Article

JIPT

Journal of International Political Theory
2018, Vol. 14(1) 60–84

DOI: 10.1177/1755088217712069
journals.sagepub.com/home/ipt

The ethics of whistleblowing: Creating a new limit on intelligence activity

Ross W Bellaby
The University of Sheffield, UK

Abstract
One of the biggest challenges facing modern societies is how to monitor one's intelligence community while maintaining the necessary level of secrecy. Indeed, while some secrecy is needed for mission success, too much has allowed significant abuse. Moreover, extending this secrecy to democratic oversight actors only creates another layer of unobserved actors and removes the public scrutiny that keeps their power and decision-making in check. This article will therefore argue for a new type of oversight through a specialised ethical whistleblowing framework. This includes, first, outlining what intelligence wrongdoings justify whistleblowing; second, whether whistleblowing is the correct remedy – something not necessarily clear with intelligence; and finally, what form the whistleblowing should take. This framework will examine the Snowden case to determine whether he was correct leaking intelligence data and whether the means were appropriate, and second, whether those involved in the Central Intelligence Agency use of torture should have blown the whistle and if they now face blame for failing to act.

Keywords
Whistleblowing, intelligence, oversight, obligation, Snowden, torture

Introduction

One of the most important sets of security questions facing modern societies is how much power should be allowed to the intelligence community and how can we ensure that this power is being used correctly. Reports of abuse at detention centres such as Guantanamo Bay and Abu Ghraib, the pervasive growth of technological surveillance

Corresponding author:
Ross W Bellaby, Department of Politics, The University of Sheffield, Elmfield, Sheffield S10 2TU, UK.
Email: r.bellaby@sheffield.ac.uk

and the increased attention on the use of torture for intelligence collection have all highlighted not only the power of the intelligence community but also the likelihood of that power being abused. Information about these events, however, was not revealed by intelligence organisations themselves. Rather the information was either leaked – such as the Snowden and Wikileaks' revelations – or was the result of a legislative investigation prompted by media claims that took years in writing and was subjected to fierce political wrangling (Baldino, 2010: 62; Finn, 2009; Mazzetti, 2015). The problem is that the intelligence community is allowed and needs a great deal of secrecy in order to carry out its function. Yet, this secrecy can also hide actions that would not necessarily meet the expected ethical or social standards. Moreover, excessively secretive environments actually promote abuses of power by creating an insider mentality that blurs the lines between the need to get results and what is acceptable behaviour towards those on the outside. This has significantly eroded the trust that people have in the intelligence community, and given its inherently secretive nature this is something that will be difficult to re-establish. This is not to say, however, that intelligence should be made utterly transparent. Intelligence does play an important and indeed ethical role in protecting the political community, and a key part of that involves using secretive methods to detect, locate and prevent threats. However, it is clear that being allowed carte blanche freedom is not workable.

The problem is that ensuring correct intelligence behaviour is especially difficult, given the need for some secrecy coupled with a complete reliance on existing democratic institutions. By relying on elected officials to act as the main allowed oversight mechanism means simply extending the sphere of secrecy and creating another layer of unobserved actors. In other areas of government, the power of these officials is kept in check through elections whereby the public have the opportunity to examine decisions made and evaluate the consequences. However, with intelligence this ring of protective secrecy surrounds and limits outside observation of those authorising its activity; information is therefore not available to the electorate and so the authorising political community are not kept in check through the normal mechanisms. Furthermore, the current oversight structures are themselves too passive and often rely on the intelligence community to bring things forward for authorisation rather than penetrating their protective shield and investigating their actions. Therefore, this article will argue that whistleblowing can offer an additional form of oversight to act as a release valve by having those on the inside reveal harmful activities and opening them up to greater degrees of external examination. This will include the argument that not only there is a right to whistleblowing, but there also exists a duty to do so when witnessing unjustified harm, and those who fail to act – and blow the whistle – can be blamed and punished as a result. The article will first outline some of the limits of only relying on democratic structures, followed by the argument for a new framework that will outline not only when someone is right to blow the whistle but where they are obliged to. This framework will then be applied to the Snowden case in order to determine whether he was justified in blowing the whistle and whether the means he used were correct. Finally, it will be applied to the US Senate Select Committee on Intelligence (SSCI) Report 'Committee Study of the Central Intelligence Agency's (CIA's) Detention and Interrogation Program' (henceforward referred to as the SSCI Report) to determine whether those involved in the CIA's

extraordinary rendition and torture programme had an obligation to reveal the practices used through whistleblowing and whether those who failed to act now face blame.[1] In combination, these criteria will therefore offer both a limitation and licence on whistleblowing in order to provide a reflective and workable additional framework for intelligence oversight.

The limits of the system

One of the key aspects of intelligence is that it is inherently secretive. It is tasked with finding out what other people wish to keep secret, a battle 'between hiders and finders, and the former usually have the easier job' (Jarvis, 2006: 11). This means that its methods, peoples, systems, practices and information are all necessarily kept secret, as letting others know would give them opportunity to undermine the operations. However, too much secrecy can result in practices and systems that are excessively harsh in nature or unequal in application. This is particularly problematic with intelligence because it 'possess[es] special powers, such as the ability to interfere with private property or communications, which clearly can limit human rights', and so requires special monitoring by the oversight institutions to ensure that these powers are not misused (Born and Leigh, 2005: 16).

To counter this potential misuse of power democratic structures are proposed as the main checking mechanisms. Indeed, oversight of political power is the mainstay of democratic theory as it places engaged, equal decision-making at its centre, relying on elections and public enquiry as a means of ensuring public engagement and to disinfect any ills of the political elites: 'The only stimulus which can keep the ability of the body itself up to a high standard is liability to the watchful criticism of equal ability outside the body' (Hollyer et al., 2007; Mill, 2005: 138; Shapiro, 2003: 200). Therefore, in order to ensure effective intelligence while also having some form of oversight, the current system uses selected elected officials to keep watch, allowing them into the circle of secrecy in order to have access to the relevant information. Extending this circle of secrecy, however, means that there is no one maintaining watch on these oversight actors; they themselves are not open to being held to account as their decision-making is protected. The role of transparency as a means of ensuring correct behaviour by political elites and limiting their potential for abuse of position is undermined at this point. Moreover, offering secrecy to an oversight mechanism that relies on populous support places significant influence on them to carry out popular rather than correct decisions. This is made more problematic in combative electoral systems that encourages 'democratic governments' to 'emphasise policy decisions that please voters while hiding those which go against the will of the majority', placing pressure to select the correct message and limit contradicting information (Kono, 2006). As former Solicitor-General Erwin Griswold noted, it is apparent 'to any person who has considerable experience with classified material that there is massive over-classification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another' (Griswold, 1989). Indeed, investigators in the 1970s found that over 90% of information in some departments was inappropriately classified, while following the 9/11 attacks the G.W. Bush administration 'encouraged officials to withhold "sensitive

but unclassified information," which arguably should be disclosed [under the Freedom of Information Act]', as well as lobbying the Homeland Security Act which specifically exempts 'critical infrastructure information' from disclosure. This included an expansion of what counted as 'sensitive but unclassified' information with officials estimating that 'Nearly 75% of all government-held information is "sensitive but unclassified"'. In 2003, the Bush administration classified over 14 million documents, an increase of 14% on the previous year (Blanton, 2003: 33–35; Joint Security Commission, 1994; Wells, 2004: 1197, 1201, 1202, 1212).

This is then coupled with the distortive effects of having secretive groups that are physically and emotionally closed off from outside influence. Indeed, there is extensive psychological research into the impact of secretive environments on those within a group on how they perceive their own role and those on the outside. The dangers of in-group/out-group differentiation are such that those on the inside lose external reference points that act as a comparative means of measuring one's moral compass, promoting the normalisation and escalation of harmful policies as officers exclude those considered outsiders from their universe of obligation while internal criticism is simultaneously limited as an act of betrayal.[2] The potential for this affect is then heightened as intelligence represents a special 'security concern'. As a security issue intelligence is raised out of the domestic sphere where political debate is dominant and into the extraordinary-security sphere where the sense of threat and urgency are heightened. This framing only serves to skew the way events, and even the concept of secrecy itself, are perceived, creating a 'do or die' mentality. This entrenches it in the mindset where threats are framed in terms of what is best for the state as the main provider of security, rather than the individual. The tension created between these two fields is such that, as Dennis Thompson notes, you are essentially left with two options, 'abandon the [security] policy or sacrifice democratic accountability' (Thompson, 1999: 182). Framing intelligence secrecy in these terms sets it as a national security question and as a binary in opposition to human rights where you can have security or you can have liberty but one must come at the cost of the other and, importantly, where national security is seen as a trump card.

Furthermore, the structures are overall too passive where authorisation or rejection comes at the point of the intelligence community asking for permission. Surveillance warrants requests are notable example of this as intelligence actors approach the courts or executive for authorisation when they decide this is required.[3] This, however, is problematic because such authorisations are limited in terms of what activities require it – in that it is only really search and interception warrants that require individual authorisation – so this leaves other activities unmonitored. 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. This is exacerbated by a serious power imbalance between the individual and the state. That is, when individuals make requests for information – through Freedom of Information (FoI) requests, for example – intelligence officers, or the executive who acts on their behalf, have all the information to make their case while other oversight actors – the legislative or individual, for instance – have very little or no information. Individuals are therefore at a significant disadvantage in regard to knowing when to ask, what to ask and how to appeal a decision. This means the emphasis is the

wrong way round. The state has the knowledge and the power, while those making the request have none.

In practice, these existing mechanisms have been shown to be physically too weak to provide the necessary form of oversight. For the executive, its oversight role exists in 'giving direction', including 'tasking, prioritising and making resources available' (Born and Leigh, 2005: 15). However, this has created a tendency among the public to place direct blame for any intelligence failure on the executive as a lack of appropriate foresight, fostering a need to project operational success and hide any failures. The executive and intelligence community have thus merged to such an extent that it can no longer be considered to have the degree of detachment required to be an oversight actor. This is more problematic in structures, most notably in the US system, where those at the higher levels of the intelligence community are political appointees as executive influence means that job security rests upon the desires of those in power. Indeed, some of the biggest intelligence scandals have included failure to fully supervise a perversion of political power. From the Watergate scandal and President Nixon abusing his power to gain advantage over his political rivals (Church Committee, 1976: 344) to the use of torture by the CIA and senior political actors – including National Security Advisor Condoleezza Rice, Secretary of Defence Donald Rumsfeld and Secretary of State Colin Powell (Phythian, 2016) – failing to investigate properly or act on what they knew. It could almost be said that the executive is the political wing of the intelligence community. In comparison, the legislative's power is limited to 'passing laws that define and regulate the intelligence and security services', which are too broad to offer real-term scrutiny, and 'by adopting the corresponding budgetary appropriations' (Fluri and Born, 2003: 22). This means that the legislative is restricted in regard to at what points in time it is able to exert its influence and is left with limited penetrative powers, examining activity only once it has been revealed. In practice, legislative oversight has become riddled with politicalisation, gridlock and turf warfare. While in the judiciary, there is arguably an unwillingness on behalf of the courts to supplant their understanding of national security over that of executive. This is coupled with an often-used executive right to have courts conceal proceedings and information in cases relating to national security, limiting the ability of others to fully interrogate the arguments made (Weaver and Pallitto, 2005: 86, 102–104).[4] Moreover, in courts where the whole proceedings are kept secret – the Foreign Intelligence Surveillance Court (FISC) being a notable case – it can be argued that this secrecy limits opportunity for engaged reflection and debate on the legal interpretation. Without different courts at different levels interrogating the interpretation of the law, the decisions can go unchallenged. Indeed, the purpose of having a hierarchy of courts with the right to appeal and challenge the ruling is so that the decision can be examined and interrogated through a reflective endeavour by one's legal peers (Dalton, 1985; Lennerfors, 2007; Nobles and Schiff, 2002).[5]

Finally, there are some existing internal avenues to the intelligence community that offer some form of outlet at certain times. For example, in the US system the Interagency Security Classification Appeals Panel (ISCAP) reviews documents for classification; the President's Foreign Intelligence Advisory Board (PFIAB) carries out investigations and initiates activities for the President; the agency's own Inspector General who report to the Secretary of the department or the director of the agency and is tasked

with conducting investigations, audients, inspection and special reviews, and other advisory commissions and advisory bodies such as the Office of Management and Budget which reviews spending, or the Department of Defense's own Intelligence Oversight Programme whose object is to ensure operations meet statutory and constitutional rights of US persons. However, depending on the issue that might prompt the whistleblower to act these internal actors could be seen as being inappropriate for the harm witnessed, or subject to the too much political control and influence to act sufficiently. Notably, the ISCAP and PFIAB comprise and are directly responsible to the executive itself (Aftergood, 2009: 407–408). While the Offices of the Inspector General might be seen by the potential whistleblower as being too imbedded within the existing system and so unable to act as a sufficient means of getting the right response. So while they can offer a good avenue for internal release of information – the importance of which is examined later on – in some circumstances they can limit opportunity for sufficient action.

This is not to equate the US intelligence oversight system as the only form of democratic oversight, but it is the most dominant and detailed in its structures and whose intelligence community dominates in terms of both size and reach. Indeed, other states have different practices and even different emphases, such as the German system recognising the Bundestag member's 'right to information' and to launch powerful and enforceable investigations (Dacre, 2009: 14; Miller, 2016). This, however, is still reliant on someone on the outside from being aware of the intelligence failing occurring from behind the barrier of secrecy. What the US system does give us is an example of where the existing democratic structures can fail; where their limits are and the need for an additional mechanism to be established to ensure that the type of abuses mentioned do not occur again. This article will argue, therefore, for the role of whistleblowing as being that backstop, a pressure release that kicks in when the other mechanisms fail to report on the abuse; one that utilises those who are already on in the inside of the intelligence community with special access to information. Indeed, the recent leaks from both Edward Snowden and Wikileaks have demonstrated an appetite both from those on the inside to express themselves when they think they see wrongdoing and from the general public to be made aware about events occurring behind the intelligence curtain. However, both of these cases also highlight how those involved in intelligence whistleblowing face a hefty cost for coming forward, including arrest, public shaming and exile. Therefore, in order to achieve this objective this article will argue for a new ethical framework that outlines not only when those on the inside have the right to release information outside the usual oversight mechanisms, but importantly where they are obligated to do so and where failing this obligation means that they are complicit in the harm being done and can be punished accordingly. This framework will act as both limiting and licensing: limiting the harm that whistleblowing can cause while also recognising that some harm is justified when done in order to protect the political community and the individual. This framework will consist of several criteria that each aid in the deliberative process, including the presence of a clear justifying reason that prompts the whistleblowing activity, that it is only done when the overall benefit it can bring is greater than the harm that blowing the whistle can potentially cause, that the information is released to the correct audience given the harm being caused, and ensuring that the potential backlash to the whistleblower is taken into account when determining their obligation to act.

A whistleblower's right and obligation

The ethical framework proposed sets out a system of criteria for the potential whistleblower to work, though. It establishes the underlying justifying reason from which the obligation to act is drawn from, the authority the whistleblower has to go against the ordinarily imposed authority of their leaders or organisational loyalty, the type of proportional calculations that they should reflect upon as a guide to understanding when whistleblowing is the correct course of action given the surrounding situation, the correct audience to release the information to, and finally, it details the limits of the whistleblower's obligation, arguing that they are relieved of the need to blow the whistle if the personal costs are too great, though they are still left with the right to act.

First, it is important to understand the justifying reason that sits as the core of why the intelligence operative has an obligation to blow the whistle when they see wrongdoing. For whistleblowing, this is drawn from the broad argument that individuals have a duty to prevent harm from being caused to others, and so represents a form of acting in defence of others. At a general level, this can be framed in terms of the 'Good Samaritan' argument, whereby 'one ought to help, or at least offer to help, those whose welfare is endangered' if there is a minimal cost to oneself (Kleinig, 1976: 385). Indeed, we normally assume that if we can save a human life at minor cost we are obligated to do so. Though Richard DeGeorge (1990) goes further in this argument stating that

> It is not implausible to claim both that we are morally obliged to prevent harm to others at little expense to ourselves, and that we are morally obliged to prevent great harm to a great many others, even at considerable expense to ourselves. (1990: 214)

Indeed, John Rawls' 'original position', the classical utilitarian's 'sympathetic spectator' or the Golden Rule, each outline how, after we put ourselves in the shoes of those in trouble, we would want the help and creates an obligation to act; or where the need to stop harm being done is seen as being no different to acting to cause others harm.[6]

However, for intelligence there is more than just a general obligation to act but a very specific one that can act as a strong justifying reason for whistleblowing. That is, given that the ethical justification for the use of intelligence is the protection of the political community, when they not only fail to meet this standard but also directly cause the undermining of this, then they fail the very reason for their existence and as such lose their ethical clout. This is not just a case where the intelligence community sees harm being caused to those it is charged with protecting and fails to act but also where the intelligence practice or policy is the actual source of the harm. This means that the obligation to blow the whistle is strong but limited. It is strong in that it requires those who are actively causing harm to have the whistle blown on them, but it is limited to those activities where they are related to the source of the harm.[7] By failing to act on those who could have prevented the harm makes themselves complicit by allowing the harm to continue through their inactivity. It will be argued later, however, that this obligation is not absolute but is mediated in a proportionality calculation whereby the costs to the whistleblower and other, wider costs to society and even the failure of future intelligence missions need to be incorporated into the ethical calculation, mediating the obligation to a right. What this principle does is establish the basis of the obligation, the

nature of which in terms of how and when to carry it out is then determined by the additional criteria.

Next is the argument that the individual has the authority to act. A key part of the whistleblowing literature is that the individual does not have the authority to act because there is a special obligation that one has to an organisation – whether contractual, reciprocal or moral – that then carries an expectation of loyalty (see Bok, 1985; Brenkert, 2010; Gadlin, 1998; Hoffman, 1984; Jensen, 1987: 324; Winfield, 1994). They must therefore defer their own judgement in preference to that of their organisation. It will be argued here, however, that the individual can act as their own authority. Indeed, at the centre of the ethical justification given to the intelligence community is the understanding that it is acting on behalf of the political community, which, in turn, means that it is responsible as both the legitimate authority to carry out harmful activities on their behalf and to them as the ethical end: 'since the care of the common weal is committed to those who are in the right authority, it is their business to watch over the common weal' (Aquinas, 2002: 214). The state's authority is not derived from its *de facto* position or its coercive sovereignty but from its role as a representative of the political community (Norman, 1995: 118). Furthermore, there is also a recognition that the state normally has a greater level of knowledge and resources; that it is physically able to weigh up the costs from a more neutral position taking into account the interests of the whole community. However, in this instance, the state, through its intelligence community, represents the source of the threat and as such the legitimate authority must rest elsewhere, and in this instance that is the 'inside individual'. That they too can, and in some circumstances must, act on behalf of the political community when they are the witness to harm being caused. These individuals on the inside have greater access to information than other forms of oversight actors (as this represents one of the benefits of exploring whistleblowers as a new form of oversight) and so has knowledge authority. They are actively made aware by the intelligence agency the importance of both their own work and the wider political situation, and so has access to information that makes an informed decision on the costs and benefits possible. Moreover, an informed individual can act on behalf of the political community when the legitimate authority – normally the state and its oversight mechanisms – is the source of the harm or is unable to act for some reason, although the whistleblowing actions taken must reflect this. They must not blow the whistle for self-aggrandisement or profit but in order to prevent harm to others or the political community, where the how, when and to whom are reflected in the actions taken.

However, just because there is harm being caused does not mean whistleblowing is the correct answer, nor does everyone have the same level of obligation to act. Rather, the whistleblowing must pass a proportionality calculation, whereby determining whether whistleblowing is the correct remedy will depend on the overall harm or benefit caused or prevented by the information release. In determining the costs and benefits to be included, Kevin Macnish argues that there are sufficient, supporting and peripheral factors that add different weights to the proportionality calculation. That is, those factors that are necessary for achieving the good proposed are the sufficient factors; supporting factors further these necessary objectives but do not on their own justify the action; and then peripheral factors are side benefits/costs that are not related to the moral end (Macnish, 2015). What this means for whistleblowing is that only those goods that are

sufficient and supportive of the ethical end of intelligence – the protection of individuals and the political community – can be included when maintaining the need to keep the secret, whereas the harms and damages that go into justifying the use of whistleblowing can include peripheral costs. In order to make this determination, two sets of key questions must be answered to weigh up the forces in play. The first set includes questions regarding what harms or damages are caused by the whistleblowing? For example, if the information is released, is it reasonable to foresee that the repercussions will put those in the field in danger, or are there any significant costs to internal and external trust or will there be a backlash to the whistleblower themselves? Then what are the benefits of not blowing the whistle? This is slightly different from the previous point and includes those supporting positive factors to keeping secrets that are separate to the damage caused when information is released. For example, the information being gained from a successful mission or maintaining and continuing international intelligence cooperation can act as a positive in the calcualtion. These factors are then balanced against a second set of questions, including what are the harms or damages caused by the intelligence activity? This could include, for example, the number of specific harms caused by the operation when it violates an individual's vital interest in privacy, autonomy, mental and physical integrity or liberty, or broader harms to society such as degradation of social cohesion if the practice involves the segregation or marginalisation of specific sectors of society.[8] Also, what are the benefits of releasing the information? For example, can timely whistleblowing represent an important move to ensuring and garnering trust within society by showing people that a system is working, or could the intelligence operation be aided in some way? This could also include highlighting examples of where internal whistleblowing has been successful and has advanced practices.

Furthermore, this proportionality calculation helps outline the different whistleblowing obligations that individuals have. Indeed, determining whether the harm caused creates an obligation or merely a right to whistleblowing is dependent on several intervening factors that include the level of responsibility the individual has, their knowledge and capabilities, the level of harm being caused and the potential backlash that they would face by blowing the whistle. For example, first, it must be determined what is expected of the individual in terms of rank and areas of concern. Those individuals who have a higher rank also carry with it a greater expectation that the organisation and individuals beneath them are behaving correctly (Bradley and Schipani, 1989: 19; Horsey, 1994: 974; Walzer, 2000: 316). The higher the position, the greater the realm of concern and the ability to monitor this realm through increased resources, training and expected capacity. For example, those at the bottom will have limited resources and point of view, meaning that they will have a limited realm of what can be reasonably expected of them, limiting their obligation to act. Whereas those at management level will have a greater view of what activities are being carried out and training on what is expected, meaning that there is a greater obligation for them to act. In terms of intelligence and political oversight, those political leaders who have a mandate of ensuring correct behaviour have an obligation to be informed and to investigate to ensure that those beneath are adhering to the standards expected of them.

This obligation is then examined against the potential backlash that they might face. Indeed, whistleblowing has historically been shown to carry with it a significant degree of

harm for the whistleblower themselves. Retaliation against whistleblowers has been reported in the literature across a range of instances and societies. Philip Jos et al. (1989) reported that 69% of the whistleblowers they surveyed answered that they were fired or forced to retire (1989: 554), while Joyce Rothschild and Terance Miethe (1999) reported that this was the case for 69% of their survey, with 84% of participants reporting suffering from anxiety or depression as a result (1999: 120), and Joseph McGlynn and Brian Richardson (2014) detail how the possibility of slander, physical intimidation and death threats is very real for those who blow the whistle (2014: 214). In terms of blowing the whistle, this means that if there is going to be clear repercussions for the whistleblower, then this can act as an intervention on the individual's obligation to reveal. This means balancing the potential instrumental costs in the form of loss of livelihood and costs to vital interests in the form of physical, emotional and mental stress the whistleblower will likely face in comparison to harm being caused by the intelligence policy or activity. If the impact on the whistleblower is too great than the demand that the individual acts is mediated, meaning there is only a right to blow the whistle rather than an obligation. If, however, the harm being caused is extreme, then it can be argued that the backlash facing the whistleblower can be outweighed and the obligation resumes. What this means is that if the blowback is high and the individual's responsibility is low, then it can be argued that their obligation to act is mediated – although they still have the right to act if they so wish. If, however, the level of harm being caused by the intelligence was high, then the blowback would have to be significant (e.g. truly life threatening) to mediate the obligation. For example, the reasonable expectation of a threat to the whistleblower's life, liberty or autonomy would only be outweighed by a greater harm being suffered to someone else or a lower level of harm being suffered by many people. While only instrumental, financial, for example, costs to the whistleblower would be easily outweighed by physical or mental costs to an intelligence target but would not be outweighed in localised instances of colleague incompetence or financial mismanagement.[9] The higher the harm being suffered and the higher one's responsibility, the greater would be the obligation to act.

While with any proportionality calculation, there is the problem of there being what Macnish refers to as a 'twilight zone' where the calculation is unclear – which in the instances of intelligence is a real problem, given structural compartmentalisation and much of the work being 'a calculation of probabilities' – this does not in itself discount the need for a proportionality calculation (Quinlan, 2000: 69). What it does is highlight the need for a more flexible set of response avenues. In this instance, an understanding of the principle of last resort helps as it argues that the least harmful answer should be pursued and in instances where the harm or benefit are especially unclear on either side of the calculation, those whistleblowing activities that are least likely to cause harm have greater moral weight. That means of the options available the appropriate audience must match the situation. There is no rigid methodology, beginning with internal management and ending in full disclosure, but it does require that some of the wider reveals are not 'jumped' to out of ease, efficiency or expediency.

That is why once each of these initial justification stages are confirmed, the last part is determining what form the whistleblowing should take and what processes should be followed. This begins with, first, recognising that some information needs to be protected as incorrect information release can put people in danger as will choosing the incorrect audience as the more people with access the more likely sensitive information will be

unjustifiably leaked, whether through incompetence, blackmail, bribery, manipulation or deception. So, initially, for example, releasing the information internally has an important role, and some argue that going through the internal chains of command should be the first step.[10] Reporting wrongdoing internally has the benefit of ensuring that those with whom the issues are discussed already have security clearance and a more open discussion can be held. This also limits unjustified leaks that would undermine the lives of intelligence operatives and mission success as the information is kept within the central circle. It can be argued, however, that there are some significant problems with keeping it only internal to the intelligence community. If the wrongdoing is the result of systematic policies or abuses that have developed over time, reporting them internally is not likely to promote the reflection that is required. People are their own worst judge and are not likely to see what is wrong with their activity: especially if the policy or activity is deeply entrenched within the structures of the agency, if it is a directive from management or if the secretive environment has cognitively restructured how officers view their behaviour.

Another option is going through the authorised external oversight mechanisms – whether it is reporting to legislative committees or working up through the executive chain of command. Again this has the benefit that those involved are well versed in the arena of intelligence activity and are within the circle of secrecy, offering an educated analysis while keeping one eye on the wider implications for the rest of society. Though, as already noted, relying on these oversight mechanisms can be problematic given that the structures are inherently politically and personally biased, or are insufficient in power or mandate to affect change.

Finally, the public represent a legitimate audience in this instance for a few reasons. First, because the ethical base from which the intelligence draws its value is protecting the political community, arguably the political community should have a say in what sort of actions it considered to be appropriate in its protection. Second, if it is something that is negatively impacting a significant number of people, then there is argument that they have a right to know what they are suffering in order to make a decision and act. Third, collectively they represent a significant power for affecting change. However, this does remove any prospect of some secrecy being retained. This could significantly undermine intelligence effectiveness as knowledge of operational methods used means that it is possible to circumvent them. Therefore, the released information should be sanitised so as to limit the impact on any singular operation or operative while giving details on the harmful elements involved. This requirement for sanitisation only serves to highlight the need for the correct form of whistleblowing to be followed; that even though there is a wrong being done that harms people, releasing information that can threaten the lives of an operative, for example, could poison the justification for the information release.[11] This means that there is an obligation on both the whistleblower and media outlet to ensure that they avoid unnecessary harm being caused and to ensure that the information released is minimised.

Edward Snowden and the NSA

In 2013, Edward Snowden, self-described as an infrastructure analyst working within the national security agency (NSA), stole 1.7 million classified documents from the US government (Greenwald, 2014; Kelley, 2013; Shane and Sanger, 2013). Once Snowden had

fled the United States, *The Guardian* began to publish details that outlined the existence of surveillance techniques used by the NSA on behalf of the US government. This includes, perhaps most famously, the revelations regarding the NSA's PRISM network that allegedly allowed access to information from several of the world's largest Internet companies (*The Washington Post*, 2013). According to a partially declassified 2011 opinion from the FISC, NSA collected 250 million Internet communications per year under this programme, with the widely reported PRISM acquiring 91% 'directly from Internet Service Providers', and the other 9% being collected through 'upstream collection' whereby data are accessed in transit from one unspecified location to another. The Obama Administration also acknowledged that given the technical limitations of the 'upstream' collection, it was very possible that some communications that were unrelated to the target or were entirely between persons located in the United States may have been collected (Liu et al., 2015: 10). So, should Edward Snowden have blown the whistle and released sensitive intelligence to the whole world? Answering this question means examining what harm was being caused and whether it was justified or not; if not justified, whether whistleblowing represented the best means of dealing with the harm; and finally, if the procedure and audience chosen was the most appropriate.

In determining whether there was a justifiable reason to act, the legal case is ambiguous. James Clapper, the Director of the National Intelligence, stated that 'We believe we have been lawful' (Shafer, 2014). Indeed, the operations were officially sanctioned by the FISC, the Senate Committee had awareness and President Obama sanctioned the operations. Moreover, in American Civil Liberties Union (*ACLU*) *v. Clapper*, Judge Pauley of the S.D.N.Y. agreed with the FISC that the NSA's metadata collection programme did not violate the Fourth Amendment as it did not reach the standard of being a search (2013: 959 F. Supp. 2d at 752). However, in *Klayman v. Obama* Judge Leon from the D.C. District Court made counter-legal arguments that were more receptive to the position that the aggregation of telephone records can result in a Fourth Amendment search, where the data collected reflected more the content of a message than the external headers and so had a higher legal standard to meet (2013: WL 6598728, at §18).

Given this lack of legal clarity, the main analysis is therefore whether the *en masse* surveillance was so excessive that it was reasonable for Snowden to perceive the NSA as representing a significant unjustified threat to our privacy and autonomy. The degree of the violations and its widespread nature meant that the NSA's programmes were unjustified. Indeed, the initial analysis relied on the longstanding *Smith v. Maryland* decision that determined collecting external data on what telephone numbers an individual dialled did not amount to a search and so is not protected under the Fourth Amendment (1979: 442 US 735,). However, it can be argued that the data collected can be very revealing of an individual's intimate information. The PRISM programme collected meta-data from 'U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple', as well as content data 'such as emails, photos and videos' (Gellman and Poitras, 2013; Greenwald and MacAskill, 2013). By analysing these data through monitoring techniques known as 'data-mining' and 'dataveillance' of people's content and meta-data, it is possible to determine what someone has done, are doing or will do next (Dempsey and Flint, 2004: 1464; Gandy, 2003: 28; Keefe, 2005: 99; Rubinstein et al., 2008: 271; Solove, 2004: 4). All of these data can be used to reveal very intimate

details about an individual. Information on what websites an individual visits (even restricted to before the first/slash) can reflect intimate details about a person's life and given the increasing transference of social life to cyberspace, information about online activity should be considered to be of a most intimate nature. This type of information is more akin to knowing the content of an individual's private conversations. Even though the majority of the online information viewed might be considered as being superficial as to a person's identity the type of data collected does not change. Distinctions are made, both ethically and legally, between 'header' information which details who is contacting whom, and content data that refer to the information retained in the message (see Diffie and Landau, 1998: 151; Shulsky, 2002: 26). Given the nature of Internet meta-data and URLs, the content of the website and the activities done by the user are inevitably revealed and are closer in nature to that of an individual's conversations than 'header' information of who you are talking to and when (Sample, 2016). Even if all you spoke about on the telephone was who won what sport, it would not remove the argument that the content of phone conversations is treated as more private – and comes with greater protection – than the header information (Bellaby, 2016a). Indeed, in two separate concurring opinions, five justices drew this distinction between the type of data being collected as being more personal and opined that although short-term government monitoring may not exceed a person's expectation of privacy, longer term monitoring may do so, as aggregating information about a person can reflect a 'wealth of detail', or mosaic, about his 'familial, political, professional, religious, and sexual associations' (United States v. Jones, 2012: 132 S.Ct. 945. If, as Gary Marx describes, information can be thought of in terms of concentric circles where the closer one goes to the centre the more intimate the information, and the more intimate the information the greater the expectation of privacy the individual has, information about an individual's sexuality, political or social views, and medical details are intimate, and so there is a demand for a very higher degree of privacy protection (Hirsch, 2000; Marx, 2004: 234).

Moreover, the interest the individual has in their privacy and autonomy has an intrinsic value that means that damaging it causes harm regardless of the repercussions. That is, even if, on balance, the individual does not experience the harm in a 'tangible and material' way, he is still harmed since his vital interests have been violated (Feinberg, 1984: 35). So, while the individual might not necessarily 'feel' the direct impact of the violation, he indeed still harmed.

In addition, it can be argued that it was directed against individuals who had done nothing to warrant being targeted. In instances where the intelligence collection activities significantly violate an individual's privacy effort should be made to discriminate between legitimate and illegitimate targets and directed against those who have explicitly acted in some way to forfeit or waive temporarily their protective rights, by acting or contributing to a threat or through or lack of regard for their own privacy, for example (Bellaby, 2014: 29; Macnish, 2015; Pfaff and Tiel, 2004). *En masse* surveillance by its very nature is unable to make this distinction and given the high level of privacy violation is unable to not negatively affect individuals who have done nothing to justify being targeted. Therefore, it can be argued that the extensive surveillance programmes being deployed by the NSA were unjustified and so for those involved they should act to prevent further harm being done.

Finally, the development of surveillance databases often over-represent particular social groups, heightening social fear of that group as well as reinforcing distorted criminal statistics (Bennetto, 2009). The databases created often leave a taint of suspicion that lingers and spreads like a stain across the associated and over-represented group, either leading to inappropriate treatment later in life or creating a loss of trust and confidence in the state apparatus. Finally, cyber-surveillance can violate an individual's autonomy by, as Macnish details, promoting 'chilling effects … behavioural uniformity … fear of control … and a fear of being "found out" when hiding legitimate information' (Macnish, 2015: 542). This is problematic as individuals are unable to make informed decisions about how they wish to be seen and as such it violates their interest in autonomy. Given this level of intrusion, therefore, it can be argued that the NSA programmes revealed by Snowden represented a severe violation of an individual's privacy and as such a strong justifying reason for some action – the nature of which would then be determined by the other criteria.

Therefore, the next question is whether whistleblowing was the correct remedy. The critique against using whistleblowing is that revealing such information threatens the methods used by intelligence actors and will therefore undermine future missions. It has been claimed, for example, by former NSA Director General Keith Alexander that Snowden had caused 'irreversible damage' to the United States (Landau, 2013: 54). Equally, Andrew Parker, the Director General of the UK Security Service, has argued that this point claiming that the revelations have resulted in a 'guidebook for terrorists' that represents a 'gift if they need to evade us and strike at will' (Whitehead, 2013). Similarly, Sir John Sawers, Secret Intelligence Service (MI6) Chief, said that terrorists would be 'rubbing their hands with glee' at the level of information that had been put in the public domain by the Snowden leaks (Whitehead, Rayner, Swinford, 2013)). Moreover, there are concerns that releasing information can put the lives of intelligence officers and agents in jeopardy, especially in terms of, as Sir Sawers argues, gaining access to a closed-off terrorist groups which can be a 'complex and often very dangerous' activity (Sawers, 2010).

However, the reality of such costs has failed to be fully substantiated. Indeed, NSA Director Admiral Michael S. Rogers played down the impact, stating that the 'sky is not falling' and made an effort to outline how new practices had been developed (Sanger, 2014). The intelligence community is an adaptable organisation, and they themselves have made it clear that they have amended their methods as a result: 'When we see a change in behaviour, our guys are changing right along with it, or we're already seeing it and adapting to it' and are updating their methods in light of the NSA releases (Schmitt and Schmidt, 2013). While such changes can incur significant costs in terms of money, time, recourses and lost intelligence, these instrumental costs are arguably outweighed by the costs of the *en masse* surveillance programme itself given the wide and significant violation of people's privacy. Indeed, while preventing imminent terrorist attack is important, it is unclear how vital these collection techniques were needed in the immediate sense. In *Klayman* Judge Leon, when turning to the efficacy of the programme, questioned whether the programme has 'actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time sensitive in nature, doubted that the program had significantly aided the government in conducting time

sensitive terrorism investigations' (2013 WL 6598728, at §23). Given this, it can be argued that there was a justification for whistleblowing and Snowden was permitted to reveal the information to prevent the harm.

If, however, this was a case where the surveillance was limited in either scope, amount of information collected or focused on superficial 'header' information, while there could still be a justifying reason for action, the costs involved would mean that the actual information revealed and the audience to which the information was revealed would be different. For example, if it related to a case regarding the instances where the surveillance was being misapplied in a limited number of cases, the costs of widely revealing the methods used (including detriment to future missions) would outweigh the benefits of tightening the procedure in a limited number of cases. In these types of cases, given the higher costs of whistleblowing and limited harm being caused the emphasis would therefore be on an internal revelation utilising either those mechanisms within the intelligence community or the political structures.

However, in the Snowden case as it stands the general public through media outlets was the best avenue to release the information. As already been noted, the NSA data collection programmes were known by the Permanent Intelligence Committee, President and FISC - and all had sanctioned them in one way or another. If the information being passed up to the oversight actors were purposefully deceptive, then it could be argued that they could be approached with truer information with the aim of acting accordingly. However, given the restricted debate among agreeing actors is not likely to create the level of debate necessary to examine difficult issues and, as Former Vice-President Al Gore argued, examining secret laws in secret represents a dangerous oversight methodology: 'that the NSA's activities in my view violates the Constitution … It isn't acceptable to have a secret interpretation of a law that goes far beyond any reasonable reading of either the law or the Constitution' (Goldenberg, 2013).

It can be argued, therefore, that the NSA surveillance operations were, by their very nature, inclusive of a large audience, and so the repercussions of their use were much wider than any previous policy. This is not about the appropriate action of a single operation or operative. If it were, then it could be argued that the harm being caused would be much lower, and so the harm caused by an external whistleblowing would outweigh the benefits of highlighting a singular or a small selection of misapplied operations. In this way, utilising some of the internal avenues or reporting it through political channels would represent a more justified action. Rather it is about a set of programmes that were harmful to a large portion of the population. This means that there needs to be a wider consultation to ensure that they are being used correctly. Indeed, given the rate at which technology and society's use of that technology is evolving, the laws are quickly outdated and need a wider discussion to ensure that the technology is being used appropriately. Releasing the information to the public offered a means of ensuring wider debate, a dramatic interception on the practices used and further enquiries as to whether the oversight actors were fulfilling their duty sufficiently.

On balance, therefore, it can be argued that the information revealed regarded an intelligence practice that was causing many individuals a high level of unjustified harm. The NSA surveillance programmes significantly violated a large number of individual's privacy by collecting intimate information, meaning that the whistleblowing was justified.

Moreover, given the widespread nature of the data collection, an equally wide reveal would offer the best way of gaining the attention and promoting the debate that would be needed to understand what place with surveillance programmes had for intelligence and the rest of society.

Failing the obligation: Where was the torture, Snowden?

In comparison, the recent revelations regarding the use of torture by the CIA offers a means of examining what happens when no one blows the whistle: was there an obligation to blow the whistle, if so for whom, and what repercussions should those who failed to act now face? So, in terms of whether the harm caused by the CIA torture regime was justified, it will argued here that it was not. The debates and issues surrounding torture are well known.[12] Torture represents one of the greatest sets of harms against an individual as the physical, emotional and psychological attacks are used to destroy any autonomy of the individual and condition their responses.[13] The harm is of such a high quality that it can be argued that the proportional calculation cannot justify its use, especially given that there was no evidence that it was producing good actionable intelligence. While there are those who argue that the utilitarian benefits can outweigh the costs (Dershowitz, 2002: 137; Herman, 2000: 306; Scheffler, 1985: 409), such calculations are either hypothetically constructed to provide a certain answer or do not take into account the long-term or wider harms torture can create (Bellaby, 2016b; Costanzo and Gerrity, 2009: 179; Luban, 2005: 1444; Matthews, 2012: 466). Systematic torture like that reported in the SSCI Report therefore represents the clear case where the intelligence practice is unjustified.

Moreover, given the high level of harm that torture causes and the extensive and systematic nature that was outlined in the SSCI Report, it can be argued that there is a need for some immediate action to stop the harms being caused. Whistleblowing would offer a powerful means for achieving this. In the first instance, the turbulent political investigation and debate used were overly drawn out, allowing the continuation of the extreme levels of harm while also highlighting the possibility that the report might never have been released. Also, the torture regime was not an ad hoc or grass roots development but was an organised and purposeful affair. Using the internal reporting mechanisms would be futile or too slow as it was the system itself that was causing the harm. This means that there is a need for a strong intervention that would have political weight and speed to counter the high levels of harm being done. A public-wide whistleblowing would therefore create the level of attention required and the surest way to stop the programme.

Understanding who should have blown the whistle, however, is less clear. From the atrocities detailed in the SSCI Report, those in the interrogation room or running the facilities do have an obligation to act (US Senate Select Committee on Intelligence, 2014: 43–44. Hereafter SSCI Report). They were the source of harm or had first-hand knowledge, meaning that they would have been credible informers. However, upon reading the STR, it can be strongly argued that it is the CIA elite who, though distanced from the act itself, have some of the greatest obligation to act. For example, the

> Headquarters formally proposed that Abu Zubaydah be kept in an all-white room that was lit 24 hours a day, that Abu Zubaydah not be provided any amenities, that his sleep be disrupted, that loud noise be constantly fed into his cell, and that only a small number of people interact with him. (SSCI Report: 26)

Moreover, not only was CIA headquarters aware of the abuse but also they actively fostered and escalated the torture culture itself. This includes isolating themselves from oversight (SSCI Report: 54, 119, 123), encouraging an inward-looking mentality and a distortion of their own goals (SSCI Report: 438), explicit training on enhanced interrogation (SSCI Report: p. 58); smothered internal criticism, and even when on-site interrogators claimed that individuals were 'compliant and cooperative', they were still ordered by CIA Headquarters 'to continue using the CIA's enhanced interrogation techniques' – escalating and protracting the abuse (SSCI Report: 78, 43, 66). They created the environment to promote the use of torture while limiting appropriate oversight. Their direct involvement meant that they were the authors of the harm caused, which heightens their obligation to blow the whistle. While there could be arguments that the fallout they would personally face, especially once it became clear the level of their involvement in the torture, might mediate this obligation, given the extremely high and consistent levels of harm caused the duty to reveal outweighs the repercussions they might face.

Finally, while the role of the political elite is less directly clear, it can be argued that they had a significant degree of obligation to act. On one hand, it could be argued that they had no knowledge of the harm being caused and so cannot be expected to act. For example, CIA records state that prior to the use of the enhanced interrogation techniques on Abu Zubaydah in 2002, 'the CIA did not brief Secretary of State Colin Powell or Secretary of Defense Donald Rumsfeld', while also significantly revising their presentation to 'eliminate references to the waterboard' (SSCI Report:38). Yet on the other hand, when DCI Tenet and CIA General Counsel Muller met with Vice President Cheney and National Security Advisor Rice on 29 July 2003 to seek reaffirmation, even if they did not make them aware of the magnitude of the abuse, they did present a list of enhanced interrogation techniques including the use of waterboarding, demonstrating that they were now aware that something far greater than is normally allowed was occurring (SSCI Report:117–118). In failing to investigate further and report upwards, they also make the president negligent for not inquiring further, which becomes especially problematic on the behalf of G.W. Bush, given the International Committee of the Red Cross's two reports on 18 November 2004 and 18 April 2006 that raised concerns over the treatment of individuals that 'amounted to torture and/or cruel, inhuman or degrading treatment' and the media attention it received over the years (International Committee of the Red Cross, 2007: 4). Their failure to investigate when it was their duty to do so places a significant degree of blame on them.

This presents a situation where each level did face an obligation to act. Those at the bottom had first-hand knowledge and were directly part of the torture, meaning that they should have acted. Moreover, historically it is workers at this level who have been the most likely to blow the whistle. However, being at the bottom also means that they are the most restricted as the influence of those higher up means that these workers have a

limited capacity – both physically and mentally – to dissent (Blass, 2000). They could also express concerns about their own physical safety when in a foreign location, though once secure the obligation would return. Whereas CIA managers had both a great obligation to act and the ability to do so, but were the least likely as they were the orchestrators of the torture regime. They therefore face the greatest blame for not acting. Finally, those political elites who either knew or who failed to investigate further should also face a significant obligation having a great responsibility and given their privileged position that provided them the means, opportunity to act with limited backlash, meaning that they too face a significant degree of blame for not speaking out.

Conclusion

The case of Edward Snowden brought to the fore need for a debate on what sort of oversight should exist on the intelligence community. There is no culture or framework within intelligence that details exactly when whistleblowing might be used as a means of limiting unjustified harms that certain policies might cause. While in a perfect scenario this might not be necessary, the fundamental flaws of the current oversight mechanisms coupled with the power of intelligence actors and the tendency for overly secretive environments to distort what practices appear appropriate, means that additional safeguards are needed within the the system;ones that allow those who already have direct access to intelligence information the guideance to know when they should speak out.

What is key, however, is that proliferate whistleblowing is not a benefit to society or the intelligence community's objective to protect others. Rather, in order for whistleblowing to be justified, the harm being caused by the intelligence community should be such that it cannot be justified, and that the act of whistleblowing is the best remedy. What is innovative about this is that it establishes an obligation to blow the whistle when the intelligence is aware of unjustified harm being caused, but that this obligation is then mediated by the additional proportionality calculations and the different forms the whistleblowing can take. It therefore does allow for some harms as an inherent part of intelligence but recognises that there needs to be limits on this by providing a means for examining when whistleblowing as an act itself is justified through detailing the different expectations to act that actors face; a way of balancing the benefits and harms that whistleblowing can bring; and finally, a more flexible means of proceeding with different whistleblowing forms depending on the circumstances involved.

Acknowledgements

The author thanks Alasdair Cochrane for his helpful feedback on earlier versions of the article and the University of Sheffield Political Theory Research Group for their insightful thoughts and comments.

Notes

1. This distinguishes the article from that of William Scheuerman (2014) who argues for whistleblowing as a justified form of civil disobedience and so comes with the weaker requirement to act alongside existing political avenues rather than highlighting the need for ethical action and offering whistleblowing as an additional requirement.

2. For works on the psychological impact of closed-off and secret groups, see Bandura (1999: 194), Bandura (1986: 376), Leynes et al. (2003), Mullen et al. (1992), Struch and Schwartz (1989), Johnson (1986), Waller (2002), Zimbardo (2008) and Fein (2007: 11).
3. Wiretaps in United Kingdom require a warrant that must be authorised by the Secretary of State, see the Regulation of Investigatory Powers Act 2000, Chapter 23, Part 1, Chapter 1, x6(1). In the United States, wiretaps must be authorised 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.
4. For example, the state secrets privilege as the Supreme Court held in *United States v. Reynolds* prevents disclosure of information in court proceedings when 'there is a reasonable danger that compulsion of the evidence will expose matters which, in the interest of national security, should not be divulged' (1953: 345 U.S. 1, 10). For examples of this right being extended, see *Halkin v. Helms, 598 F.2d 1 (D.C. Cir., 1979*); *Maxwell v. First National Bank of Maryland*, 143 F.R.D. 590 (Dist. of Maryland, 1991); *Barlow v. United States*, (2000: Court of Federal Claims. Cong. Reference No. 98-887X) (; *Patterson v. FBI*, 893 F.2d 595 (3rd Cir., 1990); *Molerio* v. *Federal Bureau of Investigation*, 749 F.2d 815 (D.C. Cir., 1984); *Sterling v. Tenet* Civil Action No. Ol-CIV-8073 (S.D. New York, 2002); *Tilden* v. *Tenet*, 140 F. Supp 2d 623 (E.D. Virginia, 2000). For other examinations on the role of the courts, see Horowitz (1977: 148); Pozen (2005, 2010); Chesney (2007); and Uhl (2003).
5. For the role of the right to appeal and the importance of multi-layered court systems, see Dalton (1985), Lennerfors (2007) and Nobles and Schiff (2002).
6. Rawls (1971: 111, 1520); Smith (1976: 9); Mack (1980: 235). There is an extensive literature regarding the expectations of the good or minimal Samaritan; see Singer (1972); Gewirth (1978); Smith (1990); Whelan (1991); and Copp (1991). For the concept of harm, see Feinberg (1984: 166)
7. This is similar to Candice Delmas' (2015) 'subject condition' which states that the 'allocation of state power [in regards to preventing whistleblowing] is overridden when secrecy threatens or stains political legitimacy' (2015: 97). However, there is an important distinction, in that this comes with a reliance democracy as the ethical foundation (Delmas, 2015: 79) and information releases are an attempt to ensure more effective democratic governance (2015: 97). It does not, however, outline how to distinguish between what information the public should know for true democratic engagement (as this leads down the road of full transparency) and what should be kept secret. It is being argued here, however, that witnessing harm is the ethical foundation of the obligation to reveal and so does not rely on the virtues of transparency in a democracy. This gives a stricter obligation to act but with a more specific focus on social, political and ethical harms.
8. Feinberg calls these requirements 'welfare interests' and John Rawls calls them 'primary goods', but essentially they both amount to the same thing, that is, regardless of what conception of the good life the individual holds or what his life plans might be in detail, these preconditions must be satisfied first in order to achieve them. If these vital interests fall below a threshold level, the ability to realise the more ultimate needs, goals or activities can become dramatically hindered. In this way, these are the most important interests a person has, and thus, cry out for protection; see Feinberg (1984: 37) and Rawls (1971: 62).
9. There are whistleblower laws that are designed for encouraging such activity in other parts of government that are not applicable to NSAs. For example, Congress passed both the Financial Institutions Reform, Recovery and Enforcement Act of 1989, 12 U.S.C. sec. 1831k (Supp.I I 1990) and Insider Trading and Securities Fraud Enforcement Act of 1988, 15 U.S.C. sec. 78u-l(e) (1988) with the objective of minimising financial mismanagement and embezzlement as a key concern; see Morehead Dworkin and Near (1997).

10. Indeed, Delmas (2015) argues that an integral part of the government whistleblower is that the internal mechanisms should be used as the first step as part of her 'act condition' (2015: 98). Also see Glazer and Glazer (1989) and Heacock and McGee (1986).
11. This poisoning effect is essentially akin to the just war distinction between *ad bellum* and *in bello*, whereby unethical practice in war can poison the initial justification for starting the war. However, the need for sanitisation can be seen as similar to that as Delmas's (2015) minimalisation criteria whereby it is argued that there is 'a duty on the part of the whistleblower to minimise the harms that might result from the disclosure. To wit, the agent ought to exercise due care when releasing the information' (2015: 100).
12. *Geneva Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, United Nations, 10 December (1984); Rome Statute of the International Criminal Court, Article 7 §1 (f) Available at http://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf; Accessed 13 December 2013.
13. For debates on torture arguably knowable to those at the time, see Shue (1978), Amnesty International (1973), Conroy (2001), and Hooks and Mosher (2002). For results from both controlled and uncontrolled studies have shown substantial evidence that for some individuals, torture has serious and long-lasting psychological effects, see Basoglu et al. (2001), De Jong et al. (2001), Priebe and Bauer (1995), and Silove et al. (2002).

References

Aftergood S (2009) Reducing government secrecy: Finding what works. *Yale Law and Policy Review* 27(2): 407–408.

Amnesty International (1973) *Amnesty International: Report on Torture*. London: Duckworth.

Aquinas T (2002) Summa Theologiae. In: Brown C, Nardin T and Rengger N (eds) *International Relations in Political Thought*. Cambridge: Cambridge University Press, pp. 213–220.

Baldino D (2010) *Democratic Oversight of Intelligence Services*. Sydney, NSW, Australia: The Federation Press.

Bandura A (1986) *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura A (1999) Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review* 3: 193–209.

Basoglu M, Jaranson JM, Mollica R, et al. (2001) Torture and mental health: A research overview. In: Gerrity E, Keane TM and Tuma F (eds) *The Mental Health Consequences of Torture*. New York: Kluwer, pp. 35–62.

Bellaby R (2014) *The Ethics of Intelligence: A New Framework*. London: Routledge.

Bellaby R (2016a) Justifying cyber-intelligence? *Journal of Military Ethics* 15(4): 309–314.

Bellaby R (2016b) Torture-Lite: An ethical middle-ground? *International Journal of Applied Philosophy* 29(2): 117–190.

Bennetto J (2009) *Police and Racism: What Has Been Achieved 10 Years after the Stephen Lawrence Inquiry Report?* London: Equality and Human Rights Commission. Available at: https://www.equalityhumanrights.com/en/file/6316/download?token=4QCFPaJj (accessed 1 July 2015).

Blanton T (2003) *National Security and Open Government in the United States: Striking the Right Balance*. New York: Campbell Public Affairs Institute.

Blass T (2000) *Obedience to Authority: Current Perspectives on the Milgram Paradigm*. London: Lawrence Erlbaum.

Bok S (1985) Distrust secrecy and the arms race. *Ethics* 95(3): 712–727.

Born H and Leigh I (2005) *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight Agencies*. Oslo: Publishing House of the Parliament of Norway.

Bradley M and Schipani C (1989) The relevance of the duty of care standard in corporate governance. *Iowa Law Review* 75(1): 1–74.

Brenkert GC (2010) Whistle-Blowing moral integrity and organizational ethics. In: Brenkert GC and Beauchamp TL (eds) *The Oxford Handbook of Business Ethics*. New York: Oxford University Press, pp. 563–601.

Chesney R (2007) State secrets and the limits of national security litigation. *George Washington Law Review* 75(5): 1249–1332.

Church Committee Final Report Book 1 p.344. Available at: http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm (accessed 4 April 2016).

Conroy J (2001) *Unspeakable Acts Ordinary People: The Dynamics of Torture*. London: Vision Paperbacks.

Copp D (1991) Responsibility for collective inaction. *Journal of Social Philosophy* 22(2): 71–80.

Costanzo M and Gerrity E (2009) The effects and effectiveness of using torture as an interrogation device: Using research to inform the policy debate. *Social Issues and Policy Review* 3(1): 179–210.

Dacre P (2009) Review of the 30 year rule page. Available at: http://webarchive.nationalarchives.gov.uk/20090516124148/http:/www2.nationalarchives.gov.uk/30yrr/30-year-rule-report.pdf (accessed 12 January 2016).

Dalton HL (1985) Taking the right to appeal (more or less) seriously. *The Yale Law Journal* 95(1): 62–107.

De Jong JT, Komproe IH, Van Ommeren M, et al. (2001) Lifetime events and posttraumatic stress disorder in four post-conflict settings. *Journal of the American Medical Association* 286: 555–562.

DeGeorge RT (1990) *Business Ethics*. New York: Macmillan.

Delmas C (2015) The ethics of government whistleblowing. *Social Theory and Practice* 41(1): 77–105.

Dempsey JX and Flint LM (2004) Commercial data and national security. *The George Washington Law Review* 72: 1459–1502.

Dershowitz A (2002) *Why Terrorism Works: Understanding the Threat Responding to the Challenge*. London: Yale University Press.

Diffie W and Landau S (1998) *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press.

Dworkin TM and Near J (1997) A better statutory approach to whistleblowing. *Business Ethics Quarterly* 7(1): 1–16.

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

Feinberg J (1984) *Moral Limits of the Criminal Law: Volume 1 Harm to Others*. Oxford: Oxford University Press.

Finn P (2009) GOP senators drop out of panel inquiry into CIA program. *The Washington Post*, 26 September. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/09/25/AR2009092503745.html (accessed 15 February 2016).

Fluri P and Born H (2003) *Parliamentary Oversight of the Security Sector: Principles Mechanisms and Practices*. (Handbook for Parliamentarians Nr. 5), Inter-Parliamentary Union and Geneva Centre for the Democratic Control of Armed Forces.

Gadlin G (1998) Can you whistle while you work? Commentary on "How to blow the whistle and still have a career afterwards". *Science and Engineering Ethics* 4: 65–69.

Gandy O (2003) Data mining and surveillance in the post 9/11 environment. In: Bell K and Webster F (eds) *The Intensification of Surveillance: Crime Terrorism and Warfare in the Information Age*. Pluto Press, pp. 26–41.

Gellman B and Poitras L (2013) U.S. British intelligence mining data from nine U.S. internet companies in broad secret program. *The Washington Post*, 6 June. Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed 8 June 2013).

Gewirth A (1978) *Reason and Morality*. Chicago, IL: University of Chicago Press.

Glazer MP and Glazer PM (1989) *The Whistle-Blowers Exposing Corruption in Government and Industry*. New York: Basic Books.

Goldenberg S (2013) Al Gore: NSAs secret surveillance program not really the American way. *The Guardian*, 14 June. Available at: http://www.theguardian.com/world/2013/jun/14/al-gore-nsa-surveillance-unamerican (accessed 3 March 2016).

Greenwald G (2014) *No Place to Hide Edward Snowden the NSA and the Surveillance State*. London: Hamish Hamilton.

Greenwald G and MacAskill E (2013) NSA prism program taps in to user data of Apple Google and others. *The Guardian*, 7 June. Available at: http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (accessed 8 June 2013).

Griswold E (1989) Secrets not worth keeping: The courts and classified information. *The Washington Post*, 15 February. At A25.

Heacock MV and McGee GW (1986) Whistleblowing: An ethical issue in organisational and human behaviour. *Business & Professional Ethics Journal* 6: 35–41.

Herman M (2000) Modern intelligence services: Have they a place in ethical foreign policies? In: Shukman H (ed.) *Agents for Change: Intelligence Services in the 21st Century*. London: St Ermin's Press, pp. 287–310.

Hirsch A (2000) The ethics of public television surveillance. In: Hirsch A, Garland D and Wakefield A (eds) *Ethical and Social Perspectives on Situational Crime Prevention*. Oxford: Hart Publishing, pp. 59–76.

Hoffman W (1984) The Ford Pinto. In: Hoffman W and Moore J (eds) *Business Ethics: Readings and Cases in Corporate Morality*. Chichester: John Wiley & Sons, pp. 249–260.

Hollyer JB, Rosendorff P and Vreelandm JR (2007) Democracy and transparency. *Journal of Politics* 73(4): 1191–1205.

Hooks G and Mosher C (2002) Outrages against personal dignity: Rationalizing abuse and torture in the war on terror. *Social Forces* 83(4): 1627–1646.

Horowitz D (1977) The courts as guardians of the public interest. *Public Administration Review* 37(2): 148–154.

Horsey HR (1994) The duty of care component of the Delaware business judgment rule. *Delaware Journal of Corporate Law* 19(3): 971–998.

International Committee of the Red Cross (2007) ICRC report on the treatment of fourteen "high value detainees" in CIA custody, February. Available at: http://www.nybooks.com/media/doc/2010/04/22/icrc-report.pdf (accessed 1 February 2015).

Jarvis R (2006) Reports, politics and intelligence failures: The case of Iraq. *Journal of Strategic Studies* 29(1): 3–52.

Jensen JV (1987) Ethical tension points in whistleblowing. *Journal of Business Ethics* 6(4): 321–328.

Johnson R (1986) Institutions and the promotion of violence. In: Campbell A and Gibbs J (eds) *Violent Transactions: The Limits of Personality*. Oxford: Oxford University Press, pp. 181–205.

Joint Security Commission (1994) Redefining security dealing with sensitive but unclassified information 28 February. Prepared for the Director of the CIA by the Secretary of Defense. Available at: http://www.fas.org/sgp/library/jsc/ (accessed 16 May 2016).

Jos P, Tompkins M and Hays S (1989) In praise of difficult people: A portrait of the committed whistleblower. *Public Administration Review* 49(6): 552–561.

Keefe PR (2005) *Chatter: Dispatches from the Secret World of Global Eavesdropping*. New York: Random House.

Kelley M (2013) NSA: Snowden stole 1.7 million classified documents and still has access to most of them. *Business Insider*, 13 December. Available at: http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12?IR=T (accessed 14 May 2014).

Kleinig J (1976) Good Samaritanism. *Philosophy & Public Affairs* 5(4): 385.

Kono D (2006) Optimal obfuscation: Democracy and trade policy transparency. *American Political Science Review* 100: 369–384.

Landau S (2013) Making sense from Snowden: What's significant in the NSA surveillance revelation. *Spotlight*, July/August. 54–63.

Lennerfors T (2007) The transformation of transparency: On the act on public procurement and the right to appeal in the context of the war on corruption. *Journal of Business Ethics* 73(4): 381–390.

Leyens JP, Cortes B, Demoulin S, et al. (2003) Emotional prejudice essentialism and nationalism: The 2002 tajfel lecture. *European Journal of Social Psychology* 33(6): 703–717.

Liu E, Nolan A and Thompson R (2015) Overview of constitutional changes to NSA collection activities. *Congressional Research Service*, 21 May. Available at: https://fas.org/sgp/crs/intel/R43459.pdf (accessed 15 February 2016).

Luban D (2005) Liberalism, torture and the ticking-bomb. *Virginia Law Review* 91: 1425–1461.

McGlynn J and Richardson BK (2014) Private support public alienation: Whistle-Blowers and the paradox of social support. *Western Journal of Communication* 78(2): 213–237.

Mack E (1980) Bad Samaritanism and causation of harm. *Philosophy & Public Affairs* 9(3): 230–259.

Macnish K (2015) An eye for an eye: Proportionality and surveillance. *Ethical Theory & Moral Practice* 18(3): 529–548.

Marx G (2004) Some concepts that may be useful in understanding the myriad forms and contexts of surveillance. *Intelligence and National Security* 19(2): 226–248.

Matthews R (2012) An empirical critique of "interrogational" torture. *Journal of Social Philosophy* 43(4): 457–470.

Mazzetti M (2015) C.I.A. report found value of brutal interrogation was inflated. *The New York Times*, 20 January. Available at: http://www.nytimes.com/2015/01/21/world/cia-report-found-value-of-brutal-interrogation-was-inflated.html?_r=1 (accessed 15 February 2016).

Mill JS (2005) *On Liberty*. New York: Cosimo.

Miller R (2016) Intelligence oversight – Made in Germany. In: Goldman Z and Rascoff S (eds) *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford: Oxford University Press, pp. 257–288.

Mullen B, Brown R and Smith C (1992) In-group bias as a function of salience relevance and status: An integration. *European Journal of Social Psychology* 22: 103–122.

Nobles R and Schiff D (2002) The right to appeal and workable systems of justice. *The Modern Law Review* 65(5): 676–701.

Norman R (1995) *Ethics Killing and War*. Cambridge: Cambridge University Press.

Pfaff T and Tiel J (2004) The ethics of espionage. *Journal of Military Ethics* 3(1): 1–15.

Phythian M (2016) An INS special forum: The US senate select committee report on the CIAs detention and interrogation program. *Intelligence and National Security* 31(1): 8–27.

Pozen D (2005) The mosaic theory national security and the freedom of information act. *The Yale Law Journal* 115(3): 628–679.

Pozen D (2010) Deep secrecy. *Stanford Law Review* 62(2): 257–340.

Priebe S and Bauer M (1995) Inclusion of psychological torture in PTSD criterion. *American Journal of Psychiatry* 152: 1691–1692.

Quinlan M (2000) The future of covert intelligence. In: Shukman H (ed.) *Agents for Change: Intelligence Services in the 21st Century*. London: St Ermin's Press, pp. 61–70.

Rawls J (1971) *Theory of Justice*. Cambridge: Cambridge University Press.

Rothschild J and Miethe T (1999) Whistle-Blower disclosures and management retaliation. *Work and Occupations* 26(1): 107–128.

Rubinstein I, Lee D and Schwartz P (2008) Data-Mining and internet profiling: Emerging regulatory and technological approaches. *The University of Chicago Law Review* 5(1): 261–285.

Sample I (2016) Even basic phone logs can reveal deeply personal information researchers find. *The Guardian*, 16 May. Available at: https://www.theguardian.com/science/2016/may/16/even-basic-phone-logs-can-reveal-deeply-personal-information-researchers-find (accessed 16 May 2016).

Sanger D (2014) New N.S.A. chief calls damage from Snowden leaks manageable. *The New York Times*, 29 June. Available at: http://www.nytimes.com/2014/06/30/us/sky-isnt-falling-after-snowden-nsa-chief-says.html?_r=0 (accessed 1 March 2015).

Sawers J (2010) The need for secrecy in the intelligence services. *The Guardian*, 28 October. Available at: http://www.theguardian.com/uk/2010/oct/28/sir-john-sawers-speech-full-text (accessed 5 April 2015).

Scheffler S (1985) Agent-Centerd restrictions rationality and the virtues. *Mind* 94(375): 409–419.

Scheuerman W (2014) Whistleblowing as civil disobedience: The case of Edward Snowden. *Philosophy & Social Criticism* 40(7): 609–628.

Schmitt E and Schmidt M (2013) Qaeda plot leak has undermined U.S. intelligence. *The New York Times*, 29 September. Available at: http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html (accessed 7 May 2014).

Shafer J (2014) Live and let leak: State secrets in the Snowden era. *Foreign Affairs*, March/April. Available at: https://www.foreignaffairs.com/reviews/review-essay/live-and-let-leak (accessed 20 May 2014).

Shane S and Sanger D (2013) Job title key to inner access held by Snowden. *The New York Times*, 30 June. Available at: http://www.nytimes.com/2013/07/01/us/job-title-key-to-inner-access-held-by-snowden.html (accessed 17 May 2014).

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

Shue H (1978) Torture. *Philosophy & Public Affairs* 7(2): 124–143.

Shulsky AN (2002) *Silent Warfare: Understanding the World of Intelligence*. Washington, DC: Brasseys.

Silove DM, Steel Z, McGorry PD, et al. (2002) The impact of torture on posttraumatic stress symptoms in war-affected Tamil refugees and immigrants. *Comprehensive Psychiatry* 43: 49–55.

Singer P (1972) Famine affluence and morality. *Philosophy & Public Affairs* 7(2): 229–243.

Smith A (1976) *The Theory of Moral Sentiment*. Oxford: Clarendon Press.

Smith P (1990) The duty to rescue and the slippery slope problem. *Social Theory and Practice* 16(1): 19–41.

Solove D (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

Struch N and Schwartz S (1989) Intergroup aggression: Its predictors and distinctness from in-group bias. *Journal of Personality and Social Psychology* 56(3): 364–373.

The Washington Post (2013) NSA slides explain the PRISM data-collection program, 10 July. Available at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed 14 May 2014).

Thompson D (1999) Democratic secrecy. *Political Science Quarterly* 114(2): 182–356.

Uhl K (2003) The Freedom of Information Act Post 9/11: Balancing the public right to know critical infrastructure protecting and homeland security. *American University Law Review* 53(1): 261–311.

US Senate Select Committee on Intelligence (2014) Committee study of the central intelligence agency's detention and interrogation program, 3 December. Available at: http://fas.org/irp/congress/2014_rpt/ssci-rdi.pdf (accessed 1 February 2015).

Waller J (2002) *Becoming Evil: How Ordinary People Commit Genocide and Mass Killing*. Oxford: Oxford University Press.

Walzer M (2000) *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books.

Weaver W and Pallitto R (2005) State secrets and executive powers. *Political Science Quarterly* 120(1): 85–112.

Wells C (2004) National security and the freedom of information act. *Administrative Law Review* 56(4): 1195–1222.

Whelan JM (1991) Charity and the duty to rescue. *Social Theory and Practice* 17(3): 441–456.

Whitehead T (2013) GCHQ leaks have gifted terrorists ability to attack at will warns spy chief. *The Guardian*, 9 October. Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10365026/GCHQ-leaks-have-gifted-terrorists-ability-to-attack-at-will-warns-spy-chief.html (accessed 7 May 2014).

Whitehead T, Rayner G and Swinford S (2013) Terrorists are 'rubbing their hands with glee' after Edward Snowden Leaks. The Telegraph 7 November. Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10434196/Terrorists-are-rubbing-their-hands-with-glee-after-Edward-Snowden-leaks.html. (accesses 9 May 2014).

Winfield M (1994) Whistle-blowers as corporate safety net. In: Vinten G (ed.) *Whistleblowing: Subversion or Corporate Citizenship?* New York: St. Martin's Press, pp. 33–41.

Zimbardo P (2008) *The Lucifer Effect: How Good People Turn Bad*. London: Rider.

Author biography

Ross W Bellaby is a Lecturer in Security Studies at the University of Sheffield's Politics Department. His main research areas revolve around the application of ethics to violence and war, with specific attention to developing an ethical framework designed for the intelligence community. This involves research into intelligence, terrorism and counterterrorism, cybersecurity, the dark web and hackers, and creation and use of torture-lite. His ethical framework is set out in his book, *The Ethics of Intelligence: A New Framework* (Routledge, 2014).