intelligence which is fragmentary and difficult to interpret'.[44] Often the intelligence operative must engage with the evidence available and determine what action is best given the range of possibilities. Therefore, actions that cause a low level of harm can be used to collect information with only a 'reasonable suspicion' that the threat exists. If the information collected proves fruitful it can be used as further evidence for the justification of those activities which cause a greater level of harm.

Conclusion

Intelligence as a field encompasses a varied and fluid set of activities and is responsible for a diverse set of issues and protections. But it is also clear that it can have a diverse and fluid impact on both individuals and society as a whole. Individuals possess fundamental interests that need to be secured and it is the ethical role of intelligence to protect all of these vital interests. But that in pursuing this objective, the act of intelligence and culture it creates can cause its own violations and in turn cause greater harm than that it seeks to prevent. The way in which individuals need protecting and the impacts that intelligence can have in pursuing that end is a complicated reconciliation process, but by recognising all of an individual's vital interests, and not inherently prioritising one over the other,

it is possible to reconcile the conflict created. Furthermore, it is also vital to recognise the distorting effect of overly secretive environments in this reconciliation process and to take into account and create new, penetrative mechanisms to make sure that the calculations made reflect the actual and wide-ranging interests held by that community. By using the spectrum approach outlined to conceptualise how different levels of harm can be caused by the intelligence collection, it is therefore possible to outline and justify the different activities of the intelligence community.

Notes

1. Dulles, "*The Craft of Intelligence*," 265.
2. Claridge, quoted in Quinlan, "Just Intelligence," 1; Jones "Is Ethical Intelligence a Contradiction," 21.
3. Herman, "Intelligence after September 2001," 342.
4. Shane, "Outfitting Spies with New Tools."
5. United Kingdom Security Service Act 1989 Chapter 5 Section 1. 1.
6. See Gaspard, "Intelligence without Essence." While the understanding and formation of intelligence is far from ubiquitous across the globe, there are common features across many systems that reflect the prioritisation of secrecy, the emphasis on national security and the interrelationship and conceptualisation between human rights and intelligence activity.
7. Quinlan, "Just Intelligence," 1. Despite the growth of critical security schools of thought post-Cold War and their general success at raising the need for a wider conception of subject topic to include issues such as identity, health, environment, as well as new referent objects to include the individual, society or even the planet, when it comes to the issue of intelligence no significant change has been achieved. Buzan, Waever and Wilde, *Security*; Browning and McDonald, "Future of Critical Security Studies"; Katzenstein, *The Culture of National Security*.
8. The topic of militarisation of political systems has been gaining momentum. The literature has built on Harold Lasswell's "garrison state," referring to the increasing focus and prioritisation of security and a security mind-set over any other concerns. Lasswell, "The Garrison State"; Lasswell, "Garrison-State Hypothesis," See Cowen and Gilbert, *War, Citizenship, Territory*; Enloe *Globalization And Militarism*; Bacevich, *New American Militarism*; Kagan, *Dangerous Nation*.
9. Sustein, *Laws of Fear*.
10. Mythen and Walklate, "Communicating the Terrorist Risk."
11. *Security Service Act 1989* Chapter 5, §1.2.
12. For the purpose of this article, core human rights are those vital interests that all individuals have by virtue of the human condition. They represent an individual's most fundamental needs that are required to exist to a minimal level in order for them to experience their own version of the good life.
13. See Gill and Phythian, *Intelligence in an Insecure World*.
14. Zedner, *Security*, 9.
15. For work on 'security studies' and the changes in referent object, the construction of security threats and security actors, see Buzan, Waever and De Wilde, *Security*.
16. For more on there being a 'right' to security, see Lazarus "Mapping the Right to Security"; Lazarus "The Right to Security."
17. Feinberg, *Moral Limits of the Criminal Law*, 37; Rawls, *Theory of Justice*, 62.
18. Schneier, *Beyond fear*, 12. 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 "The Right to Security."
19. Rawls *Lectures on the History of Political Philosophy*, 226.
20. Waldron, "Security and Liberty." See Posner *Not a Suicide Pact: The Constitution in a Time of National Emergency* where he argues for the 'balance between the interest in liberty... and the interest in public safety', 31.
21. Pozen, "Privacy-Privacy Tradeoffs"; McArthur, "Reasonable Expectations of Privacy."
22. Dragu 'Is There a Trade-Off Between Security and Liberty. Also, see Ackerman *Before the Next Attack*; Hardin, "Civil Liberties in the Era of Mass Terrorism."
23. Thompson "Privacy, secrecy and security"; Dragu, 'Is There a Trade-off between Security and Liberty; Bambauer, "Privacy Versus Security." For arguments against security necessarily trumping privacy, see Moore, "Privacy, Security, and Government Surveillance." Arguments for security trumping privacy, see Himma, "Privacy vs. Security," 857.
24. See Baker, "National Security versus Civil Liberties"; Silberstein, *War of Worlds*.
25. Clarke et al., "President's Review Group."
26. Moore, "Privacy, Security, and Government Surveillance," 142.
27. Fabre, "Cosmopolitanism," 964.
28. Bellaby, *The Ethics of Intelligence*.
29. For a detailed on this culture of secrecy, see Vincent, *The Culture of Secrecy*.

30. Bandura, "Moral Disengagement," 194.
31. Fein, *Human Rights and Wrongs*, 11.
32. Bandura, *Social Foundations*, 376.
33. US Senate Select Committee on Intelligence *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, 2.
34. Arendt, *The Origins of Totalitarianism*, 423.
35. Simitis, "Reviewing Privacy in an Information Age," 719; Merton, *Social Theory and Social Structure*, 477; Harris, "Racial Profiling Revisited"; Harris, "Driving While Black"; Kennedy, *Race Crime and the Law*; Lever, "Why Racial Profiling is Hard to Justify"; and Robinson, "Construction and Reinforcement."
36. Thompson, "Democratic Secrecy," 182.
37. For government secrecy generally, see Chambers, "Behind Closed Doors"; Shapiro, *The Moral Foundations of Politics*; Thompson, "Democratic Secrecy"; Pozen, "Deep Secrecy"; Sagar, *Secrets and Leaks*. For intelligence focused work on oversight, see Aldrich and Richterova, 'Ambient Accountability; Fenster, "The Opacity of Transparency"; and Dobson "The Last Forum." For a critique of the existing intelligence oversight mechanisms and the particular problems secrecy raises, see Bellaby, 'Too Many Secrets?'.
38. Baldino, *Democratic Oversight*, 62.
39. Wiretaps in United Kingdom require a warrant that must be authorized by the Secretary of State, see Regulation of Investigatory Powers Act 2000 Chapter 23, Part 1, Chapter 1, x6(1). In the USA wiretaps must be authorized by a three judge panel whose sole purpose is to review applications for electronic surveillance warrants. See The Foreign Intelligence Surveillance Act 1978 'Electronic Surveillance Within the United States for Foreign Intelligence Purposes', x101–105.
40. Feinberg, *Harm to Others*, 37; Rescher, *Welfare*, 5.
41. Marx, "Some Concepts that May be Useful," 234; and von Hirsch, "The Ethics of Public Television Surveillance."
42. Lee "A New Societal Self-Defense," 346; Walzer, *Just and unjust Wars*.
43. Polyviou, *Search and Seizure*, 97.
44. *Blackstone's Counter-Terrorism Handbook*, 95.

Disclosure statement

Funding

Notes on contributor

Ross W Bellaby is a Senior Lecturer in the Department of Politics and International Relations, University of Sheffield, Sheffield, UK.

ORCID

Ross W Bellaby 🔬 http://orcid.org/0000-0002-6975-0681

Bibliography

Ackerman, B. *Before the Next Attack: Preserving Civil Liberties in the Age of Terrorism*. New Haven, CT: Yale University Press, 2006.
Arendt, H. *The Origins of Totalitarianism*. London, Harcourt, Brace & World, 1979.
Bacevich, A. *The New American Militarism: How Americans are Seduced by War*. New York: Oxford University Press, 2005.
Baker, N. "National Security versus Civil Liberties." *Presidential Studies Quarterly* 33, no. 3 (2003): 547–567. doi:10.1111/1741-5705.00006.
Baldino, D. *Democratic Oversight of Intelligence Services*. Sydney: The Federation Press, 2010.
Bambauer, D. E. "Privacy Versus Security." *The Journal of Criminal Law and Criminology* 103, no. 3 (2013): 667–683.
Bandura, A. *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall, 1986.
Bandura, A. "Moral Disengagement in the Perpetration of Inhumanities." *Personality and Social Psychology Review* 3, no. 3 (1999): 193–209. doi:10.1207/s15327957pspr0303_3.

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

Bellaby, R. W. "Too Many Secrets? When Should the Intelligence Community Be Allowed to Keep Secrets?" *Polity* 51, no. 1 (2019): 62–94. doi:10.1086/701165.

Browning, C., and M. McDonald. "The Future of Critical Security Studies: Ethics and the Politics of Security." *European Journal of International Relations* 19 (2011): 1–21.

Buzan, B., O. Waever, and J. De Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner, 1998.

Chambers, S. "Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation." *The Journal of Political Philosophy* 12, no. 4 (2004): 389–410. doi:10.1111/j.1467-9760.2004.00206.x.

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., and Swire, P . "President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, 2013." https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Cowen, D., and E. Gilbert, Eds. *War, Citizenship, Territory*. New York and London: Routledge, 2008.

Dragu, T. "Is There a Trade-Off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention." *American Political Science Review* 105, no. 1 (2011): 64–78. doi:10.1017/S0003055410000614.

Dulles, A. *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering in a Free World*. Guildford: Lyons Press, 2006.

Enloe, C. *Globalization and Militarism: Feminists Make the Link*. Lanham: Rowman & Littlefield, 2007.

Fabre, C. "Cosmopolitanism, Just War Theory and Legitimate Authority." *International Affairs* 84, no. 5 (2008): 963–976. doi:10.1111/j.1468-2346.2008.00749.x.

Fein, H. *Human Rights and Wrongs: Slavery, Terror and Genocide*. Boulder: Paradigm Publishers, 2007.

Feinberg, J. *Moral Limits of the Criminal Law: Vol.1 Harm to Others*. Oxford: Oxford University Press, 1984.

Gaspard, J. "Intelligence without Essence: Rejecting the Classical Theory of Definition." *International Journal of Intelligence and CounterIntelligence* 30, no. 3 (2017): 557–582. doi:10.1080/08850607.2017.1263527.

Gill, P., and M. Phythian. *Intelligence in an Insecure World*. Cambridge: Polity Press, 2018.

Hardin, R. "Civil Liberties in the Era of Mass Terrorism." *Journal of Ethics* 8, no. 1 (2004): 77–95. doi:10.1023/B:JOET.0000012253.54321.05.

Harris, D. "Driving while Black and Other Traffic Offences: The Supreme Court and Pretextual Traffic Stops." *The Journal of Criminal Law and Criminology* 87, no. 2 (1999): 544–582. doi:10.2307/1143954.

Harris, D. "Racial Profiling Revisited: 'Just Common Sense' in the Fight against Terror?" *Criminal Justice* 17, no. 2 (2002): 36–59.

Herman, M. "Ethics and Intelligence after September 2001." *Intelligence and National Security* 19, no. 2 (2004): 342–358. doi:10.1080/0268452042000302038.

Himma, K. "Privacy Vs. Security: Why Privacy Is Not an Absolute Value or Right." *San Diego Law Review* 44 (2007): 857–920.

Jones, J. "Is Ethical Intelligence a Contradiction in Terms?" In *Ethics of Spying: A Reader for the Intelligence Professional Volume 2*, edited by J. Goldman. Plymouth: Scarecrow Press, 2010: 21-33.

Kagan, R. *Dangerous Nation: America's Foreign Policy from Its Earliest Days to the Dawn of the Twentieth Century*. New York: Vintage Books, 2006.

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

Kennedy, R. *Race Crime and the Law*. New York: Patheon, 1997.

Lasswell, H. "The Garrison State." *The American Journal of Sociology* 46, no. 4 (1941): 455–468. doi:10.1086/218693.

Lazarus, L. "Mapping the Right to Security." In *Security and Human Rights*, edited by B. J. Goold and L. Lazarus. Oxford: Hart Publishing, 2007: 87-106.

Lazarus, L. "The Right to Security – Securing Rights or Securitising Rights." In *Examining Critical Perspectives on Human Rights*, edited by R. Dickinson, E. Katselli, C. Murray and O. W. Pedersen . Cambridge: Cambridge University Press, 2012.

Lee, H. "A New Societal Self-Defense Theory of Punishment – The Rights-Protection Theory." *Philosophia* 46, no. 2 (2018): 337–353. doi:10.1007/s11406-017-9931-z.

Lever, A. "Why Racial Profiling Is Hard to Justify: A Response to Risse and Zeckhauser." *Philosophy and Public Affairs* 33, no. 1 (2005): 94–110. doi:10.1111/j.1088-4963.2005.00026.x.

Marx, G. "Some Concepts that May Be Useful in Understanding the Myriad Forms and Contexts of Surveillance." *Intelligence and National Security* 19, no. 2 (2004): 226–248. doi:10.1080/0268452042000302976.

McArthur, R. "Reasonable Expectations of Privacy." *Ethics and Information Technology* 3, no. 2 (2001): 123–128. doi:10.1023/A:1011898010298.

Merton, R. *Social Theory and Social Structure*. New York: Free Press, 1968.

Moore, A. "Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability." *Public Affairs Quarterly* 25, no. 2 (2011): 141–156.

Mythen, G., and S. Walklate. "Communicating the Terrorist Risk: Harnessing a Culture of Fear?" *Crime, Media, Culture: An International Journal* 2, no. 2 (2006): 123–142. doi:10.1177/1741659006065399.

Polyviou, P. *Search and Seizure: Constitutional and Common Law*. London: Duckworth, 1982.

Posner, R. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. Oxford: Oxford University Press, 2006.

Pozen, D. "Deep Secrecy." *Stanford Law Review* 62, no. 2 (2010): 257–340.

Pozen, D. "Privacy-Privacy Tradeoffs." *The University of Chicago Law Review* 83, no. 1 (2016): 221–247.

Quinlan, M. "Just Intelligence: Prolegomena to an Ethical Theory." *Intelligence and National Security* 22, no. 1 (2007): 1–13. doi:10.1080/02684520701200715.

Rawls, J. *Theory of Justice*. Cambridge: Harvard University Press, 1971.

Rawls, J. "*Lectures on the History of Political Philosophy*." Samuel Freeman (ed.). Cambridge, MA: Harvard University Press, 2007.

Rescher, N. *Welfare: The Social Issue in Philosophical Perspective*. Pittsburgh: University of Pittsburgh Press, 1972.

Robinson, M. "The Construction and Reinforcement of the Myth of Race Crime." *Journal of Contemporary Criminal Justice* 16, no. 4 (2000): 133–156. doi:10.1177/1043986200016002002.

Sagar, R. *Secrets and Leaks: The Dilemma of State Secrecy*. Princeton: Princeton University Press, 2016.

Schneier, B. *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Berlin: Springer, 2006.

Shane, S. "Outfitting Spies with New Tools: Moral Compass." *New York Times* 28 January 2006 A1

Shapiro, I. *The Moral Foundations of Politics*. New Haven, CT: Yale University Press, 2003.

Silberstein, S. *War of Worlds: Language, Politics and 9/11*. London: Routledge, 2004.

Simitis, S. "Reviewing Privacy in an Information Age." *University of Pennsylvania Law Review* 135, no. 3 (1987): 707–746. doi:10.2307/3312079.

Sustein, C. *Laws of Fear: Beyond the Precautionary Principle*. Cambridge University Press: Cambridge, 2005.

Thompson, D. "Democratic Secrecy." *Political Science Quarterly* 114, no. 2 (1999): 181–193. doi:10.2307/2657736.

Thompson, P. B. "Privacy, Secrecy and Security." *Ethics and Information Technology* 3, no. 1 (2001): 13–19. doi:10.1023/A:1011423705643.

US Senate Select Committee on Intelligence. 2014. "Committee Study of the Central Intelligence Agency's Detention and Interrogation Program." http://fas.org/irp/congress/2014_rpt/ssci-rdi.pdf

Vincent, D. *The Culture of Secrecy: Britain, 1832-1998*. Oxford: Oxford University Press, 1998.

Von Hirsch, A. "The Ethics of Public Television Surveillance." In *Ethical and Social Perspectives on Situational Crime Prevention*, edited by A. Hirsch, D. Garland, and A. Wakefield. Oxford: Hart Publishing, 2000. 59–76.

Waldron, J. "Security and Liberty: The Image of Balance." *Journal of Political Philosophy* 11, no. 2 (2003): 191–210. doi:10.1111/1467-9760.00174.

Walzer, M. *Just and Unjust Wars: A Moral Argument with Historical Arguments*. New York: Basic Books, 2000.

Zedner, L. *Security (Key Ideas in Criminology)*. London: Routledge, 2009.