Too Many Secrets?

When Should the Intelligence Community be Allowed to Keep Secrets

Abstract

In recent years revelations regarding reports of torture by the CIA and the unnoticed growth of the NSA's pervasive cyber-surveillance system have significantly brought into doubt the level of trust afforded to the intelligence community. Central to this is determining how much secrecy they should enjoy and what mechanisms should be employed to detect and prevent future abuse. This is not a call for complete transparency, however, as secret intelligence does play an important and ethical role in society. Rather, that existing systems built on a prioritisation of democratic assumptions are fundamentally ill-equipped for dealing with the particular challenge of intelligence secrecy. That, as the necessary circle of secrecy is extended around the political actors they are insulated from the very public gaze that ensures they are working in-line with the political community's best interests. Therefore, a new framework needs to be developed, one this paper will argue should be based on the just war tradition, where the principles of just cause, legitimate authority, last resort, proportionality and discrimination are able to balance the need to protect people while placing limits in terms of who can be harmed and to what degree.

Key Words: Secrets, ethics, intelligence, just war

Introduction

The debate on state secrets is an ethically charged one from the outset. Revelations regarding reports of torture by the CIA and the unnoticed growth of the NSA's pervasive cyber-surveillance system have significantly brought into doubt the level of trust afforded to the intelligence community. This paper is not a call for complete transparency, however, as this is both ethically problematic and inherently unworkable. Indeed, intelligence secrecy is a special type of state secrets, playing an important and ethical role in society by protecting both the individual and the political community, and without the ability to keep its tactics and the information it produces secret to some extent intelligence would be dramatically weakened. This means that ensuring a degree of secrecy is necessary. But this does not mean unrestrained action, as without some supervision the powers of the intelligence community can cause unjustified harm. This paper will

argue, however, that the existing oversight structures, built on a prioritisation of democratic assumptions, are fundamentally ill-suited to the task. That, as the necessary circle of secrecy is extended around the political actors they are insulated from the very public gaze that ensures they are working in-line with the political community's best interests. Furthermore, it will be argued that the security mentality that surrounds intelligence activity means that demands based on a need to prevent national security threats overrides any requirement for a more informed public. This mentality therefore distorts the debate and further undermines the oversight process. Therefore, a new framework needs to be developed, one this paper will argue should be based on the just war tradition. Indeed, the just war tradition is well versed in examining debates on security, balancing the necessity to protect the people and the harm that such activities can cause to both the individual and political community while placing limits in terms of who can be harmed and to what degree. After examining the shortcomings in the current theoretical foundations and their problematic practical applications, this paper will establish an ethical framework based on the principles of last resort, legitimate authority, just cause, proportionality and discrimination offering a key original theoretical contribution to the field. Indeed, this paper will argue that protecting the political community and the individuals within it is the at heart of the principle of legitimate authority, and as the sphere of secrecy undermines and poisons existing democratic structures a new set of systems based on societal experts and representatives offers a means of better protecting the interests of the political community. This will work with the principle of last resort to place the emphasis on the intelligence community to present their case to this independent legitimate authority as to why the information should be retained, rather than outsiders asking for its release. Whereas the principle of just cause will recognise the importance of intelligence secret keeping to prevent threats from harming the political community as a form of pre-emptive self-defence, while also arguing that this does not mean focusing only on traditional conceptions of national security, but recognising that protecting the political community is more than just protecting the state and includes its ethical, moral, social and legal norms. This, in conjunction with the principle of proportionality, ensures that all the different conceptions of threat and harm are included in the ethical calculation. Finally, the principle of discrimination will argue, first, that different groups of individuals have various claims to be informed depending on the type of information retained and how they were involved or impacted, and second, will work with the principle of last resort to argue that those

individuals who are unaware of their involvement in an intelligence operation should be actively sought out and informed.

Advancing a framework based on the just war tradition in this way will allow for the development of an evaluative framework that can understand the ethical role secrecy can play while also setting out limits on when it should be used, the level of harm allowed and the different obligations it has to various individuals. This will be applied to a series of key examples covering operational and strategic intelligence asking if, what and when information should be released.

Secrecy, Democracy, and Intelligence

When examining the topic of state secrecy three questions are raised: why should we have transparency or be allowed to keep secrets; what secrets should be kept and what information should be released; and how do we go about ensuring that the correct information is revealed or locked away. The first two questions ask us to determine what normative basis we should be guided by, while the last points towards what institutional mechanisms these normative assumptions then create. However, while there is strong work on the normative value of secrecy most broadly,[1] works that specifically question its place within government activity have been dominated by debates on the importance of transparency and democracy.[2] For intelligence oversight this is even more pronounced with much of the literature examining and working within existing democratic assumptions and the frameworks they create, asking how different branches of government are suited for the task of monitoring the intelligence community's extraordinary range of powers and extraordinary level of secrecy.[3] This is not surprising given that much of democratic theory's

[1] Sissela Bok, Secrets: On the Ethics of Concealment and Revelation (New York: Vintage Books, 1989); Georg Simmel, 'The Sociology of Secrecy and of Secret Societies' The American Journal of Sociology 11/4 (1906): 441-498; Stanton Tefft, Secrecy, a Crosscultural Perspective (New York: Human Sciences Press, 1980).

[2] This is Susan Maret's general argument, see Susan Maret, 'Introduction: Government Secrecy' in Government Secrecy (Research in Social Problems and Public Policy, Volume 19) edited by Susan Maret (Emerald Group Publishing Limited, 2011): xi. For government secrecy generally see Simone Chambers, 'Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation' The Journal of Political Philosophy 12/4 (2004): 389-410; Ian Shapiro, The Moral Foundations of Politics (New Haven, CT: Yale University Press, 2003); Dennis F. Thompson, 'Democratic Secrecy' Political Science Quarterly 114/2 (1999): 181-193; David E. Pozen, 'Deep Secrecy' Stanford Law Review 62/2 (2010): 257-340; Jennifer Earl, 'Information access and protest policing post-9/11: Studying the policing of the 2004 Republican National Convention' American Behavioral Scientist 53 (2009): 44–60; Itzhak Galnoor, 'What Do We Know About Government Secrecy' in Government Secrecy in Democracies, edited by Itzhak Galnoor (New York: New York University Press, 1977): 275–313; J. Fulbright, 'The High Cost of Secrecy' The Progressive, 35/9 (1971): 16–21.

[3] For works not discussed directly elsewhere see Simon Chesterman, One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty (Oxford: Oxford University Press, 2011); J. William Leonard, 'The Corrupting Influence of Secrecy on National Policy Decisions' Government Secrecy (Research in Social Problems and Public Policy, Volume 19) edited by Susan Maret (Emerald Group Publishing Limited, 2011): 421-434; Fred Schreier, 'The Need for Efficient and Legitimate Intelligence', in Democratic Control of Intelligence Services: Containing Rogue Elephants edited by Hans Born and Marina Caparini (London: Routledge, 2016): 25-44, at 36, 37; Marina Caparini, 'Controlling and Overseeing Intelligence Services in Democratic States', in Democratic Control of Intelligence Services: Containing Rogue Elephants edited by Hans Born and Marina Caparini (London: Routledge, 2016): 3-24; Zachary K. Goldman and Samuel J. Rascoff, Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford: Oxford University Press, 2016); Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies (Oslo: Parliament of Norway, 2005): 55-59; Hans Born, Loch Johnson, and Ian Leigh, Who's Watching the Spies (editors) (Washington: Potomac Books Inc, 2005).

intellectual history has engaged heavily with the question of what role secrecy should or should not have as well as designing systems to prevent the harmful effects of state activity. So, while there are important utilitarian arguments made on the instrumental harms of secrecy and the good offered by transparency – dating back to Jeremy Bentham,[4] arguing that openness provides better policies and social norms through a more engaged and reflective process – many of these have become synonymous with the good found within an engaged and deliberative democratic process as a whole.[5] Indeed, from classical liberals such as John Stuart Mill and John Locke arguing that oversight is a fundamental part of a meaningful representative body;[6] through to John Rawls placing transparency as a key means of ensuring a just society as well as a means to monitor established institutions,[7] to contractarians arguing the need for governments to give account and justify decisions to the community,[8] there is an entrenched heritage arguing for the need for transparency in a democracy. Key amongst such arguments is the position that 'The public, as sovereign, must have all information available in order to instruct its servants, the government. As a general proposition, if democracy is to work, there can be no holding back of information; otherwise ultimate decision making by the people, to whom that function is committed, becomes impossible'.[9] Secrecy limits access to information and in doing so undermines the people's role as the sovereign power; the Madisonian argument that 'meaningful participation in democratic processes requires informed participants. Secrecy reduces the information available to the citizenry, hobbling their ability to participate *meaningfully'*.[10] Secrecy is therefore considered wrong in as much as it challenges democracy by delaying its processes, limiting engagement, or weakening an individual's role. Furthermore, there is a recognition that government decision-makers, like all humans, are fallible. For this reason, public scrutiny is the most effective check on individual shortcomings, a point made by Mill: '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'.[11] Indeed Daniel Kono argues that because 'democratic governments will emphasise policy

[4] See Jeremy Bentham, Political Tactics, edited by Michael James, Cyprian Blamires, and Catherine Pease-Watkin (Oxford, Oxford University Press, 1999): 29-44
[5] Mark Fenster, 'The Opacity of Transparency' Iowa Law Review 91 (2006): 885-949.
[6] John Stuart Mill, Considerations on Representative Government (London: Parker, Son, and Bourn, 1861): 104; for a discussion on transparency in Locke's work see Ajume H. Wingo, Veil Politics in Liberal Democratic States (Cambridge, Cambridge Univeristy Press): 16-18.
[7] John Rawls, A Theory of Justice (Cambridge Mass: Harvard University Press, 1971): 16, 454; John Rawls, Political Liberalism (New York, Columbia University Press, 1993): 35, 68.
[8] Amy Guttman and Dennis Thompson, Democracy and Disagreement (Harvard University Press, 1996): 100-01; Joshua Cohen, 'Democracy and Liberty', in Deliberative Democracy edited by Jon Elster (Cambridge, Cambridge University Press, 1998): 185-231, at 185, 193-94.
[9] Thomas Emerson, 'The First Amendment and the Right to Know: Legal foundations of the Right to Know', Washington University Law Quarterly, 1 (1976): 14.
[10] Joseph Stiglitz, 'On Liberty, the Right to Know, and Public Discourse: The Role of Transparency in Public Life' in Globalising Rights: Oxford Amnesty Lecture 1999 (1999): 125. Emphasis in original.
[11] John Stuart Mill, On Liberty (New York, Cosimo, 2005): 138.

decisions that please voters while hiding those which go against the will of the majority' greater transparency is needed to ensure participation is based on correct information.[12] The normative value found within transparency over secrecy according to democratic theory, therefore, is enabling engaged sovereignty and preventing abuse of authority.

From answering this first question democratic theory places a dominant emphasis on engaged transparency in determining what should be kept secret: instilling an open framework so that all decisions can be made in-line with the beliefs and values of the community served, underpinning the importance of popular sovereignty: 'an action or policy that cannot withstand publicity is one that cannot garner popular consent, and that is why the action is wrong'.[13] Where transparency cannot be guaranteed then decision-makers should act as if it could be. This promotes the publicity principle, Kant's argument that the first test for a political maxim is to ask oneself 'could I still get away with this if my action and reason for doing it were publically known?'.[14] Indeed, Simone Chambers argues, 'All theories of deliberative democracy contain something that could be called a publicity principle', whereby determining what secrets should be kept involves 'having to defend one's policy preferences in public' so that the decision 'leans one towards using public reason' or 'reasons that this public at large could accept'.[15] Such a principle 'encourages participants to examine their own beliefs and arguments', promoting critical self-reflection within decision-makers, while also conferring legitimacy as the policy 'ought be to in the general interest'.[16] For Jon Elster and Joshua Cohen this will therefore limit the private reason of individual maximisers; while Rawls and Seyla Benhabib are concerned, for very different reasons, about 'the private reason of particular moral, religious, or cultural world-views'.[17] This, therefore, supports social virtues such as freedoms of speech, assembly and press[18] with value stated in terms of instrumental procedural benefits or the promotion of social goods such as liberty, morality, or equality.[19] Arguments for the benefits of secrecy in

[12] Daniel Kono, 'Optimal Obfuscation: Democracy and Trade Policy Transparency', American Political Science Review 100 (2006): 369–384
[13] David Luban, 'The Publicity Principle' in The Theory of Institutional Design edited by Robert E. Goodin (Cambridge: Cambridge University Press, 1998): 192
[14] David Luban, 'The Publicity Principle' (1998): 156
[15] Simone Chambers, 'Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation' The Journal of Political Philosophy 12/4 (2004): 390
[16] Simone Chambers 'Behind Closed Doors' (2004): 390
[17] Simone Chambers 'Behind Closed Doors' (2004): 392
[18] Robert Dahl, Polyarchy: Participation and Opposition (New Haven: Yale University Press, 1971)
[19] J. Schumpeter, Capitalism, Socialism and Democracy (New York: Harper and Row, 1956). For instrumental arguments see John Stuart Mill, 1861, Considerations on Representative Government (Buffalo, NY: Prometheus Books, 1991): 74; J. Elster, 'The Market and the Forum: Three Varieties of Political Theory' in Philosophy and Democracy, ed. T. Christiano, (Oxford: Oxford University Press, 2002): 152; and Amartya Sen, Development as Freedom (New York: Knopf, 1999): 152. For non-instrumental see Carol Gould, Rethinking Democracy: Freedom and Social Cooperation in Politics, Economics and Society (New York: Cambridge University Press, 1988): 45-85; Joshua Cohen, 'Procedure and Substance in Deliberative Democracy' in Philosophy and Democracy, ed. T. Christiano, (Oxford: Oxford University Press, 2002): 17-38, at 21; Peter Singer, Democracy and Disobedience (Oxford: Oxford University Press, 1973): 30-41; J. Waldron Law and Disagreement (Oxford: Oxford University Press, 1999); and T. Christiano, 'The Authority of Democracy' Journal of Political Philosophy, 12/3 (2004): 266-290.
[19] Amartya Sen, Development as Freedom (1999): 152.

a democracy are possible but limited to instances of aiding in processes and furthering its own democratic ends: 'Juries and judicial panels, subcommittees and caucus meetings, peace negotiations and trade agreements, constitution writing and rights statements, not to mention hiring and admission committees, are just a few examples of where we might think it appropriate to close the doors and exclude the public'.[20]

However, while this work on democracy is incredibly strong it can be problematic when examined in relation to intelligence. Firstly, in answering why we should (not) keep secrets, the ethical end for intelligence is to protect the political community from threats, not to aid in the democratic agenda.[21] The good found within secret intelligence is not that it aids the democratic process but is the degree it acts as a direct positive in providing for the security of the political community by locating and preventing the realisation of threats. While the harm with keeping secrets is not the limitation it has on public engagement per se, but the impact it has directly on people's autonomy as well as the additional harms too much secrecy can promote. Autonomy is the ability to decide for oneself, without external manipulation or interference, what shape one's own life will take; that is, 'being able to form a conception of the good and to engage in critical reflection about the planning of one's life – the protection of the liberty of conscience'.[22] This autonomy requires that the individual's rational functioning be protected, maintaining the capacity to plan, choose, and reflect on options.[23] To be able to act according to their own reasoning all the way down.[24] This includes how people decide how they should act in regards to their important relationship with their polis. However, withholding information means people are unable to make a fully informed rational decision, forced to act based on the will of those withholding the necessary information. With intelligence secret keeping the distortion is both general in that the whole community is unable to decide how to make decisions in regards to its own intelligence actors, and specific in that those individuals who are unknowingly targeted or impacted are unable to decide how they specifically should react. Secondly, there are additional harms caused when secret organisations create insular environments, separated from review, which can cause an escalation of policies that violates people's liberty, privacy or physical and mental

[20] Simone Chambers, 'Behind Closed Doors' (2004): 392. Also see Mark Chinen, 'Secrecy and Democratic Decisions' Quinnipiac Law Review 27/1 (2009): 1-53, at 9.
[21] While arguments have been made that 'a democracy could decide to accept the possibility of incompletely-considered decisions now in the hopes of a better, and this in some sense freer and more meaningful decision, later' (Chinen, Secrecy and Democratic Decisions (2009): 10) and that 'If the public has voted to install any particular regime of secrecy, and thereby authorized certain officials to keep certain types of secrets in certain ways, those officials can be said to be carrying out their popular mandate when they do so'. David E. Pozen, 'Deep Secrecy' Stanford Law Review 62/2 (2010): 257-340, at 287. Critiques in terms of informed consent would undermine such arguments in a way that they would not in terms to the justification of intelligence for national security.
[22] Martha Nussbaum, Women and Human Development: The Capabilities Approach, (Cambridge: Cambridge University Press, 2000): 79.
[23] Harry Frankfurt, 'Freedom of the Will and the Concept of the Person', Journal of Philosophy, 68/1 (1971) p.7.
[24] Barbara Herman, The Practice of Moral Judgement (Harvard University Press, 1996): 228

integrity. This places the harm associated with keeping secrets in terms of the degree to which it violates the individual's sovereignty and damages their most vital interests.[25] Indeed, overly secretive environments separate those on the outside who are unaware and unable to engage, from those on the inside who are subjected to a process of in-group/out-group differentiation that dehumanises others and when coupled with a lack of outside input there is no differential means of measuring one's moral compass.[26] As a result, officers learn to exclude those considered as outsiders from their universe of obligation.[27] 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.[28] Secretive environments normalise the in-group/out-group differentiation 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, restricting alternative analysis as group-mentality smothers dissenting points of view.[29]

This is especially problematic in regards to intelligence as the perceived pressure of the security environment shapes the internal culture of an organisation as well as those oversight actors who are drawn into the special sphere of secrecy. This means that intelligence secrecy needs to be examined as a social and cultural problem so as to better understand Weber's impersonal and rational bureaucracy.[30] Indeed, the power of the security mind-set is such that when the answer to the question, 'why is transparency important' is a 'more informed public' and the answer to 'why intelligence should be allowed to keep secrets' is 'the protection of national security', then the latter is often given primacy. As a key example of securitisation, intelligence is still seen as quintessentially a topic for realpolitik,[31] and as a result is raised

[25] '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. Joel Feinberg, Moral Limits of the Criminal Law: Vol.1 Harm to Others (Oxford: Oxford University Press, 1984): 37; John Rawls, A Theory of Justice (Cambridge Mass: Harvard University Press, 1971): 62.

[26] Albert Bandura, 'Moral Disengagement in the Perpetration of Inhumanities' Personality and Social Psychology Review, 3/3 (1999): 193-209, at 194.

[27] Helen Fein, Human Rights and Wrongs: Slavery, Terror and Genocide (Boulder: Paradigm Publishers, 2007): 11

[28] Albert Bandura, Social Foundations of Thought and Action: A Social Cognitive Theory. (Englewood Cliffs, NJ: Prentice Hall, 1986): 376. Also see Leynes et al. 'Emotional Prejudice, Essentialism, and Nationalism', European Journal of Social Psychology 33/6 (2003): 703-717; Brian Mullen, Rupert Brown, and Colleen Smith, 'In-group Bias as a Function of Salience, Relevance, and Status: An Integration', European Journal of Social Psychology 22 (1992): 103-122; Naomi Struch, and Shalom Schwartz, 'Intergroup Aggression: Its Predictors and Distinctness From In-Group Bias', Journal of Personality and Social Psychology 56/3 (1989): 364-373; R. Johnson, 'Institutions and the Promotion of Violence' in Anne Campell and John Gibbs (eds) Violent Transactions: The Limits of Personality (Oxford: Oxford University Press, 1986); James Waller, Becoming Evil: How Ordinary People Commit Genocide and Mass Killing (Oxford: Oxford University Press, 2002); Philip Zimbardo, The Lucifer Effect: How Good People Turn Bad (London: Rider, 2008).

[29] US Senate Select Committee on Intelligence Committee Study of the Central Intelligence Agency's Detention and Interrogation Program (2014) Available at http://fas.org/irp/congress/2014_rpt/ssci-rdi.pdf [Accessed 1 February 2015]: 2.

[30] Max Weber, From Max Weber: Essays in sociology Edited and Translated by H. H. Gerth and C. W. Mills (New York: Oxford University Press, 1946, 1958). Also see Susan Maret 'Introduction: Government Secrecy' in Government Secrecy (Research in Social Problems and Public Policy, Volume 19) edited by Susan Maret (Emerald Group Publishing Limited, 2011): xi-xxx

[31] Michael Quinlan, 'Just Intelligence: Prolegomena to an Ethical Theory' Intelligence and National Security, 22/1 (2007): 1-13, at 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. Barry Buzan, Ole Waever and Jaap De Wilde, Security: A New

out of the political realm and placed in the extraordinary security sphere where normal political rules and concerns are not given the same consideration and weight. The tension created is such that, as Dennis Thompson notes, you are essentially left with two options, 'abandon the [security] policy or sacrifice democratic accountability';[32] and importantly a decision where national security is the trump card. As Eric Posner and Adrian Vermeule argue, there is a natural trade-off between civil liberties and security and that 'governments do – and should' make the trade to 'reduce civil liberties in order to enhance security' in times of emergency.[33] Security generally, and intelligence specifically, however, comes with a culture of constant emergencies, one that emerged throughout the Cold War and has continued under the War on Terror, reflecting a resurgence in Lasswell's 'garrison state' and the prioritisation of a security mind-set that privileges a militaristic culture and policy imperatives over other concerns.[34] This is matched by Cass Sustein's growth in a risk culture, distorting how threats such as terrorism are perceived, overemphasising their importance and degree of the threat, promoting fear and social decohesion within society while driving an escalation of security policy.[35] Such mentality means that the publicity principle can have limited use as it is not incongruous to believe one is doing what is best for the political community by adhering to the needs of national security. As David Luban notes, the restrictions of the publicity principle are subject to 'self-deception' as 'decision makers will undoubtedly persuade themselves that their subjective motivations are unimpeachable'.[36] Those within the intelligence community and their authorising political actors are not necessarily acting according to some private or nefarious agenda. But rather the insular atmosphere has skewed their evaluation. Indeed, intelligence professionals are not bad people, but as Hannah Arendt highlighted, 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.[37]

Framework for Analysis (Boulder: Lynne Rienner, 1998); Christopher Browning and Matt McDonald, 'The Future of Critical Security Studies: Ethics and the Politics of Security' European Journal of International Relations (2011): 1-21; Peter Katzenstein (ed.) The Culture of National Security: Norms and Identity in World Politics (New York: Columbia University Press).

[32] Dennis Thompson, 'Democratic Secrecy' Political Science Quarterly, 114/2 (1999) 181-193, at 182.

[33] Eric A. Posner and Adrian Vermeule, Terror in the Balance: Security, Liberty, and the Courts (Oxford: Oxford University Press, 2007): 5.

[34] 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. Harold Lasswell, 'The Garrison State' The American Journal of Sociology, 46 (1941): 455-468; Harold Lasswell, 'The Garrison-State Hypothesis Today' Changing Patterns of Military Politics edited by Samuel Huntington (New York: Free Press, 1962): 51-70. See Debora Cowen and Emily Gilbert, (Editors). War, Citizenship, Territory (New York and London: Routledge, 2008); Cynthia Enloe Globalization And Militarism: Feminists Make the Link (Lanham: Rowman & Littlefield, 2007); Andrew Bacevich, The New American Militarism: How Americans Are Seduced By War (New York: Oxford University Press, 2005); Robert Kagan, Dangerous Nation: America's Foreign Policy From Its Earliest Days To The Dawn Of The Twentieth Century (New York: Vintage Books, 2006).

[35] Cass Sustein, Laws of Fear: Beyond the Precautionary Principle (Cambridge, Cambridge University Press, 2005).

[36] David Luban, 'The Publicity Principle' in The Theory of Institutional Design edited by Robert E. Goodin (Cambridge: Cambridge University Press): 154-198, at 169.

[37] Hannah Arendt, The Origins of Totalitarianism (London, Harcourt, Brace & World: 1979): 423.

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.[38] In terms of intelligence this can result in tactics far harsher than was originally planned, including escalating interrogation techniques, increasingly intrusive collection methods, or unequal treatment based on race or ethnicity. Democratic theory offers no direct intellectual means of guiding how decision makers should balance the concerns of security over the threat that intelligence generally, or intelligence secrecy specifically, represents; it informs little on what goods and harms should be involved in the moral calculation; and it fails to combat the power of the national security mind-set. Therefore, if we are to better understand when secrets are best kept we need to meet ethical questions of national security on their own grounds; through a theoretical framework that is experienced in balancing and limiting the excesses of national security while still acting to protect the political community.

Finally, the answer to the third question of how we go about monitoring secret keeping is directly shaped by the answers to the previous questions, and has thus proven particularly problematic in terms of intelligence. Indeed, there is what David Estlund calls a misplaced 'modern enthusiasm for democracy' whereby the assumption is that the structures or institutions will 'promote justice or avoid horrors all by themselves, as if guided by an invisible hand'.[39] By taking the answer to the first two questions as a given, liberal democracies utilise their executive, legislative and judiciary as the most appropriate set of structures to evaluate what secrets should be kept and when. Secondary actors are then used but are directly answerable to one of the three government branches, predominantly the executive. For example, in the US this includes the Interagency Security Classification Appeals Panel (ISCAP) that reviews documents for classification; the President's Foreign Intelligence Advisory Board (PFIAB) carries out investigations and initiates activities for the President; agency Inspector Generals who report to the Secretary of the department or the director of the agency it is responsible for; and other advisory commissions and advisory bodies such as the Office of Management and Budget which reviews spending, or the Department of

[38] Spiros Simitis, 'Reviewing Privacy in an Information Age' University of Pennsylvania Law Review 35/3 (1987): 707-746, at 719; Robert Merton, Social Theory and Social Structure (New York: Free Press, 1968): 477; David Harris, 'Racial Profiling Revisited: 'Just Common Sense' in the Fight Against Terror?' Criminal Justice 17 (2002): 36-59; David A. Harris, 'Driving While Black and Other Traffic Offences: The Supreme Court and Pretextual Traffic Stops' The Journal of Criminal Law and Criminology 87 (1999): 544-582; Randall Kennedy, Race Crime and the Law (New York: Patheon, 1997); Annabelle Lever, 'Why Racial Profiling is Hard to Justify: A Response to Risse and Zeckhauser' Philosophy and Public Affairs 33/1 (2005): 94-110; and Matthew Robinson, 'The Construction and Reinforcement of the Myth of Race Crime' Journal of Contemporary Criminal Justice 16 (2000): 133-156

[39] David Estlund, 'The Democracy/Contractualism Analogy' Philosophy and Public Affairs, 31/4, (2003): 387-412, at 387.

Defense's own Intelligence Oversight Program whose object is to ensure operations meet statutory and constitutional rights of US persons.

The nature of intelligence, however, makes these structures fundamentally unsuitable. This is initially because in order to ensure effective intelligence while also having some form of oversight, those selected to keep watch must be allowed into the circle of secrecy in order to have access to the relevant information. Extending this circle of secrecy means there is no one maintaining a watch on these oversight actors; they themselves are not being held to account and their decision-making is protected. The pressure on the elected officials to act accordingly is removed and other pressures – both personal and professional – are allowed to flourish. Offering secrecy to an oversight mechanism that relies on populous support allows them space to react according to personal biases or what would be reported as the popular choice. Indeed, as Kono has argued and demonstrated, electoral systems encourage 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.[40] This protection undermines the very purpose of a democracy by preventing public observation and scrutiny.

Secondly, the use of checks and balances through the separation of powers and a differentiation of their mandate, does not work for intelligence.[41] Intelligence is not positioned in opposition to these actors but is subsumed, if not hidden, within them. Compartmentalisation, unequal power and unequal access to information means that the legislative and judiciary are always at a disadvantage to the executive. Indeed, in terms of critiques of how these structures act and interrelate there is an extensive set of works. Prominent among them is Rahul Sagar's Secrets and Leaks: The Dilemma of State Secrecy, offering a detailed and systematic evaluation of each branch of government. His review includes arguments that 'where the Congress is concerned, its structure and composition… make it prone to undisciplined disclosures'[42] while also 'Given the President's stronghold over the flow of national security information, there is little reason to believe that lawmakers will be able to take the lead in uncovering policies and actions'.[43] Whereas in terms of the judiciary he argues that 'judges are not trained, and the courts not equipped, to make politically

[40] Daniel Kono, 'Optimal Obfuscation: Democracy and Trade Policy Transparency' American Political Science Review, 100/3 (2006): 369–384.
[41] For the intellectual heritage of the importance of the separation of powers see James Madison, The Federalist No. 51: The Structure of the Government Must Furnish the Proper Checks and Balances Between Different Departments 1788 (New York: Dover Publications, INC: 2014); B. Montesquieu, Spirit of Laws 1748 (London: T. Evans: 1777); John Locke, Two Treatises of Government, P. Laslett, ed. (Cambridge, Cambridge University Press: 2004)
[42] Rahul Sagar, Secrets and Leaks: The Dilemma of State Secrecy (Princeton University Press, 2016): 23.
[43] Rahul Sagar, Secrets and Leaks (2016): 128. Emphasis in the original. Also see Philip Fluri and Hans Born, Parliamentary Oversight of the Security Sector: Principles Mechanisms and Practices (DCAF, 2003): 22.

charged decisions about what state secrets are appropriate' coupled with a 'judicial deference towards the executive's claims about the harm likely to be caused by the disclosures'.[44] Kathleen Clark has also written extensively on the executive's refusal to open intelligence oversight to external review and the failure of the legislative to act as a counter force. That despite President Obama's promise of a 'new era of openness', there were 'disappointments' in his willingness to 'hold accountable those involved in several controversial Bush administration intelligence programs'. This includes a critique of the 'gang of eight' system where legislative notification through the eight leading members of Congress – including leaders of both parties from the Senate and House of Representatives, and the chair and ranking members of both the Senate and House Committee for Intelligence – who, during the Bush administration's use of warrantless surveillance, were silenced by executive instructions that no information was to be shared as it exerted its own authority to keep such information secret.[45] William Weaver and Robert Pillitto argue that in the US 'the executive branch over the last several decades have been emboldened to assert secrecy privileged because of judicial timidity and because of Congressional ineffectiveness'.[46] Their conclusion is that 'the privilege is invariably fatal to efforts to gain access to covered documents'; that the structures are insufficient to prevent abuse of the privilege as courts are unable to administer costs for misappropriate use; or because the intelligence services claim that small bits of information are part of a much bigger intelligence secret related to national security and the courts are unable and unwilling to supplant their understanding of national security over that of the intelligence and security infrastructure.[47] Moreover, in courts where the whole proceedings are kept secret – the Foreign Intelligence Surveillance Court being a notable case – secrecy limits opportunity for engaged reflection and debate on the legal interpretation as judicial peer review and the right to appeal is prevented.[48] What this highlights is that these existing political structures lack the physical power to keep the intelligence community in check; are insufficient in manpower,

[44] Rahul Sagar, Secrets and Leaks (2016): 74.
[45] Kathleen Clark, '"A New Era of Openness?" Disclosing Intelligence to Congress Under Obama' Constitutional Commentary 26 (2010): 313-337, at 315. Also see Kathleen Clark, 'Congress's Right to Counsel Intelligence Oversight' University of Illinois Law Review, 2011/3 (2011): 915-960; Kathleen Clark, 'The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program' Brigham Young University Law Review 2010/2 (2010): 357-420.
[46] William Weaver and Robert Pallitto, 'State Secrets and Executive Powers' Political Science Quarterly 120/1 (2005): 85-112, at 86.
[47] William Weaver and Robert Pallitto, 'State Secrets and Executive Powers' (2005): 85-112, at 103-104. For more on the institutional arrangement and executive dominance of the classification system see Nathan Brooks, The Protection of Classified Information: The Legal Framework (Washington, DC: Congressional Research Service, 2004): 2, n. 6; David Morrissey, Disclosure and Secrecy: Security Classification Executive Orders (Columbia: AEJMC, 1997): 35–7. On the relationship between the courts and other parts of government see Norman Dorsen and John H. F. Shattuck, 'Executive Privilege, The Congress and the Courts' Ohio State Law Journal 35/1 (1974): 1-40; Meredith Fuchs, 'Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy' Administrative Law Review 58/1 (2006): 131-176; Robert Deyling, 'Judicial Deference and De Novo Review in Litigation over National Security Information under the Freedom of Information Act' Villanova Law Review 37/1 (1992): 67-112.
[48] For the role of the right to appeal and the importance of multi-layered court systems see Harlon Leigh Dalton, 'Taking the Right to Appeal (More or Less) Seriously' Yale Law Journal 95/1 (1985): 62-107; Thomas Lennerfors, '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 (2007): 381-390; Richard Nobles and David Schiff, 'The Right to Appeal and Workable Systems of Justice' The Modern Law Review 65/5 (2002): 676-701.

intellectual mandate or drive to do so; or cannot separate their own political interests from their role as overseer.

A third problem is that the system is overall too passive. 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.[49] 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.[50] 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.

Finally, these transparency mechanisms have inherent asymmetries of power in the wrong direction. That is, intelligence agencies, or the executive who acts on their behalf, has all the information to make their case while other oversight actors – the legislative or individual for instance – have very little or no information. Individuals making Freedom of Information (FoI) requests, for example, are at a significant disadvantage in regards to knowing when to ask, what to ask and how to appeal a decision. This means the emphasis is the wrong way around. The state has the knowledge and the power, while those making the request have none.

Therefore, it is not surprising that historically and contemporarily intelligence practice has been stalked by both an overreach of the intelligence community and a lack of intervention by the existing oversight apparatus. Watergate was an intelligence scandal that resulted from President Nixon abusing his power to not only attempt to gain advantage over his political rivals but then to cover up his involvement.[51] While the NSA surveillance techniques exposed by Edward Snowden demonstrated the limited review growing intelligence practices were subjected to.[52] Or, as detailed by the Senate in 2015, the use of torture by the

[49] Daniel Baldino, Democratic Oversight of Intelligence Services (Sydney: The Federation Press, 2010): 62.
[50] 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.
[51] Church Committee Final Report Book 1 (1975) Available at http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm [Accessed 4th September 2015]: 344
[52] Dan Roberts, 'Patriot Act author prepares bill to put NSA bulk collection "out of business"' The Guardian, 10 October 2013. Available at http://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill [Accessed 20 September 2015].

CIA had been exacerbated by senior political actors – including National Security Advisor Condoleezza Rice, Secretary of Defence Donald Rumsfeld and Secretary of State Colin Powell – failing to either investigate properly what was going on or to act on what they knew.[53] What these examples show is that the abuse of intelligence powers is not limited to that of just the intelligence community itself, but to political elites that are either the source of the abuse or fail to sufficiently investigate and report on intelligence activity.

The Just War Solution

The current system, therefore, has become beset with some key problems: an ethos of passivity; a structural asymmetry of power; emphasis on the importance of the political community over the individual; and organisational impotence.[54] What is needed is a reimagining of the theoretical foundation, bringing in one that is well versed in dealing with the types of debates had at the security level, balancing the needs of protecting the state against the harms that pursuing those ends can cause. To this end this paper will argue that the just war tradition and its principles of last resort, legitimate authority, just cause, proportionality and discrimination can offer some interesting contributions to the discussion. This framework will aid by providing a better guiding light for those who are to make the decisions by highlighting what factors must be included while also providing new ideas as to what structures can be developed to actualise these criteria.

As a broad body of thought the just war tradition 'remains one of the most popular frameworks for evaluating the morality of war and warfare';[55] influencing and becoming reflected in political rhetoric and legal cannon.[56] At its core is the argument that there are some acts (namely killing) that 'in the normal context are gravely wrong' but cannot be totally 'dismissed by pacifist anathema'[57] as the state must be able to act to safeguard those it is charged with protecting. This does not mean allowing unrestrained action as the just war tradition acts as both a limiting and licensing ethical framework. It seeks to limit when the

[53] Ross W. Bellaby, 'An INS Special Forum: The US Senate Select Committee Report on the CIA's Detention and Interrogation Program' Intelligence and National Security 31/1 (2016): 8-27, at 13.
[54] Robert Chesney, 'State Secrets and the Limits of National Security Litigation' George Washington Law Review, 75/5 (2007): 1249-1332; Kristen Uhl, '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 (2003): 261-311; Christina Wells, 'National Security and the Freedom of Information Act' Administrative Law Review, 56/4 (2004): 1195-1222
[55] Scott Fitzsimmons, 'Just War Theory and Private Security Companies' International Affairs 91/5 (2015): 1069-1084, at 1069. For a summary of the various different historical thematic and contemporary intellectual developments see James Turner Johnson, 'The Just War Idea: The State of the Question' Social Philosophy and Policy 23/1 (2006): 167-195.
[56] For political use see John Kelsay, 'Just War Thinking as Social Practice' Ethics and International Affairs 27/1 (2013): 67-86. For the principle of discrimination see, Article 48, first additional protocol to the Geneva Conventions; for the principle of proportionality see Article 51(4b), first additional protocol to the Geneva Conventions; for the principle of just cause see Article 51 UN Charter.
[57] Michael Quinlan, 'Just Intelligence: Prolegomena to an Ethical Theory' (2007): 1-13, at 1.

harms of war can be deployed, allowing them to protect the political community from harm, but again limiting what sort of actions can be performed in pursuing this objective.[58] From this basis theorists have adapted the just war tradition to tackle emerging ethical-security problems of the day, from acts of terrorism and counterterrorism policy,[59] drone warfare,[60] biosecurity,[61] private military companies,[62] and civil wars.[63] Most related to the questions examined here is the turn towards the applying the just war tradition to intelligence use. Michael Quinlan and Ross Bellaby, for example, each argue that there are important analogies between the conduct of war and the use of intelligence that make the transference of the framework possible.[64] That is, on the one hand intelligence inherently involves violating people's vital interests: 'Effective espionage requires intelligence officers to deceive, incite, and coerce in ways not acceptable for members of the general public';[65] 'intelligence carries an ethical baggage with it or – to be more accurate – a baggage of unworthiness'.[66] But on the other hand the harm caused can be justified when these acts are used for protecting the political community from a variety of threats, though there are still limits needed to ensure the method used is justified given the surrounding circumstances.

But how does this help understand questions of state secrets and what ethical framework it is likely to create. Firstly, on a theoretical level the just war tradition gives an important starting point in the need to understand the fundamental harm caused to the individual – that is, the impact it has on our most fundamental vital interests – and how this relates to the harm that the national security agenda is seeking to prevent. Just as the just war tradition recognises a general presumption against killing to be justified

[58] James Turner Johnson, 'Contemporary Just War Thinking: Which Is Worse, to Have Friends or Critics?' Ethics and International Affairs 27/1 (2013): 25-45, at 25. Not everyone agrees with this general assessment. Valerie Morkevicius, for example, argues that pursuing the justice objectives of the just war tradition makes conflict more likely than realism and its prudential and sceptic designs. Valerie Morkevicius, 'Power and Order: The Shared Logics of Realism and Just War Theory' International Studies Quarterly 59 (2015): 11-22.

[59] Scott Lowe, 'Terrorism and the Just War Theory' Perspective on Evil and Human Wickedness 1/2 (2003): 46-52; Michael Walzer, 'Terrorism and Just War' Philosophia 34 (2006): 3-12; Neta Crawford, 'Just War Theory and the U.S. Counterterror War' Perspectives on Politics 1/1 (2003): 5-25; Naomi Sussman 'Can Just War Theory Delegitimate Terrorism?' European Journal of Political Theory 12/4 (2013): 425-446; Andrew Valls, 'Can Terrorism be Justified?' in Ethics in International Affairs edited by Andrew Valls (Lanham, Maryland: Rowman & Littlefield, 2000): 65-79; Uwe Steinhoff, 'How Can Terrorism be Justified?' in Terrorism: The Philosophical Issues edited by Igor Primoratz (Palgrave-Macmillan, 2004): 97-109.

[60] John Williams, 'Distant Intimacy: Space, Drones and Just War' Ethics and International Affairs 29/1 (2015): 93-110.

[61] Koos van der Bruggen, 'Biosecurity and the Just-War Tradition' in On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects edited by Brian Rappert and Michael J. Selgelid (Australian University Press, 2013): 207-222.

[62] Scott Fitzsimmons 'Just War Theory and Private Security Companies' International Affairs 91/5 (2015): 1069-1084; James Pattison 'Just War Theory and the Privatisation of Military Force' Ethics and International Affairs 22/2 (2008): 143-162.

[63] Tamar Meisels 'Fighting for Independence: What Can Just War Theory Learn from Civil Conflict' Social Theory and Practice 40/2 (2014): 304-326; Anna Floerke Scheid 'Waging a Just Revolution: Just War Criteria in the Context of Oppression' Ethics and Moral Philosophy 32/2 (2012): 153-172

[64] Michael Quinlan, 'Just Intelligence: Prolegomena to an Ethical Theory' (2007): 113, at 2; Ross W. Bellaby, The Ethics of Intelligence: A New Framework (London: Routledge, 2014); Also see Angela Gendron, 'Just War, Just Intelligence: An Ethical Framework for Foreign Espionage' International Journal of Intelligence and Counterintelligence 18/3 (2005): 398-434; Kevin Macnish, 'Just Surveillance? Towards a Normative Theory of Surveillance' Surveillance & Society 12/1 (2014): 142-153; David Omand and Mark Phythian, 'Ethics and Intelligence: A Debate' International Journal of Intelligence and CounterIntelligence 26/1 (2013): 38-63; David Omand, 'The Dilemmas of Using Secret Intelligence for Public Security' in New Protective State: Government, Intelligence and Terrorism edited by Peter Hennessy (London: Continuum, 2007): 142–169, at 157.

[65] Tony Pfaff and Jeffery Tiel, 'The Ethics of Espionage' Journal of Military Ethics 3/1 (2004): 1-15, at 1.

[66] Michael Herman, 'Ethics and Intelligence after September 2001' Intelligence and National Security 19/2 (2004): 342-358, at 342.

within a set of given limits, the impacts of secret keeping on people's autonomy and other vital interests means there is also a general presumption against secrecy unless a direct justification is given.[67] The tradition then breaks down the justification into a set of ethical sub-questions and debates to be had that, in combination, provide an extensive understanding as to whether the act is just or not. These criteria are well versed in dealing with the types of ethical debates that are raised in the security sphere, drawing on both absolutist as well as utilitarian questions and concerns. For example, the principle of just cause asks us to consider the underlying reason given for why the harm is justified, drawing on wider ethical arguments on self-defence, the duty of the state to protect the political community and even the right to punish, explored through hypotheticals and real life and historical cases to understand what reasons are justifiable for different acts.[68] For intelligence secrets the just cause therefore directs us to evaluate what threats we are likely to face if the information is known and the veracity of those threats. The principle of legitimate authority places the political community at the centre, allowing for a move away from democratic structures and their necessary elected element. While the principle of proportionality delineates what costs and benefits should be included in the calculation and ensures that the overall benefit is in the positive. Whereas the principle of discrimination seeks to distinguish the rights and obligations the state has to different groups of people, outlining who gets to know what and when. So not only does the just war tradition direct us to ask certain ethical questions that are relevant in the security world but it also establishes a body of thought to guide the types of debates we should be having, and the variety of answers available to us.

Types of Intelligence Secrets

Depending on the type of intelligence information, the nature of the secret can change. Operational information, for example, refers to the 'on-the-ground' details about how operations are run and can include information on tactics used and the people involved. Recent revelations regarding undercover police operations and infiltration of domestic groups, such as trade unions, have raised questions about

[67] Laurie Calhoun, 'The Metaethical Paradox of Just War Theory' Ethical Theory and Moral Practice 4/1 (2001): 41-58.

[68] Some early revisionists relied heavily on highly artificial cases (e.g., McMahan 1994; Rodin 2002). They were criticized for this by traditionalists, who generally use more empirically-informed examples (Walzer 2000). But one's standpoint on the substantive questions at issue between traditionalists and revisionists need not be predetermined by one's methodology. Revisionists can pay close attention to actual conflicts (e.g., Fabre 2012). Traditionalists can use artificial hypotheticals (e.g., Emerton and Handfield 2009; Lazar 2013). See Jeff McMahan, 'Innocence, Self-Defense and Killing in War' Journal of Political Philosophy, 2/3 (2994): 193–221; David Rodin, War and Self-Defense (Oxford: Clarendon Press, 2002); Michael Walzer, Just and Unjust Wars: A Moral Argument with Historical Illustrations (New York: Basic Books, 2000); Cécile Fabre, Cosmopolitan War (Oxford: Oxford University Press, 2012); Patrick Emerton and Toby Handfield, 'Order and Affray: Defensive Privileges in Warfare' Philosophy & Public Affairs, 37/4 (2009): 382–414; Seth Lazar, 'Associative Duties and the Ethics of Killing in War' Journal of Practical Ethics 1/1 (2013): 3–48.

which organisations should be targeted and the recourse they should have in terms of knowing what was collected about them.[69] One of the main problems at this level of analysis is that people will not know if they are connected to an infiltration operation, even tentatively; whether they are suspected, followed or investigated in some way; or whether their information is being stored on a database somewhere. Moreover, the current system offers no means of resolving this. The passive nature of the system, relying on individuals to inquire, coupled with an over-enthusiastic confidentiality system, means that individuals can be involved in some operation without ever knowing about it.

In comparison, while operational information is the on-the-ground details, strategic information can refer to embedded cultures, structures and policies. For example, the Edward Snowden's disclosures confirmed that between 'Prism', 'XKeyscore' and 'Enterprise Knowledge', the NSA has been collecting and storing some two billion 'record events' per day since 2010, demonstrating that en masse surveillance had grown to become an established practice.[70] So, leaving aside the question of whether Snowden was correct to release the information himself, there is a long-term, wide-ranging practice that needs to be determined about what can be revealed for an engaged evaluation.

Last Resort

The principle of last resort sets where the presumption towards secret keeping should lie. Traditionally the principle of last resort is an attempt to allow means that cause lower levels of harm, like diplomacy or economic pressure, a chance to resolve the threat before the higher harms of war are permitted. However, Robert Phillips warns that, 'it is a mistake to suppose that 'last' necessarily designates the final move in a chronological series of actions'.[71] There is no rigid methodology, beginning with the least harmful and ending in war, but it does require that some of the more harmful actions are not 'jumped' to out of ease, efficiency or expediency. That the emphasis should be to avoid harm if possible, while recognising when the lesser activities are inappropriate or redundant.

[69] Rob Evans and Paul Lewis, 'Trade unionists call for public inquiry to examine claims that police spied on them' The Guardian 30th June 2015. Available at http://www.theguardian.com/uk-news/undercover-with-paul-lewis-and-rob-evans/2015/jun/30/trade-unionists-call-for-public-inquiry-to-examine-claims-that-police-spied-on-them [Accessed on 1 July 2015]. For more on 'covers' – a mainstay during the Cold War – see Christopher Andrew and Vasili Mitrokhin, The Mitrokhin Archive: The KGB in Europe and the West (London: Allen Lane, 1999): 248-50, 532-538; Christopher Andrew, Defence of the Realm: The Authorised History of MI5 (London: Penguin Books, 2010): 179-181, 401; Mark Hollinsworth and Nick Fielding, Defending the Realm: MI5 and the Shayler Affair (London: André Deutsch, 1999): 62.

[70] Michael Kelley, 'NSA: Snowden Stole 1.7 MILLION Classified Documents And Still Has Access To Most Of Them,' Business Insider, 13 December 2013. Available at http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12. [Accessed 14 May 2014]; George Lucas, 'NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden' Ethics and International Affairs, 28/1 (2014): 29-38.

[71] Robert Phillips, War and Justice (Norman: University of Oklahoma Press, 1984): 14

For the issue of secret keeping this seeks to redress the power imbalance and places a strong expectation not to retain information indiscriminately or out of habit, establishing a presumption that information should be released unless there is a direct reason presented as to why it should be retained. This principle therefore gives a reorientation on the emphasis, away from the one of classification unless justified for release, to release unless a direct case can be made for retention. The burden must be placed on intelligence actors to justify why they wish the information to be withheld. Without a direct reason the information should be released. This is important as it contradicts what has been a growing tendency towards blanket classification procedures. For example, investigators in the 1970s found that over 90% of information in some departments were 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.[72] Likewise, in the UK the 20 Year Rule (which was the 30 Year Rule pre-2015) stated that central government departments along with other public bodies are mandated to identify records of historical value by the time they are 20 years of age, illustrating the assumption both that it is left to the departments to decide what is sensitive information and that there is no check on the classification decision until much later on. This represents a blanket system that is unreflective and does not take into account the benefit of revealing the information at the time of publication.

The principle of last resort therefore does some key things. First, it re-orientates the emphasis away from class-based exemptions and a situation where those on the outside must petition for information release, to a system where the intelligence community must argue for information retention. Second, it sets the bar higher than previously considered. This means that arguments for retention based on 'mosaic theory' – where disparate information sets are retained in case they combine to give significance at a later stage – would not be sufficient unless the intelligence community could make a compelling argument for

[72] Christina Wells, 'National Security and the Freedom of Information Act' Administrative Law Review, 56/4 (2004): 1201-1212

how information release would cause direct harm.[73] Finally, this principle works with the later discrimination principle to argue that those who have been involved in an intelligence operation, unknowingly and without result, should be sought out and informed. In practice this would mean that operational and procedural examination by the independent board can be petitioned by the intelligence community as to why the information should be kept secret against an advocate arguing for its release. Short of a compelling reason for why, as outlined by other just war criteria and the necessary level of evidence, the information will be released.

Legitimate Authority

In the just war tradition the principle of legitimate authority argues that in order for a war to be considered morally permissible it must be authorised by the right (or legitimate) authority. This authorising actor must have both the moral weight of representing and protecting the needs of the political community as well as ensuring practical considerations, such as having the physical, intellectual and emotional ability while limiting personal costs or bias: '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'.[74] While traditionally legitimate authority is placed with the state and its representatives as the most appropriate actor to fulfil these needs, this does not necessarily have to be the case. The state will often represent a good choice as it has extensive experience and knowledge and in many instances is a manifestation of the political community. However, as Cecile Fabre argues, the rights and privileges that a state has is justified 'only in so far as they thereby serve individuals' fundamental interests'.[75] At the heart of this is the understanding that the individual and their sovereignty is the fundamental ethical unit, and it is from here that the principle of legitimate authority draws its importance. So, when the state fails in this task or begins to represent the source of the problem then there is a need to rest the legitimate authority elsewhere.

What this means for intelligence and secret keeping is that while established political leaders have been used as the main oversight actor because they represent the state in other areas, we can look beyond these established institutions and create new ones that are more suited to preventing the special type of

[73] For more on 'mosaic theory' see David E. Pozen, 'The Mosaic Theory, National Security, and the Freedom of Information Act' The Yale Law Journal 115 (2005) 628-679

[74] Thomas Aquinas, 'From *Summa Theologiae'*, in International Relations in Political Thought edited by Chris Brown, Terry Nardin, and Nicholas Rengger (Cambridge: Cambridge University Press, 2002): 2013-220, at 214.

[75] Cecile Fabre, 'Cosmopolitanism, Just War Theory and Legitimate Authority' International Affairs 84/5 (2008): 963-976, at 964. Emphasis in original. It is from this position that Fabre argues that other actors – especially in instances of resisting an oppressive regime or fighting colonialism – can possess the ability to be a legitimate authority.

harm that intelligence secret keeping can cause. As previously argued, the current extension of the sphere of secrecy over the existing frameworks has allowed the security mind-set to take primacy with no external viewer to limits its influence. This means the existing system is the source of the problem and so legitimate authority needs to be located elsewhere, in-line with the principles of the just war tradition.

Since the authority should represent the political community it does not have to be limited to only state representatives nor do they necessarily have to be elected or subject to populous demands – as restricting it in this way can be more detrimental to the actual review. Therefore, alternative representative mechanisms can be utilised such as using legal, moral and societal experts, chosen because of their merit rather than because of their elected status, interrogated by the legislative in a public debate to test their suitability. To limit the distortive effect of political interference the body should be able to determine for itself what information should be released and to whom, free from censure. If it detects intelligence activity that contravenes the principles outlined in the other criteria it should be free to determine for themselves what to reveal according to the interests of the community free from worries of political scandal.

In order to ensure the organisation is suitably monitored – so that the watchers are watched – wider political community examination can be assured through regular reports on procedures, decision justifications and rates of classification, including statistics and summaries of its own activities to the public free from editing so they can be reviewed by the public. It must detail what they have investigated, what they chose not to reveal, and when it should be looked at again to see if the reasoning made still stands. This is similar to David Pozen's recommendation for 'second order disclosure requirements' to 'raise the level of generality' in order to make the decision process 'translucent' while not making the secret transparent.[76] Further, the justification given should be examined periodically to determine if the reason still stands, where the time lapsed would depend on the reason given. For example, that the operation is still active is a strong justification for not releasing the information, but would need examining once the operation would have expected to have reasonably been finished. While justifications for maintaining secrecy regarding policies and practices could be set up to be reviewed at set intervals to ensure that the practice has not escalated beyond its original mandate. Sunset clauses for both the review of decisions and for membership will help avoid a stagnant mentality within the decision-making body. They themselves will then be held to account in a similar way to how a Supreme Justice in the US system

[76] David E. Pozen, 'Deep Secrecy' (2010): 257-340, at 327.

is reviewed, with relative ease to initiate an investigation but with increasing difficult to successfully remove them. For example, the bar for legislative impeachment should start relatively low, needing only a simple majority to start an investigation, but should require a two-third majority by both Houses to be successful. This should establish a significantly rigorous bar for their removal in order to protect them from political interference.

The devil, however, is often in the detail of such arguments, and while it is not the aim of this paper to give organisational specifics but to highlight underlying principles, it is possible to foresee a general shape around what a suitable structure might look like. For example, in order to achieve the penetration needed to overcome the passivity problem and carry out the level of review required the oversight actor could consist of a web of observers within each of the different levels of the intelligence community, with sets of individuals physically present at meetings, work-stations and within chain-of-commands who can collect and process the information for a board of governors who then determine what should be released, when and to whom. This web would be a parallel and integrated, but separate in terms of chain-of-command. This is an extension and strengthening of the 'police patrol' model that is argued for, so that the oversight presence is felt throughout and through its surveillance misuse is discouraged.[77] It limits the ability and opportunity to hide poor performance, while offering a point of contact for real-time clarification and authorisation. Indeed, one concern of political oversight is slow or lengthy chain-of-commands that can be delayed by the alternative pressures and needs of the politician carrying out their other duties. Individuals within this web would be unknown to the wider world in order to protect them from counter-intelligence operations. However, they would report directly to a public board of governors who would decide what information should be revealed and when. In order to have a balance of expertise and representation the board's composition can come with guaranteed number of places for legal, moral, intelligence and community leaders.[78] By ensuring these different perspectives we can reproduce 'as best we can, the critical function of pluralism within the deliberative body' that will aid in 'safeguarding against a particularist view'.[79] None should be sitting elected officials who might feel external populous pressures. By giving the board of governors a new mandate to examine intelligence information in terms of the harm

[77] Mathew D. McCubbins and Thomas Schwartz, 'Congressional Oversight Overlooked: Police Patrols versus Fire Alarms' American Journal of Political Science, 28/1 (1984): 165-179, at 166.
[78] For example, information commissioners are in many countries - the UK's Information Commissioner's Office for example – are independent bodies whose leadership is drawn from experts on information rights and procedures and so whose personnel could offer support in terms of data protection and freedom of information.
[79] Simone Chambers 'Behind Closed Doors' (2004): 408.

caused, guided by the other just war criteria, free of the normal political pressures that elected politicians face, and one where its remit is to tackle national security concerns directly, a new culture can be developed.[80] The diversification of membership will offer a suitable cross-representation of concerns held by the political community. In combination, this diversification along with a clearer mandate will further prevent the stagnation and insulation that was experienced by the Foreign Intelligence Surveillance Court as examinations will be subject to a wider realm of peer review with concerns outside the direct legal interpretation being considered and incorporated.[81]

Just Cause

Often considered one of the core propositions of the just war tradition, the principle of just cause requires and evaluates the central justifying reason for why the harm done is ethically necessary. Within the just war literature there is much debate as to what constitutes a just cause, with traditionalists focusing on self-defence as the dominant justification for war, while revisionists such as Jeff McMahan argue for a more flexible interpretation where different kinds of wrongs can justify a comparable state response.[82] What is important for intelligence and its secret keeping is that the ethical end is the protection of the political community and the individuals within it by detecting, locating and preventing threats. This means that the value of both secrecy and transparency is ensuring this end. Given that the presumption is against keeping secrets, in order for the intelligence community to justify information retention it must put forward an argument that secret keeping is an essential part of protecting people and that releasing the information would be harmful to them. In many ways, this supports the national security argument often made, revolving around the need to safeguard against 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'.[83] However, protecting the political community is more than just protecting the state, and includes its ethical, moral, social and legal norms. Indeed, this was

[80] Relying on independent experts is not wholly unheard of as Information Commissioners, for example, have independent review powers but are limited in scope, power and practice. For the UK see the Information Commissioner's Office, https://ico.org.uk ; in Australia the Office of the Australian Information Commissioner https://www.oaic.gov.au ; in Canada Office of the Information Commissioner of Canada http://www.oic-ci.gc.ca/eng/. Accessed 14 December 2015.

[81] The other criteria ask for a balancing of social costs and harms that requires a wider examination beyond the letter of the law to include the spirit of the principles outlined. Also see Scott Sagan, The Limits of Safety: Organizations, Accidents, and Nuclear Weapons (Princeton, Princeton University Press); Charles Perrow, 'Normal Accidents: Living with High Risk Technologies' (Princeton: Princeton University Press, 1999) who both argue that in complex systems – such as a large intelligence community – have a life or set of characteristics, where new problems will arise that there is no contingency for. This means relying on simply legislating the problem away very is impossible, and rather the system need to have a flexibility built-in to deal with new types of threats and activities.

[82] Jeff McMahan, 'Just Cause for War' Ethics and International Affairs 19/3 (2005): 1-21

[83] United Kingdom Security Service Act, 1989, §5.1

the sentiment outlined in the President's Review Group on Intelligence and Communications Technologies, noting 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'.[84] The purpose of the just cause is not necessarily to balance these, but is to highlight what they are and interrogate them.[85] Reconciling these different conceptions of security and determining if there is a suitable threat to keep the information secret can be achieved by answering critical questions that include asking, first, whether releasing the information will cause a direct, foreseeable or immediate harm to come to the political community or individual. The answer to this then rests on some sub-questions regarding how realistic the threat is: who represents the source of the threat; what are the social, historical and cultural contexts to this supposed threat; how realistic is the threat given the current climate, abilities and opportunities; and how immediate is the threat.[86] In contrast, it should also be asked to what extent the activity or information represents a threat to the individual or society's ethical, social or political rights or norms. This can include questions on which rights are being violated; how severe is the violation; and whether the violation is accepted in some way.[87]

In terms of operational information, the just cause is in determining the potential harms for releasing and keeping the information so that they can then be balanced in the proportionality calculation. For example, when infiltrating another closed-off state or group, the use of a cover protects the operative's safety as well as ensuring mission success. If it is clear that revealing the information would put operative lives in danger and there are no other harms foreseen to others by retaining the information then there is a just cause to keep the information secret. Gaining access to a terrorist groups, for instance, is a very 'complex and often dangerous' operation with deadly results for the operative if things go wrong.[88] In this instance, the potentially significant threat of harm to the operative means that there is a strong case for keeping the details secret. In comparison, infiltrating a peaceful organisation such as a trade union would not come with the same threat of violent repercussions. So, while in this instance the operative's identity

[84] President's Review Group on Intelligence and Communications Technologies, (2013): 12, 15.
[85] For McMahan the principle of proportionality is therefore directly connected to the principle of just cause as it enables the balancing of the just cause against the various potential harm to be caused by the act of war. Jeff McMahan, 'Just Cause for War' (2005): 1-21
[86] Michael Walzer, Just and Unjust Wars: A Moral Argument with Historical Illustrations (New York: BasicBooks, 2000): 252
[87] Bellaby, for example, distinguishes between levels of harm and corresponding levels of threat to justify its use, though also includes an absolute limit on the use of torture; Ross W. Bellaby The Ethics of Intelligence: A New Framework (London: Routledge, 2014): 17-18; While Erskine outlines the different types of utilitarian, deontological and realist arguments that can be made when looking for threats and the need to protect the political community. Toni Erskine ''As Rays of Light to the Human Soul?' Moral Agents and Intelligence Gathering' Intelligence and National Security 19/2 (2004): 359-81.
[88] John Sawer, 'Sir John Sawer's Full Speech' The Guardian 28 October 2010. Available at http://www.theguardian.com/uk/2010/oct/28/sir-john-sawers-speech-full-text [Accessed 15 May 2015]

might still be retained to prevent any personal backlash, the operation itself can be revealed to those involved as there is not the same threat of repercussions.

Whereas with strategic information the just cause is understanding the type of threat created when a policy is known and potentially undermined, against the harm that the policy itself can cause, including the wider threat that such methods represent to the security of society and its ethical norms. For example, Andrew Parker, the Director General of the UK Security Service, has argued that the Snowden revelations have resulted in a 'guidebook for terrorists' that represents a 'gift if they need to evade us and strike at will'.[89] Equally, 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.[90] However, the argument that such awareness fundamentally undermines intelligence practices has little evidence. One senior intelligence officer argued that, 'The problem for Al Qaeda is they cannot function without cellphones… You can't run a sophisticated organisation without communications in this world. They know all this, but to operate they have to go on'.[91] While in Klayman v. Obama, Judge Leon, when turning to the efficacy of the surveillance program, questioned whether the program 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'.[92]

In comparison, these en masse data collection methods undermine an individual's privacy when they access personal information without his permission or knowledge. It was revealed that the purpose of the NSA programs is to collect as much information as possible (through surveillance programs referred to as Upstream, Quantuminsert, Tempora) and that by using monitoring techniques such as 'data-mining' and 'dataveillance' it is possible to determine what someone has done, are doing or will do next.[93] By doing this, however, the intelligence services significantly violate the individual's privacy, even if he does not

[89] Tom Whitehead, 'GCHQ Leaks Have 'Gifted' Terrorists Ability to Attack 'At Will', Warns Spy Chief' The Telegraph 9 October 2013. 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]

[90] Eleftheriou-Smith, 'Edward Snowden Revelations have Left UK Vulnerable to Terrorist Attacks' The Independent 1 June 2014. Available at http://www.independent.co.uk/news/uk/home-news/edward-snowden-revelations-have-left-uk-vulnerable-to-terrorist-attacks-9467525.html [Accessed 1 June 2014].

[91] Eric Schmitt and Michael Schmidt, 'Qaeda Plot Leak Has Undermined U.S. Intelligence*' New York Times* 29 September 2013. Available at http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html. [Accessed 7 May 2014].

[92] Klayman, 2013 WL 6598728, at *23

[93] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R. Walker 'After Snowden: Rethinking the Impact of Surveillance' International Political Sociology, 8/2 (2014): 121-144, at 122; Patrick Keefe, Chatter: Dispatches From The Secret World Of Global Eavesdropping (New York: Random House, 2005): 99; Oscar Gandy, 'Data Mining and Surveillance in the Post 9/11 Environment' in The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age edited by Kirstie Bell and Frank Webster (Pluto Press, 2003): 26-41, at 28.

feel the impact directly, as he is unable to decide who has access to what information and how that information is being used.[94] Such databases also often over-represent particular social groups, reinforcing distorted criminal statistics often with individuals unaware that their information is being used.[95] Therefore there is a just cause for revealing the information which can then be balanced against the reason given of mission success in the proportionality calculation.

A different key development in intelligence practices has been the use of torture – either directly or through the extraordinary rendition program – as detailed in the Senate Select Committee on Intelligence's report Committee Study of the Central Intelligence Agency's Detention and Interrogation Program. This report outlined how the CIA had developed an interrogation program, the nature of which had become systematically abusive, as well as acting to limit outside awareness and oversight.[96] The case put forward for retaining the information was made by the CIA and some Republican Senators who argued that the release of the report would provide too many details, leading to compromised relationships with other governments, while in June 2013 the top intelligence official at the State Department, Philip Goldberg, wrote a classified letter to Congress warning against the disclosure of the names of countries who had participated in the program.[97] In this instance the just cause for releasing the report is stronger than in the previous NSA case. Whereas in the NSA surveillance case there could be an argument that knowledge of such methods allows terrorists to circumvent their use, there is no such argument for the use of torture. Aside from the extraordinary levels of harm caused and the affect such practices can have on social cohesion, knowing that the CIA uses torture will not undermine the practice of torture itself. The efficiency of the program is not affected and those kidnapped through extraordinary rendition are still likely to be successfully detained. Furthermore, the use of torture is one of the most extreme forms of abuse and significantly violates both domestic and international ethical, legal and political norms.

Proportionality

[94] Joel Feinberg, Moral Limits of the Criminal Law: Vol.1 Harm to Others (Oxford: Oxford University Press, 1984): 35; Ross W. Bellaby, 'Justifying Cyber-Intelligence?' Journal of Military Ethics 15/4 (2016): 309-314.
[95] Jason Bennetto, 'Police and Racism: What Has Been Achieved 10 Years After the Stephen Lawrence Inquiry Report?*' London: Equality and* Human Rights Commission (2005) Available at http://www.equalityhumanrights.com/sites/default/files/uploads/documents/policeandracism.pdf [Accessed 30 October 2014] p.5
[96] US Senate Select Committee on Intelligence Committee Study of the Central Intelligence Agency's Detention and Interrogation Program (2014). Available at http://fas.org/irp/congress/2014_rpt/ssci-rdi.pdf [Accessed 1 February 2015] p.2
[97] Josh Rogin and Eli Lake, 'Inside the Battle Over the CIA Torture Report' Bloomberg 3 December 2014. Available at https://www.bloomberg.com/view/articles/2014-12-03/inside-the-battle-over-the-cia-torture-report [Accessed 1 February 2015].

The principle of proportionality weighs up the different costs and benefits involved and outlines the course of action most likely to avoid the greatest harm or provide the greatest benefit. This calculation takes into account the strength of the various just causes presented and balances them to see where the greatest harm is being caused, while also incorporating wider harms or damages. In order to make this determination four key questions must be answered to weigh up the forces in play. Firstly, what level of harm is caused if the information is released? For example, how reasonable is it to foresee that those in the field will be put in danger. Second, what are the benefits for keeping the secret? This is slightly different to the previous point in that there can indeed be positives to keeping secrets separate to the damage caused when information is released. For example, an important part of international intelligence cooperation is relying on others to keep your shared intelligence secret. Maintaining this trust and continuing such relationships is a positive to be included in the ethical calculation. Third, what are the harms or damages caused by keeping the information secret? This could include, for example, the number of specific harms caused when the secrecy allows for the violation of an individual's privacy; or broader harms to society and social cohesion when secrecy becomes widespread or systematic. Finally, what are the benefits of releasing the information? For example, can information be released to enable a crowd-sourcing response that might aid the investigation; or used as an important move to ensuring and garnering trust within society. What is important is that the onus of the ethical calculation is towards releasing the information. Therefore, while wider damages can be included when assessing the need to release the information only specific goods directly relating to the just cause can be included when arguing for information retention.[98]

In terms of operational information, the proportionality calculation balances the threat to the intelligence officer's life in the in the field and the directly foreseen benefits of operational success against the danger caused by having the information remain secret. However, in the majority of cases the need to protect the agent will exceed the benefit of revealing details of a particular operation. This will therefore point to exactly what information can be revealed. For example, in the terrorist infiltration case, the potentially high level of harm to the operative and potentially destructive wider backlash or undermining of future operations places a strong limit on any operational information being release. Whereas, infiltration of a peaceful group would mean that there is not the same potential harm if they are made aware

[98] Thomas Hurka 'Proportionality in the Morality of War', Philosophy and Public Affairs, 33/1 (2005): 34-66, at 40.

of a general operation; but to protect the operative from harm their direct participation and even direct means used can be retained.

In a different example the use and disclosure of communication codes is a topic that was prominently raised by Gordon Welchman, British mathematician and Second World War code breaker at Bletchley Park, who passed his final conclusions and corrections to the story of wartime code breaking for publication.[99] In response Sir Peter Marychurch, then Director of GCHQ, chastised Welchman in a letter – published in The Guardian in 1985 in accordance with Welchman's wishes – whereby Marychurch suggests that the information released could cause 'direct damage to security'.[100] Sir Stuart Milner-Barry – another codebreaker from Bletchley Park – responded to Marychurch's criticisms by stating that this is a 'prime example of the lengths to which GCHQ paranoia about the preservation of ancient secrets will carry them' and that to talk of direct damage to security is 'surely absurd'.[101] This does raise an important tension. On the one hand the information revealed is arguably of no direct gain as it refers to technical details of work done. On the other hand, revealing such technical details could undermine code breaking at GCHQ and so there is a need for the information to be kept secret. On balance, therefore, if the question is whether there was a need to reveal such details then the simple answer is no, the information does not have to be released. Such technical information on how cryptography works does not directly impact individuals nor has revealing it provided any great benefit. No one's vital interests are harmed in keeping them secret. There is no overall proportional gain. Nevertheless, there is a clear just cause to keep the information secret in terms of classic national security concerns and the proportional losses in terms of others' understanding the (even out-dated) practices of an intelligence organisations by other security actors.

In terms of proportionality for strategic information, questions on what systematic damages or harms are being caused are important. For example, the growth of a torture culture brings an additional harms in the form of the normalisation of such activities along with wider social harms. Richard Matthews argues that no individual is an island, but is a part of a complex set of social networks that are also damaged when someone is tortured: 'In torturing one person, torturers also harm these networks… Torture never merely attacks a single "terrorist"; its run-on effect is well documented and involves wide-ranging pain and

[99] Gordon Welchman, 'From Polish Bomba to British Bombe: the birth of Ultra' Intelligence and National Security, 1/1 (1986): 71-110.
[100] Peter Marychurch, 'Codebreaker cracks Wartime secrets ban' The Guardian, 15 October 1985.
[101] Stuart Milner-Barry, 'Letters to the Editor: Using a sledgehammer to crack the closed-shop safe' The Guardian, 29 November (1985).

suffering across the communities and contexts from which the torture victim comes'.[102] Additional costs can therefore include, 'loss of international stature and credibility, and the risk of retaliation against soldiers and civilians', significantly affecting the United States' role in world politics, promoting retaliation overseas and hindering foreign policy operations.[103] While it might be argued that releasing the information can heighten social tension and even promote radicalisation, the counter is that if such practices are causing discontent amongst certain social groups, it is only by being made publicly accountable for their actions that the potential radicalisation of individuals can be successfully dealt with.[104] Therefore, given the wide impact of such practices there is a need for a public disclosure of CIA activity.

Discrimination

The basic idea of discrimination is that there is a distinction between two groups of people, legitimate and illegitimate, to which different rights, duties and expectations are bestowed, affecting how the state should treat them. For secret keeping the principle of discrimination sets out that there can be different ways and degrees to inform different groups of people depending on who they are and what they have done. That is, depending on how the information relates or impacts an individual there are different claims as to whether they are to be informed or not. The argument is that information about the individual can be considered their personal property and so they can make claims to control who has access to it. If the secret information is about them or is created by their actions then they have a right to know who is accessing, storing or using it.[105] Also, if the information – the collection, retention or use of – will affect someone detrimentally then they have a right to know in order to make fully rational decisions about how then to act. Similar to the right to know if you are living in the vicinity of a hazardous chemical factory or the potential dangers of medicine before taking it, in order to be fully autonomous individuals must be able to have enough information in order to make a rational choice. This right to know, however, can be qualified by the individual waiving their claim to the information through some (in)activity or circumstance. For example, by becoming a threat individuals can waive some of their protective rights in the process and so can have

[102] Richard Matthews, 'An Empirical Critique of "Interrogational" Torture' Journal of Social Philosophy 43/4 (2012) 457-470, at 466.
[103] Mark Costanzo and Ellen Gerrity, '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 (2009) 179-210, at 179.
[104] Johan Steyn, 'Guantanamo Bay: The Legal Black Hole' The International and Comparative Law Quarterly, 53/1 (2004): 1-15, at 14; Alex Wilner and Claire-Jehanna Dubouloz 'Home-grown Terrorism and Transformative Learning: An Interdisciplinary, Approach to Understanding Radicalisation', Global Change, Peace and Security, 22/1 (2010): 33-51, at 43.
[105] Andrei Marmor, 'What is the Right to Privacy?' Philosophy and Public Affairs, 43/1 (2015): 3-36, at 6.

their information retained. Or, if the repercussions of releasing the information are likely to negatively affect another then the negative effects can be balanced between those involved.

In terms of who should be informed on what operational details the fall of the East German Stasi is an interesting case in point. The Stasi held extensive archives on individuals and with their fall the newly united German authorities made an effort to allow individuals to request access to information if it is related to them. This offered the individual a halfway house as a clear mandate of openness was set down with established processes for requesting and gaining access to the information. However, the effort remained with the individual to request the information, representing the best of a passive machine. FoI requests offer neither the openness mandate nor would individuals be aware that they were involved and so would not think to ask. Resolving these problems, therefore, must start with a form of authority that actively (when the time and situation is right according to the other criteria) locates individuals involved and informs them if any of their information was collected, if they were targeted or involved in some way, and why.

For operational information is that for those individuals who are directly involved, while they might not know about operational details they do have a right to know how they were involved, what information was collected on them and to have that information destroyed if they wish. Given that the emphasis is on the need to reveal unless there is a strong reason not to, the agency must approach the individual rather than waiting for them to make an appeal of some form. For strategic information on policies such as the surveillance program, given that the collection detrimentally effects the whole of society there is a cause for wide disclosure. The indiscriminate nature means large portions of society are affected. Indeed, the subsequent backlash from both the public and political elite demonstrates that there is a disconnect between what was thought to be occurring and the intelligence practiced. Elected representatives in both the United Kingdom and the United States have since complained that they have insufficient information to adequately oversee the work of intelligence agencies, or are barred from publicly objecting to problematic intelligence activities they are aware of.[106]

[106] Nick Hopkins and Matthew Taylor, 'Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne' The Guardian 6 October 2013. Available at http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne#. [Accessed 13th February 2014]

Conclusion

The argument is that democracies are unable to keep suitable control over their intelligence community because an inherent incompatibility of mentality and organisational structure. On the side of the overseers, systems that fundamentally rely on public pressures as both their place from where they draw their core value of sovereign legitimacy as well as a practical means of ensuring correct activity, the extending circle of secrecy has corroded their very purpose and function of these oversight actors. While on the intelligence side, this is a field that comes with it an inherent security pressures that have created a culture that raises itself above the ordinary domestic concerns. Such a privileged position distorts the view of not only those on the inside of the organisation so that their decisions become escalated, but also that of their overseers who have given deference to the executive wing and are reluctant to restrict any area which comes with the perceived fear of limiting national security. Therefore, the proposed new system comes with the benefit of being already well-versed in tackling ethical dilemmas that are faced at the level of national security. By examining the different forms of intelligence information it is clear that there is no single answer for when secrets should be kept or released. Rather, that a more nuanced balanced between the different forces is required, taking into account both the harm and benefit that secrecy can bring. What is difficult is how to ensure and reassure that this balance is maintained when people cannot see it. Therefore there should be a strong assumption that the information be released and that in instances where it is to be retained an explicit case should be presented as for why. This means using the principles outlined to stress the need for a new way to think about how secrets are seen in society and what the short comings of the existing system are. There needs to be a proactive, robust and politically neutral organisation that is not subjected to political whim or influence. The just war tradition offers a set of ethical principles that should guide the development of any oversight structure by providing some key critical questions that must be asked: is the legitimate authority truly able to act without bias and in the best interests of the whole political community, and how should the structure be designed in order to limit the inherent biases and political warfare found within the system; is the emphasis on where the secrecy line must rest in the correct place, erring on the side of revealing information and forcing the intelligence community to work up a steep slope to justify their need for secrecy; what is the underlying argument for the secrecy and does it take a wider view of security of the whole political community over that of a narrow national security understanding; what are the overall harms caused by wide reaching policies and practices; and are those individuals within the

community who are affected given notice of the impact on their lives and the opportunity to inquire about their involvement. Only by replacing the emphasis in this way and establishing more explicit criteria can the trust that has recently been lost begin to be rebuilt.