2009

# Secrecy and Democratic Decisions

Mark A. Chinen

# Articles

## SECRECY AND DEMOCRATIC DECISIONS

*Mark A. Chinen* *

### I. INTRODUCTION

Secrecy to protect intelligence sources and methods arises often in the nation's discourse on several controversial security matters. Protective secrecy itself is controversial because it seems inimical to democracies, where open discussion and accountability serve as touchstones.[1] Citizens, to whom their government is supposed to be accountable, appear to be in a quandary. It seems with national security matters and the secrecy that often cloaks them, people "cannot evaluate some policies and processes because the act of evaluating defeats the policy or undermines the process" in question.[2]

Patrick Keefe suggests we digest concepts like national security "whole, to take them as undifferentiated and unexamined absolutes."[3] The same holds true with secrecy to protect intelligence sources and methods. My purpose here is to unpack the sources and methods argument. There have been a number of explorations of this reason for secrecy, as well as secrecy and democracy more generally,[4] but what I

---

* Associate Professor, Seattle University School of Law. I would like to express my thanks to Charity Anastacio and Jeffrey Leeper for their research assistance for this project, and as always, to Robert Menanteaux, research librarian at the Seattle University School of Law.

1. Dennis F. Thompson, *Democratic Secrecy*, 114 POL. SCI. Q. 181 (1999).

2. *Id.* at 182.

3. PATRICK R. KEEFE, CHATTER: UNCOVERING THE ECHELON SURVEILLANCE NETWORK AND THE SECRET WORLD OF GLOBAL EAVESDROPPING xvi (2006).

4. Among many authors who have examined secrecy and democracy are SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION (1982); PAT M. HOLT, SECRET INTELLIGENCE AND PUBLIC POLICY: A DILEMMA OF DEMOCRACY (1995); LOCH K. JOHNSON, AMERICA'S SECRET POWER: THE CIA IN A DEMOCRATIC SOCIETY (1989); William

hope to contribute to the debate is my belief that the argument for protective secrecy needs to be assessed on at least two levels. In a democracy, it is appropriate to ask about the extent to which democratic values or processes guide the uses of secrecy. I argue in Part II that such principles and processes frame and legitimate questions about secrecy, but in and of themselves they do not always provide definitive guidance about the uses of secrecy to protect sources and methods. It appears a democratic government can accommodate uneasy compromises between openness and secrecy.

The second level of inquiry is more technical and for the most part specific to sources and methods. In Part III, I point out that the protection of sources and methods can be a compelling reason for secrecy, but not always.[5] Given general knowledge about certain intelligence sources and methods, and, to a lesser extent, differences in their vulnerability to countermeasures, the need for secrecy is not uniform. Further, the protection of sources and methods is only as important as the intelligence derived from them, which in turn is only as important as the role intelligence plays in policymaking. The value and influence of either can be modest. Additionally, the secrecy argument is akin to the precautionary principle, which in some contexts provides little help in decision-making. Finally, as is usually true when information asymmetries exist, secrecy creates inefficiencies and perverse incentives in the collection, processing, and dissemination of intelligence, which in the end allows the government to shift the costs of inaccurate information to citizens and yet remain unaccountable for those costs.

In Part IV, I juxtapose the conclusions drawn from these two levels of inquiry and ask what can be learned from the fact that at best democratic principles and processes offer rough guidance on how to use secrecy, but that the secrecy argument itself is often unconvincing. As an initial matter, it means the relationship between democracy and protective secrecy is not one of abstract ideals against the concrete

---

E. Colby, *Intelligence Secrecy and Security in a Free Society*, 1 INT'L SECURITY 3 (1976); Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247 (2005); Thompson, *supra* note 1; *see also* COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, SECRECY, S. DOC. NO. 105-2 (1997), *available at* http://www.gpo.gov/congress/commissions/secrecy/index.html.

5. As I note in Part III, there are other reasons for protecting classified information from disclosure, which are beyond the scope of this paper.

realities of national security. It also means it is proper to ask tough questions of proponents of secrecy—particularly when decisions of national moment are being considered, like going to war, or when individual civil liberties are at stake and one is determining whether the government is obeying laws designed to protect those liberties—and to heavily discount the secrecy argument when such questions are not satisfactorily answered. Lastly, it provides ways to assess how well elected representatives and others charged with oversight respond to those who hold and wield secrets.

## II. DEMOCRATIC PRINCIPLES AND PROCESSES AND SECRECY

### *A. Democracy and the Dangers of Secrecy*

Amartya Sen argues that the most important development of the past 100 years has been the emergence of democracy "as the preeminently acceptable form of governance."[6] Similarly, in his remarks on the rule of law, J.H.H. Weiler states it is now generally accepted that obedience to law can "neither be claimed, nor justified, if the laws in question did not emanate from a legal system embedded in some form of democracy."[7] Given this strong legitimating power, it is natural to ask whether democracy, either as an idea or in its incarnations, can help society make difficult choices, including how to use secrecy. Indeed, democracy and secrecy seem to be linked: the question of legitimacy boils down to whether citizens have a moral obligation to obey or to respect the laws and decisions of their government.[8] Secrecy is useful to a society,[9] but it also seems to threaten that very

6. Amartya Sen, *Democracy as a Universal Value*, J. DEMOCRACY, July 1999, at 3, 4.

7. J.H.H. Weiler, *The Geology of International Law—Governance, Democracy and Legitimacy*, 64 HEIDELBERG J. INT'L L. 547 (2004). *But see* Joshua Cohen, *Is there a Human Right to Democracy?, in* THE EGALITARIAN CONSCIENCE: ESSAYS IN HONOR OF G. A. COHEN 226, 226 (Christine Sypnowich ed., 2006) (arguing that non-democratic governments can claim legitimacy as long as they are responsive to the interests of their citizenry).

8. *See* Mattias Kumm, *The Legitimacy of International Law: A Constitutionalist Framework of Analysis* 15 EUR. J. INT'L L. 907, 908 (2004) (pointing out that "[t]he very idea of legitimacy develops clearer contours when connected to questions of obedience.").

9. Sissela Bok identifies three reasons why secrecy is useful to a society: deliberation, surprise, and confidentiality. BOK, *supra* note 4, at 175-76. By deliberation, Bok refers to the ability of government agencies (or any group) to consider a course of action before it is made public, out of a concern that pre-mature transparency will stifle the deliberative process. *Id.* at 175. Further, secrecy is sometimes needed to preserve the element of surprise in government actions. *Id.* at 176. Offshoots of these justifications include the need for secrecy in diplomatic relations, the development or abandonment of plans, and missions in wartime, *see,*

legitimacy.[10] Does it matter therefore how secrecy is used in a democracy? Is it meaningful to speak of democratic and undemocratic uses of secrecy, such that we know when to allow secrecy and when to forbid it?

Of course, these are hard questions. Democracy itself is an under-specified term[11] such that there is the danger of setting up a straw man. Since one must begin somewhere, however, consider John Dunn's argument that "the structure of modern representative democracy . . . provides . . . a practical basis through which to *refuse* to be ruled unaccountably and indefinitely against your will."[12] He adds, "Less steadily and on far less egalitarian terms, it also provides a framework through which to explore what people should and should not attempt to do as a community."[13]

Much is packed into these two sentences. For Dunn, citizens must have some say in who governs, no matter how attenuated this ability might be, due to the delegation of power in large, modern democracies. Concomitant with say in governance are accountability and limitations on power. There is also Dunn's sense that democracy provides a space for communal decisions, although for Dunn not everyone has an equal voice in that space. Given this spare and highly qualified description of the term, it is not surprising Dunn doubts democracy's ability to help decide "what people should and should not attempt to do as a community." In his view, "Virtually none of the elements of an answer to that question can come from democracy as an idea."[14] This is not a propitious starting point, but it is worth asking in what sense Dunn could be right.

The idea of having a say in who governs is accompanied by a web of interrelated concepts: equality, autonomy, meaningful consent, freedom from coercion, accountability, the protection of civil liberties,

---

*e.g.*, COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, *supra* note 4, at 6-7, and the need to protect the privacy of innocent citizens. BOK, *supra* note 4, at 176; *see also* AMY GUTMANN & DENNIS THOMPSON, WHY DELIBERATIVE DEMOCRACY? 4 (2004) (discussing justifications for secrecy in government).

10. Allen Dulles writes: "Free peoples everywhere abhor government secrecy. There is something sinister and dangerous, they feel, when governments 'shroud' their activities. It may be an entering wedge for the establishment of an autocratic form of rule, a cover-up for their mistakes." ALLEN DULLES, THE CRAFT OF INTELLIGENCE 237 (1963).

11. Weiler, *supra* note 7, at 547.

12. John Dunn, *Getting democracy into focus*, OPEN DEMOCRACY, Oct. 20, 2005, http://www.opendemocracy.net/democracy-opening/focus_2944.jsp (emphasis in original).

13. *Id.*

14. *Id.*

as well as institutional features deemed necessary to enable self-government, such as free and fair elections, universal suffrage, etc. Two such ideas I focus on here stem from a general sense that persons are not bound to collective decisions unless they have in some meaningful way consented to be so bound.[15] This in turn leads to concepts familiar in any system of agreement: agreements must be free from coercion or the inappropriate withholding of relevant information, or there is no real assent.

Both concepts appear in a number of accounts of democracy. Take, for example, coercion. For Dunn, democracy as an idea "requires the systematic elimination of power (the capacity to make others act against their own firm inclinations) from human relations."[16] Frank Michelman's "jurisgenerational" politics entail "a set of prescriptive social and procedural conditions such that one's undergoing, under those conditions, such a dialogic modulation of one's understandings is not considered or experienced as coercive, or invasive, or otherwise a violation of one's identity or freedom."[17]

Of course, these and other scholars accept that some level of coercion is inevitable because, as Robert Dahl argues, the complete absence of coercion leads to anarchy.[18] Coupling the idea of democracy with representative government enables persons to enjoy, on the one hand, the economies of scale possible in large populations and territories (including those that go to security) and on the other, institutions that approximate democratic forms of government.[19] In modern democracies, persons have delegated decision-making power to their elected leaders. But the agency problems that arise with representatives, and the tenuous link between most citizens and their elected leaders—because of the size of the nation-state—make it equally sensible to argue that the average citizen has very limited ability to participate in, and

15. Either at a specific point in history, such as the ratification of a constitution, or as a necessary part of a theory of democracy.

16. JOHN DUNN, DEMOCRACY: A HISTORY 169 (2005). Dunn thinks it is impossible to order a society based on this idea.

17. Frank I. Michelman, *Law's Republic*, 97 YALE L. J. 1493, 1526-27 (1988).

18. ROBERT A. DAHL, DEMOCRACY AND ITS CRITICS 37-51 (1989).

19. *Id.* at 28-30, 213-16. It is this delegation of authority that leads to institutions such as elected officials, free and fair elections, inclusive suffrage, the right to run for office, freedom of expression, access to alternative information, and associational autonomy. *Id.* at 221.

thereby meaningfully consent to, important decisions that impact her life.[20]

It is precisely where the degree of delegation is high that the connection between coercion and access to relevant information becomes most salient. As Amy Gutmann and Denis Thompson put it, consensus requires people to give accessible reasons for decisions because "[t]o justify imposing their will on you, your fellow citizens must give reasons that are comprehensible to you."[21] Although some coercion may be inevitable in large democracies, the point where delegation of authority limns into authoritarianism is where there cease to be comprehensible reasons for exercises of authority. Such reasons include descriptions of states of the world that require exercises of governmental power to respond to them. Secrecy can, of course, be used to conceal overt forms of government coercion, but more subtle and widespread coercion can arise when meaningful discussion of public decisions requires an accurate assessment of a given situation, and secrecy is used to distort that assessment.

It is not surprising then that Gutmann and Thompson begin their most recent account of deliberative democracy by discussing the lead-up to the Second Iraq War. This presents the hard case. "The decision to go to war, it would seem, is unfriendly territory for pursuing the kind of reasoned argument that characterizes political deliberation."[22] Gutmann and Thompson note that when the Bush Administration announced it would take military action against Saddam Hussein, it understood the need to justify its actions to the American people and to the world, and so in the months before the invasion, the Administration found itself in a heated debate with Congress, and later, the United Nations. The government argued that war was justified because it believed, based in part on classified information, that Saddam Hussein posed a threat to the United States and to international peace and security: first, because his

---

20. With important exceptions discussed in Part IV, this might particularly be the case with foreign affairs and national security. *See, e.g.*, Robert A. Dahl, *Can international organizations be democratic? A skeptic's view*, *in* DEMOCRACY'S EDGES 19 (Ian Shapiro & Casiano Hacker-Cordon eds., 1999) (discussing a general lack of public involvement in foreign affairs issues).

21. GUTMANN & THOMPSON, *supra* note 9, at 4. John Dryzek, who also writes from a deliberative perspective, argues for democratic authenticity, measured by the degree to which social control takes place through communication that encourages reflection on one's preferences without coercion. JOHN S. DRYZEK, DELIBERATIVE DEMOCRACY AND BEYOND: LIBERALS, CRITICS, CONTESTATIONS 8 (2000).

22. GUTMANN & THOMPSON, *supra* note 9, at 1.

regime was developing weapons of mass destruction, and second, because it was associated with terrorists who had attacked the United States. There was vigorous debate about those claims, and about the methods for responding to the purported threat, but such debate was "cut short" by the invasion in 2003.[23] Subsequent events have proved neither of the two claims was true.[24]

Accurate assessments of information go to both what one might term democracy's substantive aspects, such as freedom from coercion, and its procedural aspects; here it is difficult to separate idea from institution. Again, what makes the process of opinion formation and the selection of policies both at the grass-roots level and in the legislature so crucial, particularly in highly plural societies, is its link to legitimacy: government decisions must be based on plausible reasons, and the process of deciding is circumvented when the reasons any branch of government gives for its actions cannot be verified or are not based in fact. Jürgen Habermas notes: "Democratic procedure, which establishes a network of pragmatic considerations, compromises, and discourses of self-understanding and of justice, grounds the presumption that reasonable or fair results are obtained insofar as the flow of relevant information and its proper handling have not been obstructed."[25]

What happens, then, when information flows are obstructed or mishandled? Gutmann and Thompson argue, "When a primary reason offered by the government for going to war turns out to be false, or worse still, deceptive, then not only is the government's justification for war called into question, so also is its respect for citizens."[26] At the extreme, using secrecy to withhold information that undercut reasons for choosing a particular policy also undermines the legitimate expectations of persons governed, which in turn undermines the legitimacy of those who govern them.[27]

---

23. *Id.* at 2.

24. *See infra* text accompanying notes 169-73.

25. JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS 296 (William Rehg trans. 1996). Elsewhere Habermas writes: "Deliberative politics acquires its legitimating force from the discursive structure of opinion-and will-formation that can fulfill its socially integrative function only because citizens expect its results to have a reasonable *quality*." *Id.* at 304 (emphasis in original).

26. GUTMANN & THOMPSON, *supra* note 9, at 4.

27. Writing from a non-deliberative framework, Dunn states: "Governmental seclusion is the most direct and also the deepest subversion of the democratic claim . . . . The more governments control what their fellow citizens can know the less they can claim the authority of those citizens for how they rule." DUNN, *supra* note 16, at 185; *see also* John Dunn,

Deliberative democracy theorists have described well the adverse effects caused by the manipulation of information as a democracy determines policy. Habermas argues elite monopolization of relevant information distorts the communicative process, thereby preventing further democratization.[28] Such monopolization involves far more than withholding information,[29] yet it is easy to see how secrecy can have a distorting effect. As the public forms its positions, the government is but one of several competitors for public attention and approval, and given the malleability of public opinion formation, it can be argued that the withholding of relevant information will have little effect on that process—people will keep their opinions irrespective of facts. However, except in some circumstances discussed below, it would seem unlikely that participants in such a discourse would accept governmental failures to disclose information that could impact opinion formation. On the legislative level, decision-makers for the most part select and justify policies that have already been "discovered" through interactions in the public sphere.[30] At the same time, legislators rely on preparatory work provided by the administration in this process of selection and justification.[31] Again, these processes can be impacted by information flows controlled in part by secrecy.

### *B. The Counterarguments*

#### *1. Secrecy and Democratic Ideals*

It is thus possible to argue that secrecy can be inimical to democracy both as a means of achieving meaningful consent and as a process through which a polity makes community decisions. Nevertheless, although secrecy can pose a danger to democracy, it is difficult to determine exactly when the danger is so great that secrecy must be prohibited. First, as others have pointed out, on the substantive

---

*Situating Democratic Political Accountability, in* DEMOCRACY, ACCOUNTABILITY AND REPRESENTATION 329 (Adam Przeworski et. al. eds., 1999).

28. HABERMAS, *supra* note 25, at 318. Habermas, who relies on the work of Dahl on this point, argues: "Privileged access to the sources of relevant knowledge makes possible an inconspicuous domination over the colonized public of citizens cut off from these sources and placated with symbolic politics." *Id.* at 317.

29. It also includes the setting of the public agenda and the uses of information to assist an administration in steering the nation in particular directions.

30. HABERMAS, *supra* note 25, at 307.

31. *Id.*

level, secrecy can be used to combat coercion. Oppressed groups often need secrecy to strengthen group cohesion and to allow for mobilization for action.[32] The very act of forming democratic constitutions has required secrecy.[33] More relevant to intelligence issues, if meaningful consent depends on a government providing its citizenry with accurate assessments of states of the world, what happens if the flow of information needed for such accuracy dries up because the sources and methods enabling that flow are disclosed and thereby evaded?

This means it is not always possible to apply a rule that would prohibit as undemocratic secrecy that disables meaningful consent and to permit secrecy that does not. Sometimes decision-makers need information to assess an evolving national security problem, but as just discussed, they face the dilemma that disclosure of such information will stop future flows of information needed to assess and respond to subsequent evolutions of the same problem. This, of course, was what confronted those who broke the Japanese diplomatic codes prior to the attack on Pearl Harbor.[34] One could argue that it is more advantageous from a democratic perspective to have a better-informed and therefore more meaningful decision in the present, and risk losing information

32. Cass Sunstein points out that several social movements, such as the civil rights and women's movements, were made possible by enclaves of marginalized persons who were then able to form positions and strategies within those particular groups. CASS R. SUNSTEIN, DESIGNING DEMOCRACY: WHAT CONSTITUTIONS DO 45-46 (2001).

33. Jon Elster, *Deliberation and Constitution Making*, *in* DELIBERATIVE DEMOCRACY 97, 109-11 (Jon Elster ed., 1998) (discussing the advantages and disadvantages of publicity in constitutional conventions).

34. By the eve of the United States' entry into the Second World War, U.S. cryptanalysts had broken Japanese diplomatic codes. This, and the subsequent decryption of Japanese naval codes, was an intelligence coup crucial to the war effort. HERVIE HAUFLER, CODEBREAKER'S VICTORY: HOW THE ALLIED CRYPTOGRAPHERS WON WORLD WAR II 3-4 (2003). Important decisions were taken on the strength of intelligence derived from the decoded intercepts, and of course, the source of that intelligence was highly classified. The Japanese diplomatic code had been broken in 1940, before the attack on Pearl Harbor, CHRISTOPHER ANDREW, FOR THE PRESIDENT'S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 105 (1995), and there were strong indications from the intercepts that the Japanese leadership was contemplating war with the United States. *Id.* at 110, 113-14; *see also* HENRY C. CLAUSEN & BRUCE LEE, PEARL HARBOR: FINAL JUDGMENT 42 (1992). Many factors contributed to the United States' inability to anticipate and prevent the attack, but one, some argue, was the failure to disseminate all relevant intercepts with those directly responsible for Pearl Harbor's defense, in part to protect Magic. That claim is controversial. *Compare* CLAUSEN & LEE, *supra,* at 300-01 (arguing that the U.S. military commanders should have been amply warned by what communications were provided to them) *with* GORDON W. PRANGE WITH DONALD M. GOLDSTEIN & KATHERINE V. DILLON, PEARL HARBOR: THE VERDICT OF HISTORY 278 (1986) (arguing that not all important intercepts were shared).

flows in the future. But a democracy could decide to accept the possibility of incompletely-considered decisions now in hopes of a better, and thus in some sense, freer and more meaningful decision, later. But of course, there is then a risk that these deferrals in disclosure will go on ad infinitum.[35]

The difficulties in assessing when concealment is coercive raises a second problem with equating the presence or absence of meaningful consent with democratic and undemocratic uses of secrecy. So far, I have evaluated secrecy through the lens of freedom from coercion; but such freedom is just one of several principles—including equality, accountability, and participation in decision-making—any of which could be selected as a yardstick for evaluating uses of secrecy. One could, for example, examine secrecy from the perspective of participation and ask whether secrecy is being used to hinder or facilitate such participation. However, my suspicion is that whether one singles out one of these principles or views them as a whole, there are many times when these concepts are too abstract—especially when melded to the structures of modern democracy—to help determine how secrecy is to be used.

*2. Secrecy and Democratic Processes*

As I discussed earlier, on the decision-making level, one can frame arguments that secrecy is harmful to the process whereby a polity makes community decisions. But deliberative democracy allows for other kinds of decision-making, including those involving secrets, as long as those other ways of deciding are justified in a deliberative process. This point is made by Thompson, who argues that the problem of secrecy and democracy is not that the two conflict, but rather, that democracies are faced with a dilemma.[36] As discussed in the Introduction, Thompson argues that democracy requires publicity to hold leaders accountable for their policy decisions, yet "some policies and processes, if they were made public, could not be carried out as effectively or at all."[37]

Faced with this dilemma, at the extremes a democracy can either abandon the policy at issue or abandon accountability. Or, a democracy can have both by "lifting the veil of secrecy just enough to allow for

35. I return to this problem in Part III, and in Part IV.
36. Thompson, *supra* note 1, at 182.
37. *Id.*

some degree of democratic accountability."[38] Thompson suggests two ways to do so. The first is to lift the veil at some point to allow public evaluation after the fact, to grant temporal secrecy.[39] But because temporal secrecy is a form of secrecy, it runs the danger of reducing accountability and consent. Thompson therefore suggests democracies engage in a form of "second-order" publicity to determine whether temporal secrecy should be granted. "[A] secret is justified only if it promotes the democratic discussion of the merits of a public policy; and if citizens and their accountable representatives are able to deliberate about whether it does so."[40] However, according to Thompson, second-order publicity has its limitations. It does not reach cases where accountability is "context sensitive."[41] "These are cases in which the controversial element of the policy is specific to the case, cannot be revealed without undermining the policy, and has irreversible effects."[42] It also does not handle cases when second-order publicity about a policy would undermine its first-order efficacy, when even a general discussion of a policy would undermine its effectiveness.[43]

The limitations of second-order publicity in certain situations motivate a second way to deal with the secrecy dilemma: one can allow "partial secrets." Thomson discusses three kinds. The first is what he calls "acoustic separation." Here, Thompson uses as an example the old maxim that ignorance of the law is no excuse. He argues the maxim in practice is untrue because there are several valid "defenses" based on such ignorance; however, it is socially useful to maintain the maxim and thus distance it from that "truth" about knowledge of the law.[44] A second form of partial secrecy is illustrated by the "don't ask, don't tell" policy regarding gays in the military—a form of compelled silence.[45] The third deals with political hypocrisy: sometimes it is useful not to reveal potentially damaging personal information about elected leaders because it has nothing to do with the merits of policies such leaders might be advocating.[46]

---

38. *Id.* at 183.
39. *Id.* at 184.
40. Thompson, *supra* note 1, at 185.
41. *Id.*
42. *Id.*
43. *Id.* at 186.
44. Thompson, *supra* note 1, at 186.
45. *Id.*at 188-90.
46. *Id.* at 190-92.

At best, however, partial secrets go only so far to resolve the dilemma posed by the desire for both accountability and policies that require secrecy; some policies will never be completely disclosed. Thompson suggests: "The only feasible solutions seem to be either to rely on representatives who can be trusted to review in private the policy and its application, or to conduct public debates in general terms without revealing the specific nature of the policy."[47] Thompson thus concedes second-order publicity and partial secrets are incomplete solutions to the dilemma. "That neither of these alternatives usually provides adequate democratic accountability is a further reason to seek ways to promote transparency in the design of the government institutions and the making of public policies."[48]

The approaches proposed by Thompson are often taken in the national security context, but with varying degrees of success. Information is declassified over time, but this can happen decades after it could be used to hold decision-makers accountable, let alone to help decide a prospective policy. Accountability is also supposed to be secured through a small number of Congressional committees charged with oversight of the intelligence community, a kind of partial secrecy. As is well known, however, such oversight is not without its problems.[49] Finally, broad public debate about national security policy in general terms can take place without revealing secrets. However, such discussion can be broad indeed and easily manipulated, thereby providing little guidance or legitimizing force. This simply confirms Thompson's point that temporary and partial secrecy are incomplete solutions to the problems of accountability and consent raised when a society wants to preserve democratic values at the same time it wants effective policies. The possible conflict between secrecy and democracy viewed as a set of principles is replaced by a deliberative dilemma—difficult, if not impossible, to resolve.

### *C. The Lessons of Democracy for Secrecy*

As discussed in Part II A, Dunn argues that democracy provides first, a practical means for refusing to be ruled by unaccountable persons for indefinite periods of time and against our will, and second, a

47. *Id.* at 193.
48. Thompson, *supra* note 1, at 193.
49. *See infra* text accompanying notes 168-221.

framework for considering questions of how we are to order ourselves as a society. The foregoing discussion confirms that view in part, at least when we ask whether democracy as an idea or as a framework for decision-making guides our uses of secrecy. The ideas or values commonly associated with democratic societies, whether realized or not, and certain presumptions about what is required in democratic deliberation do have the effect of drawing our attention to situations where secrecy claims become enmeshed with those values or activities and conflicts with them.

I argue later in Part IV that heightened attention, particularly in light of some of the technical aspects of secrecy to support sources and methods I am about to discuss, might be enough to provide some clarity on how secrecy is used in some situations. However, such ideas, values, and principles are not sufficient in themselves to inform when the protection of sources and methods should give way to them. On the level of ideas, values, or commonly held assumptions about the individual, sometimes secrecy can simultaneously support and frustrate those values. On the level of deliberation, secrecy can either impede or facilitate reason-giving, and there is always the reality that citizens legitimately want both accountability and effective policies and are willing at times to compromise one in favor of the other. This leads to second-best measures that only serve to highlight, not resolve, the dilemma posed by those two sometimes conflicting desires.[50]

---

50. Space does not permit a comparative study of secrecy in other democracies. However, the United Kingdom's Official Secrets Act is well known. Official Secrets Act of 1989, 1989 c. 6. That act provides for criminal penalties for unauthorized disclosures of official information of various kinds and has been used to prosecute persons who have allegedly provided sensitive information to the press. *See, e.g.*, *Civil servant cleared as secrets case dropped*, TIMES ONLINE, Jan. 9, 2008, http://business.timesonline.co.uk/tol/business/law/article3159398.ece (describing a case brought against a British Foreign Office civil servant for alleged breaches of the Official Secrets Act by providing information to the media). For a history of the Act, see John Griffith, *The Official Secrets Act 1989*, 16 J. L. & SOC'Y 273 (1989). The Act has had its own troubled history and has been criticized as being in conflict with the freedom of expression and preventing government accountability. *See* HUMAN RIGHTS WATCH, ABDICATION OF RESPONSIBILITY: THE COMMONWEALTH AND HUMAN RIGHTS 56-57 (1991), *available at* http://www.hrw.org/reports/pdfs/g/general/general291o.pdf; LAURENCE LUSTGARTEN & IAN LEIGH, IN FROM THE COLD: NATIONAL SECURITY AND PARLIAMENTARY DEMOCRACY 245 (1994). The Act, however, as well as other differences between U.S. and U.K. national security policy and organization, indicates it is possible for democracies to have differing approaches to the treatment of national security secrets. For a brief comparison of U.S. and U.K. approaches to domestic security, see TODD MASSE, DOMESTIC INTELLIGENCE IN THE

## III. SECRECY TO PROTECT INTELLIGENCE SOURCES AND METHODS

### *A. The Need for Secrecy*

At this point, it would seem that secrecy wins out in a contest with democracy because of the amorphous character of the latter and its power to guide. However, secrecy to protect sources and methods must also be considered on its own merits.

Michael Herman discusses three reasons for secrecy in intelligence activities. In wartime, secrecy hides from an adversary the fact that its plans have been detected and are being countered. Here, that such plans are known is crucial, not how they are known.[51] A second reason given by Herman[52] is what Richard Posner terms the "embarrassment factor." National security sometimes involves what at best can be termed questionable practices; [53] there is the risk that intelligence gathering, if disclosed, will jeopardize foreign relations. Thus emerges plausible deniability. According to this theory, certain persons, including elected leaders, should not know about certain intelligence activities because they must be able to deny credibly knowledge of such activities.

The protection of sources and methods of intelligence collection and analysis is the third and most important reason for secrecy.[54] Such sources and methods must be kept secret because they are vulnerable to countermeasures.[55] Intelligence agents can be arrested and executed,[56]

---

U.K.: APPLICABILITY OF THE MI-5 MODEL TO THE U.S., CRS Report RL31920, at 6-11 (2003), *available at* http://www.fas.org/irp/crs/RL31920.pdf.

51. MICHAEL HERMAN, INTELLIGENCE POWER IN PEACE AND WAR 88 (1996).

52. *Id.* at 88-89.

53. RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 187 (2006).

54. HERMAN, *supra* note 51, at 89 (stating that the main reason for secrecy is to protect intelligence sources); ROBERT M. CLARK, INTELLIGENCE ANALYSIS: A TARGET-CENTRIC APPROACH 96-97 (2004) (arguing that secrecy is important to protect sources and methods); HOLT, *supra* note 4, at 73 ("The sources of intelligence and the methods used to acquire it are possibly the most sensitive secrets of the intelligence community . . . ."); MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 73 (3d ed. 2006) ("The details of collection capabilities—and even the existence of some capabilities—are among the most highly classified secrets of any state.").

55. HERMAN, *supra* note 51, at 89-90; *see also* CLARK, *supra* note 54, at 97 ("[A]lmost every intelligence service has lost collection assets because an intelligence customer gave the press information or acted in such a way that the collection source was 'blown.'").

56. JOHNSON, *supra* note 4, at 70-71 (describing instances where failure to protect sources resulted in the deaths of secret agents).

codes can be changed,[57] or persons can avoid using cell phones or e-mail, or stay out of sight of reconnaissance satellites. Alternatively, sources can be manipulated by an adversary to spread false information; spies can be persuaded to become double agents, or false messages can be given in encrypted transmissions.

At the outset, two points should be made about the need to protect sources and methods through secrecy. As Herman notes, the main concern is to ensure the availability and quality of future flows of information, as opposed to current information.[58] Problems arise when the disclosure of current information threatens the flow of future information because disclosure now could reveal its source. Further, the need for such protection gives rise to a penumbra of principles, practices, and institutions to preserve secrets: since the possibility of disclosure increases with the number of persons privy to information,[59] such information is limited to those who need to know. The protection of sources and methods also requires a complex bureaucracy to decide what information should be secret and who should have access to it.[60]

### *B. The Protection of Sources and Methods in Context*

#### *1. Knowledge and Vulnerability of Sources and Methods*

All things equal, the argument for protecting sources and methods of intelligence is persuasive. We tend to believe that more, not less, information is necessary to make good judgments. Other countries and entities do not always publicize their plans and intentions, thus we need to gather and develop intelligence on our own. Furthermore, the sources and methods for producing useful intelligence often involve human lives and are expensive.

There are times, however, when the strength of the secrecy argument wanes. Secrecy, for example, is not useful if the intelligence

57. This was the primary reason for keeping the sources of intelligence on Japanese foreign and military policy secret. Stephen Budiansky, *Closing the Book on Pearl Harbor*, 24 CRYPTOLOGIA 119 (2000).

58. HERMAN, *supra* note 51, at 90.

59. Memorandum from Alfred Cumming, Specialist in Intelligence and Nat'l Security Foreign Affairs, Def. and Trade Div., Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions 9 (Jan. 18, 2006), *available at* http://epic.org/privacy/terrorism/fisa/crs11806.pdf.

60. For a brief discussion of the legal framework for the system of classification and access to confidential information, see LOWENTHAL, *supra* note 54, at 62-67.

sources and methods at issue are already known, and here it bears emphasizing that a significant amount of information about them is readily available. Groupings vary, but in general, three disciplines are used in the collection and development of information:[61] signals intelligence,[62] imagery intelligence, and human intelligence.[63] Each of these fields involves various kinds of technology and other resources—the details of which are not public—but it is possible to make educated guesses about the capabilities of some of the sources and methods employed in these fields.[64] For example, in the area of signals intelligence, it is widely believed that the U.S. intelligence community, together with foreign agencies, has broad capacities to intercept electronic communications taking place anywhere in the world.[65] Amateur observers have identified and tracked the paths of spy

61. Intelligence gathering and dissemination are sometimes understood as a cycle of planning and directing intelligence resources to answer specific questions; collecting raw intelligence; processing, producing and analyzing such raw intelligence into finished intelligence useful for policymakers; and disseminating it to relevant "consumers." JOHNSON, *supra* note 4, at 76. Others view the process as more interactive and spontaneous than a cycle: each "stage" continuously impacts what goes on in other stages, and there is, or should be, close collaboration between intelligence "producers" and "consumers." *See, e.g.*, CLARK, *supra* note 54 (advocating a more collaborative model of deriving actionable intelligence). Wilhelm Agrell is critical of the concept of the intelligence cycle and advocates its disposal. In his view, the concept works fairly well for handling mass data, but does not serve as a good model for problem-solving. TOWARD A THEORY OF INTELLIGENCE 21 (Gregory F. Treverton et al. eds. 2006) (Remarks of Wilhelm Agrell), *available at* http://www.rand.org/pubs/conf_proceedings/2006/RAND_CF219.pdf.

62. Under this discipline are the sub-disciplines of communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.

63. RICHARD A. BEST, JR., INTELLIGENCE ISSUES FOR CONGRESS, CRS report RL33539, at 4 (2008), *available at* http://www.fas.org/sgp/crs/intel/RL33539.pdf.

64. These guesses are often aided by media reports, which are sometimes followed by confirmations by the government. The disclosure of the Administration's interception of communications between persons in the United States and abroad is a case in point. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005 at A1 (reporting based on information gained from government sources that the President ordered the intercepts); Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (confirming general aspects of program).

65. *See* JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY FROM THE COLD WAR THROUGH THE DAWN OF A NEW CENTURY 354-418 (2001) (discussing the development of signals intelligence and international efforts to intercept telecommunications).

satellites.[66] Moreover, intelligence from publicly available sources has become an important, albeit non-exclusive, component of intelligence development.[67]

To a lesser extent, the need for secrecy also depends on the vulnerability of a source or method to countermeasures. It is unlikely that any source is completely invulnerable to detection or evasion, but Herman points out there are some differences in the "fragility" of sources.[68] Intelligence gained from breaking codes is particularly vulnerable to countermeasures because codes can be changed. Intelligence gathered through imagery, however, is less fragile: satellites can be countered through camouflaging techniques, but eventually large scale developments, such as troop movements, must happen in the open.[69] Gregory Treverton speculates that world events also have an impact on vulnerability.[70] According to Treverton, during the Cold War, intelligence was dependent on a relatively small number of collectors so that the exposure of one was very damaging. He writes, "Arguably, that is less so now with many, varied targets and much more information."[71]

---

66. The Visual Satellite Observer Home Page identifies and discusses several surveillance satellites. Spy Satellites, http://www.satobs.org/spysat.html (last visited Sept. 2, 2008); Naval Ocean Surveillance System (NOSS) Double and Triple Satellite Formations, http://www.satobs.org/noss.html (last visited Sept. 2, 2008).

67. Loch K. Johnson, *Spies*, 120 FOREIGN POL'Y 18, 22-23 (2000). Johnson estimated that "[d]uring the Cold War, about 85 percent of the information contained in espionage reports came from the public domain." *Id.* at 22. Writing in 2000, he estimated that 90 to 95 percent of such information comes from public sources. *Id.* Johnson nevertheless argues open source intelligence will never eliminate the need for human intelligence. *Id.* at 22-23. For a general discussion of intelligence sources and collection, see CLARK, *supra* note 54, at 63-96.

68. HERMAN, *supra* note 51, at 71, 90. Within signals intelligence, for example, the surveillance of electronic emissions is less vulnerable than the surveillance of communications. *Id.*

69. *Id.* at 90. According to Clark, clandestine communications intelligence, often derived from wiretaps, is the most highly protected source, with decrypted messages coming second. CLARK, *supra* note 54, at 96. At the same time, imagery intelligence has very little protection because information needs to be provided quickly to persons in the field and an adversary is aware satellites are being used. *Id.* at 96-97. Public sources are not protected but the methods for deriving intelligence from them are. *Id.* at 97.

70. *See* GREGORY F. TREVERTON, THE NEXT STEPS IN RESHAPING INTELLIGENCE (2005), *available at* http://www.rand.org/pubs/occasional_papers/2005/RAND_OP152.pdf.

71. *Id.* at 28. This leads Treverton to propose changes to the "need to know" policy to aid in the dissemination of information. *Id.* at 27. With regard to imagery, adversaries have learned to avoid detection by conducting activities underground or masking activities in buildings with no obvious indications of what is taking place inside them. JORDAN TAMA, THE PRINCETON PROJECT ON NAT'L SEC., INTELLIGENCE REFORM: PROGRESS, REMAINING

The public availability of general (and sometimes, quite detailed) information about sources and methods, as well as differences in their fragility, drain some strength from the secrecy argument. A rational adversary with access to publicly available information will make his own guesses about the capabilities of intelligence collection, or presume the worst. He will assume any electronic communication will be intercepted; every effort will be made to decrypt coded communications and will eventually succeed; his movements will be observed via satellite; any electronic funds transfers will be traced; and at some point, his organization will be infiltrated by foreign agents.[72] Since some forms of information do not reveal anything about sources or methods that an adversary does not already know or assume to be true, at a minimum it should be possible to have public debate about the general features of national security policy.[73] Moreover, if some sources are in fact less fragile than others, it should be possible in some cases to have a quite detailed debate using intelligence obtained from sources that are relatively robust.

There are, however, two responses to this argument. First, adversaries make mistakes. The Japanese military never realized its wartime codes had been broken, even though there was evidence to that effect.[74] Second, the problem becomes more complex if one moves from the broad brushstrokes of national security policy to finer detail. Information about the effectiveness of a particular surveillance program would obviously be useful in a debate about whether to start the program in the first place or later to continue it, but at the same time such information would alert an adversary to the limitations of that program

---

DEFICIENCIES, AND NEXT STEPS 18-19 (2005), *available at* http://www.princeton.edu/~ppns/papers/intel_reform.pdf.

72. *See* Mark Sappenfield & Mark Clayton, *How media leaks affect war on terror*, CHRISTIAN SCI. MONITOR, Jun. 30, 2006, at USA Section, *available at* http://www.csmonitor.com/2006/0630/p02s01-usfp.html (reporting how some intelligence experts assume terrorists are aware of various forms of electronic monitoring reported by the press).

73. DAVID M. BARRETT, THE CIA AND CONGRESS: THE UNTOLD STORY FROM TRUMAN TO KENNEDY 95 (2005). Sometimes, adversaries do not have to guess U.S. intentions; in 1951, Congress publicly authorized $100 million for covert operations against the Soviet Union. *Id.* at 103.

74. ANDREW, *supra* note 34, at 137-38 (discussing use of information from intercepts to assassinate Admiral Isoroku Yamamoto); ABRAM N. SHULSKY & GARY J. SCHMITT, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 46 (3rd ed. 2002) (noting that after the Battle of Midway, the Chicago Tribune published materials derived from decoded messages).

and provide ways to circumvent it. Or it may be that finished information can be attributed to only one or two sources of raw information, or is dependent on a web of sources, some of which are open or robust, others of which are fragile.[75] We are thus at the point where Thompson's dilemma, that sometimes it is not possible to have both effective policy and full accountability at the same time, becomes most salient.[76] However, as I discuss more fully below, these considerations do not take away from the sense that, given the information on intelligence sources and methods already available, some forms of democratic debate are possible. Moreover, we are able to frame better questions of both those who hold secret information and those who oversee them.

### *2. The Limitations of Intelligence and its Role in Public Policy Decisions*

Like Russian dolls, secrecy to protect sources and methods nests within the collection and development of useful intelligence, which in turn nests within the development of national security policy—just one of several areas important to the United States. It follows that the value of sources and methods and the need to protect them depends in part on the value of the intelligence derived from them, which in turn depends on how important intelligence is in the formation of national security policy. The value of both can be modest.

#### *a. Intelligence as Educated Guess*

As an initial matter, it is worth considering what one means by intelligence. The definition of intelligence is subject to debate, some of which goes to whether intelligence differs from information in general, whether the term should also encompass covert operations, and so

75. At the same time, an overemphasis on particular kinds of sources and methods might lead to biased judgments. Jennifer Sims argues: "There is . . . an analytical bias towards intelligence that comes with higher classification . . . . The sensitivity of the collection method, a key determinant of classification, does not necessarily correlate with the quality of the product." TOWARD A THEORY OF INTELLIGENCE 23, 23 (Gregory F. Treverton et. al. eds. 2006) (Remarks of Jennifer Sims). She states: "Assuming good intelligence involves information collected principally through secret means renders the United States particularly vulnerable to manipulation and deception." *Id.*

76. *See supra* text accompanying notes 36-49.

forth.[77] Kristan Wheaton and Michael Beerbower define intelligence as "a process, focused externally and using information from all available sources, that is designed to reduce the level of uncertainty for a decisionmaker."[78] As Clark points out, such definitions imply that what constitutes meaningful intelligence depends entirely on the user of intelligence and her needs.[79] Another implication is that some kinds of intelligence will be of legitimate interest to citizens and their representatives and others will not. In most cases, it is not obvious why citizens should have access to information about specific details about a source or method; for example, the identity of a foreign agent, the design of equipment used to detect radioactive emissions from a nuclear weapons test, or the specific algorithms used in data-mining. Nor is it obvious why the public should have access to tactical information like troop movements.

However, if scholars like Wheaton and Beerbower are correct, one must not lose sight of the fact that the ultimate purpose of intelligence is to help decision-makers make wise choices by reducing uncertainty. In fulfilling that primary mission, the only thing the intelligence community can do to reduce uncertainty is to make guesses—educated guesses about current and future states of the world, but guesses nonetheless—fraught with difficulty and naturally prone to "failure." As Richard Best explains, first, "hostile foreign countries and groups work hard to mask their capabilities and intentions."[80] Second, "many factors are inherently unforeseeable."[81] Third, "intelligence agencies do not always perform at maximum effectiveness."[82] Steps can be taken to minimize these problems, and the litany of intelligence failures should be accompanied by the litany of successes,[83] but in the end, it is

77. CLARK, *supra* note 54, at 13-14; LOWENTHAL, *supra* note 54, at 1-10.

78. Kristan J. Wheaton & Michael T. Beerbower, *Towards a New Definition of Intelligence*, 17 STAN. L. & POL'Y REV. 319, 329 (2006).

79. CLARK *supra* note 54 at 13.

80. RICHARD A. BEST, JR., U.S. INTELLIGENCE AND POLICYMAKING: THE IRAQ EXPERIENCE, CRS Report RS21696, at 1-2 (2005), *available at* http://www.fas.org/sgp/crs/intel/RS21696.pdf. For a good discussion of what can go awry in the intelligence cycle, see JOHNSON, *supra* note 4, at 76-99.

81. BEST, *supra* note 80, at 2.

82. *Id.* On organizational pressures on analysis, see e.g., Patricia M. Wald, *Analysts & Policymakers: A Confusion of Roles?*, 17 STAN. L. & POL'Y REV. 241, 262 (2006) (discussing internal pressures within the intelligence community to conform).

83. These successes include the CIA's judgment during the 1950s and early 1960s that the USSR was not planning to start a war with the United States. BARRETT, *supra* note 73, at 462.

unrealistic to expect the intelligence community to prevent all Pearl Harbors.[84]

The 2007 National Intelligence Estimate (NIE) on Iran's nuclear intentions and capabilities, a version of which was released to the public,[85] confirms the nature of the intelligence analysis of interest to policymakers. NIEs are intended to be the intelligence community's "most authoritative written judgments on national security issues."[86] They describe current information and "make judgments about the likely course of future events and identify the implications for US policy."[87]

The intelligence community is quite candid about the limitations of such judgments and about the role evidence plays in reaching them:

> We use phrases such as *we judge, we assess,* and *we estimate*—and probabilistic terms such as *probably* and *likely*—to convey analytical assessments and judgments. Such statements are not facts, proof, or knowledge. These assessments and judgments generally are based on collected information, which often is incomplete or fragmentary. Some assessments are based on previous judgments. In all cases, assessments and judgments are not intended to imply that we have "proof" that shows something to be a fact or that definitely links two items or issues.[88]

With respect to assessing the likelihood of developments or events, the NIE uses phrases along a continuum of certainty from "remote," "very unlikely," "unlikely," "even chance," "probably," "likely," "very likely," to "almost certainly."[89] The NIE also ascribes "high," "moderate," and "low" confidence levels to their judgments based on the scope and quality of information relevant to the intelligence

84. Rhodri Jeffreys-Jones views what he calls an "obsession" with crisis-prevention as peculiar to U.S. intelligence. RHODRI JEFFREYS-JONES, THE CIA & AMERICAN DEMOCRACY 249 (3d ed. 2003).

85. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, NATIONAL INTELLIGENCE COUNCIL, IRAN: NUCLEAR INTENTIONS AND CAPABILITIES, NATIONAL INTELLIGENCE ESTIMATE (2007), *available at* http://www.dni.gov/press_releases/20071203_release.pdf [hereinafter 2007 IRAN NIE].

86. *Id.* at 3. The U.S. intelligence community was restructured under the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified in scattered sections of 50 U.S.C.). For a general description of the structure of the community after 2004, see LOWENTHAL, *supra* note 54, at 30-53.

87. 2007 IRAN NIE, *supra* note 85, at 3.

88. *Id.* at 5 (emphasis in original).

89. *Id.*

community's judgments.[90] According to the NIE, high confidence "generally indicates that [the intelligence community's] judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment."[91] Moderate confidence "generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence."[92] Finally, low confidence "generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that [the intelligence community has] significant concerns or problems with the sources."[93] These remarks confirm, as L. Britt Snider puts it, that even the most considered and objective assessment of the intelligence community reflects a collective judgment, which in nature is an educated opinion and nothing more or less.[94]

The question arises what difference the opinion-like nature of important forms of intelligence makes on the need to protect the sources of information upon which those opinions are based. On the one hand, it could be argued it makes no difference at all. No one expects us to abandon intelligence activities simply because their end products are opinions; people rely on expert opinions all the time and believe on balance that they are much better than none at all. On the other hand, because the end products are assessments, it is perfectly appropriate for their recipients to ask about the bases of the various conclusions reached by the intelligence community. Indeed, it has been argued that policymakers misuse intelligence estimates if they take such assessments as infallible. Snider quotes a member of Congress as saying: "The real

90. *Id.* The NIE, however, immediately qualifies this statement by pointing out that a judgment of high confidence "is not a fact or a certainty . . . . [S]uch judgments still carry a risk of being wrong." 2007 IRAN NIE, *supra* note 85, at 5.

91. *Id.*

92. *Id.*

93. *Id.*

94. L. Britt Snider, *Sharing Secrets with Lawmakers: Congress as a User of Intelligence*, *in* INTELLIGENCE AND THE NATIONAL SECURITY STRATEGIST: ENDURING ISSUES AND CHALLENGES 85, 98 (Roger Z. George & Robert D. Kline eds., 2006); *see also* CYNTHIA M. GRABO, ANTICIPATING SURPRISE: ANALYSIS FOR STRATEGIC WARNING 13 (2002) ("Policymakers must recognize that warning cannot be issued with absolute certainty, even under the best of circumstances, but will always be an assessment of probabilities."); Mark Mazzetti, *With New Data, U.S. Revises Its View of Iran*, N.Y. TIMES, Dec. 5, 2007, at A12 (discussing how various changes in assessing the reliability of certain intelligence sources led to discarding some sources used in an NIE on Iran issued in 2005).

problem is, Members [of Congress] don't spend enough time probing what they hear from the Intelligence Community. If they spent more time analyzing what they were hearing, they would know more what needs to be fleshed out in order to make their own judgments."[95]

Consider how a decision-maker, who is being told by the intelligence community that its predictive judgments should not be taken as infallible, might go about making her own judgment about a national security matter. Suppose the intelligence community is moderately confident about an adversary's plans. The decision-maker could simply take the fact of moderate confidence at face value. However, it seems more consistent with the intelligence community's own characterization of its products for the decision-maker to ask questions; for example, whether there are competing theories among the various intelligence agencies which leads to moderate confidence. Eventually, such an inquiry could lead to a discussion of a particular source and why one agency has greater confidence in that source while another does not. Would it then be acceptable for secret-holders to tell that decision-maker to reach her own conclusions and withhold information necessary to do so?[96] In that situation, one cannot expect to enjoy the protection gained by acknowledging the necessarily speculative nature of one's assessments without allowing others to assess the factual bases of those speculations.

### *b. The "Facts" as one Factor among Many*

A proper assessment of the need to protect sources and methods involves not only understanding the tentative nature of the intelligence derived from them, but also understanding the role intelligence plays in the formation of foreign and national security policy. Lowenthal argues: "[I]ntelligence exists solely to support policy makers."[97] Yet,

95. Snider, *supra* note 94, at 98.

96. Of course, the problem becomes trivial if finished intelligence products do not jeopardize sources and methods. *See* CLARK, *supra* note 54, at 96 ("[U]sually the product is accorded less protection than the sources and methods . . . [because] the product, if lost, reveals only itself and not how it was obtained."). Wheaton and Beerbower argue that if intelligence is defined in part with respect to the policymakers for whom intelligence is developed and furnished, the need for secrecy, although not completely eliminated, is curtailed. Wheaton & Beerbower, *supra* note 78, at 329. Such a definition, in their view, would still require operational secrecy to protect sources and methods, but "[o]nce a decision has been made and an action carried out (without, of course, divulging sensitive sources and methods, particularly human sources), the need for secrecy is largely obviated." *Id.*

97. LOWENTHAL, *supra* note 54, at 2.

intelligence is only one of several factors policymakers take into account when deciding: others include an assessment of the costs and benefits of a particular policy, geopolitical objectives, available resources, and diplomatic and domestic risks, including political risks.[98] As a result, "[e]ven when official justifications for a chosen course of action highlight the conclusions of intelligence estimates, there are usually multiple factors involved."[99]

Intelligence is thus rarely the sole or determinative factor in public decision-making. Further, even when it plays a leading role, the correlation between intelligence and good policy can be weak. "Intelligence may be good or bad and policies may be good or bad, but in the real world good policy may be made in the absence of perfect intelligence and sound intelligence may not preclude making poor policy."[100] This is true in part because, as Abram Shulsky and Gary Schmitt put it, "Intelligence information and analyses will most likely support arguments both for and against any proposed policy . . . ."[101]

The public release in December, 2007 of the NIE on Iran's nuclear intentions and capabilities illustrates the complex relationship between intelligence and policymaking.[102] Whether Iran is developing nuclear weapons is of crucial concern. The 2007 NIE concluded with high confidence that in fall 2003, Iran halted its nuclear weapons program, but with moderate-to-high confidence that it is keeping open the option to develop nuclear weapons.[103] It also concluded that Iran had halted its

98. BEST, *supra* note 80, at 1.

99. *Id.*

100. *Id.* On the difficulties in crafting effective foreign or national security policy in general, see Richard K. Betts, *Is Strategy an Illusion?*, INT'L SECURITY, Fall 2000, at 5 (discussing the difficulties in deciding whether to use military force to achieve political ends). There is a broad collection of literature on the impact of cognitive heuristics on public opinion about foreign policy and on the formation of foreign policy. *See, e.g.*, Paul R. Brewer et. al., *International Trust and Public Opinion about World Affairs*, 48 AM J. POL. SCI. 93 (2004); Paul Goren, *Political Sophistication and Policy Reasoning: A Reconsideration*, 48 AM. J. POL. SCI. 462 (2004) (discussing the impact of beliefs on sophisticated and unsophisticated persons in their preferences for military spending); Josh Kerbel, *Thinking Straight: Cognitive Bias in the US Debate about China* (2004), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article03.html; Philip E. Tetlock, *Theory-Driven Reasoning about Plausible Pasts and Probable Futures in World Politics: Are We Prisoners of Our Preconceptions?*, 43 AM. J. POL. SCI. 335 (1999) (arguing that even experts cope with the complexities and ambiguities of world politics by resorting to theory-driven heuristics).

101. SHULSKY & SCHMITT, *supra* note 74, at 136.

102. 2007 IRAN NIE, *supra* note 85.

103. *Id.* at 9.

program because of pressure from the international community.[104] These results in 2007 contrasted with an earlier NIE issued in 2005 which found that Iran had not halted nuclear weapons development.[105] The 2007 report quickly became the center of controversy, as policymakers opposed to military intervention in Iran used the report to argue that economic sanctions against Iran were being effective, while others criticized the report as inaccurate or incomplete, in part because it did not focus on nuclear fuel enrichment, while still others debated whether the report's very release was helpful or harmful to U.S. foreign policy.[106]

"Everyone accepts the utility of intelligence as part of the bases upon which decisions are made."[107] However, if intelligence is at best one of several factors that contribute to policy decisions, and is subject to being discounted or ignored (particularly when controversial issues are involved), and if sometimes the link between intelligence and good policymaking is weak, the question arises whether the marginal benefits gained from that intelligence (and by implication the secrets used to protect its production), are worth their price in all contexts.

### *3. Secrecy and the Precautionary Principle*

Thus far I have examined the sources and methods argument for secrecy within the context of intelligence and policymaking. It is also important to examine the argument for its logical coherence. One problem in this respect is that it is often closely linked to the precautionary principle, which can lead to paralysis in certain situations. The precautionary principle dictates it is better to be safe than sorry. It is embodied in international environmental instruments, such as the United Nations Framework Convention on Climate Change and the Rio Declaration, both of which provide that scientific uncertainty about environmental issues should not prevent states from responding to those

104. *Id.*

105. *Id.*

106. *See* George Perkovich, *Assessing the NIE*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, (Dec. 4, 2007), http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=19747 (evaluating the 2007 NIE and discussing its implications for future U.S. responses to Iran); *see also* Steven Lee Myers, *An Assessment Jars a Foreign Policy Debate About Iran*, N.Y. TIMES, Dec. 4, 2007, at A1 (discussing various reactions to the assessment).

107. LOWENTHAL, *supra* note 54, at 177.

issues.[108] Its usefulness is apparent in the international response to climate change via the Kyoto Protocol, which requires reductions in greenhouse gas emissions, even though the Protocol was drafted when there was some uncertainty whether human activity impacts climate change.[109] Subsequent research has since led to broad consensus on the issue.[110]

Cass Sunstein points out, however, that in many situations the precautionary principle provides no guidance whatsoever because it works only when at least one of the available choices is risk-free.[111] Suppose someone must decide between action and inaction with regard to a particular matter. If action runs a risk of harm and refraining from action does not, the choice is obvious. But in most cases risk is involved whether one acts or not. Unless one can quantify and balance the potential risks of action and inaction, the precautionary principle leads to deadlock: it dictates it is better to act than be sorry, and at the same time, it dictates it is better not to act than be sorry.

At times, the sources and methods argument can take on the logical form of the precautionary principle. A holder of information must decide whether to disclose information derived from a combination of sources and methods or keep it secret. The principle advises against disclosure if there is a risk it would lead to the discovery of the underlying sources or methods. But the failure to disclose might also create a risk of discovery. Sharing information about particular troop movements so they can be intercepted could cause an adversary to conclude its codes have been broken. However, failing to share such information may allow the same troops to capture personnel, documents, or equipment that will lead the adversary to reach the same conclusion. As one moves from these tactical situations to more strategic decisions,

---

108. United Nations Framework Convention on Climate Change, art. 3, ¶ 3, May 9, 1992, S. Treaty Doc. No. 102-38, 1771 U.N.T.S. 170; United Nations Conference on Environment and Development, June 3-14, 1992, *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/26 (June 14, 1992).

109. Lisa Heinzerling, *Climate Change, Human Health, and the Post-cautionary Principle*, 96 GEO. L. J. 445, 456-57 (2008).

110. INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE, CLIMATE CHANGE 2007: THE PHYSICAL SCIENCE BASIS, SUMMARY FOR POLICYMAKERS 3 (2007), *available at* http://www.aaas.org/news/press_room/climate_change/media/4th_spm2feb07.pdf (concluding with "very high confidence," that human activities have led to global warming). Lisa Heinzerling argues that there was much less scientific uncertainty about global warming when the Rio Declaration was issued. Heinzerling, *supra* note 109, at 457.

111. CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE, 26-34 (2005).

the merits of the precautionary principle become even more tenuous because, as discussed above, intelligence sources and methods are not ends in themselves, but must be placed in the larger context of intelligence production and the uses of intelligence in policymaking. There, the precautionary principle leads nowhere because mirrored against the risk that disclosure will harm society is the risk that failure to disclose now will lead to ill-considered decisions that will harm it even more.

### *4. Secrecy and the Impacts of Information Asymmetries*

Finally, it is important to recall the impact of secrets in general on decision-making. By definition, secrets create information asymmetries, causing inefficiencies that have been well described in the literature.[112] Disparities in knowledge create two problems: adverse selection and the moral hazard. Adverse selection arises when a party with less information does not trust the party with more and thus does not enter what would have been a mutually beneficial transaction. The moral hazard arises because a party with less information does not know whether the party with more is acting in the former party's interests. Because asymmetries often result in inefficiencies, it is important to trace the possible dynamics of using secrets to protect sources and methods, both the dynamics specific to intelligence, and those that relate to secrets in government more generally, particularly when such asymmetries exist in bureaucracies and other institutions.

As was true with the breaking of the Japanese diplomatic codes, in many respects, the problem of secrecy to protect sources and methods is one of dissemination. When should information be shared and when should it be kept secret, given that any time information is shared there

112. The pioneering work was begun by scholars such as Kenneth Arrow and George Akerlof. *See, e.g.*, George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970); Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963). For examples of how information asymmetries operate in politics, including a discussion of the incentives that information asymmetries create in committee structures, see David Austin-Smith & William H. Riker, *Asymmetric Information and the Coherence of Legislation*, 81 AM. POL. SCI. REV. 897 (1987); Vijay Krishna & John Morgan, *Asymmetric Information and Legislative Rules: Some Amendments*, 95 AM. POL. SCI. REV. 435 (2001). For a review of the literature on sensitive information from the perspective of economics, psychology, sociology, etc., see E. Dale Thompson & Michelle L. Kaarst-Brown, *Sensitive Information: A Review and Research Agenda*, 56 J. AM. SOC'Y INFORMATION SCI. & TECH. 245 (2005).

is a risk the underlying sources and methods will be revealed? [113] Someone must decide whether the benefits of disclosure outweigh the potential harm. The benefits of such disclosure could be measured by the magnitude of harm that might be avoided, or the strategic or tactical advantage that might be gained from disclosure, discounted by the possibility that such disclosure will have little or no impact on a decision-maker. The variables that go to the risks of disclosure include an assessment of the availability of alternative sources of information, the vulnerability of the source involved, and the value of future information flows from that source, which, in turn, depends on the anticipated persistence of a particular threat or national security situation.

It goes without saying; each of these assessments is inexact. The real problem arises, however, when one asks who is in a better position to make these assessments. As between the information holder and the potential recipient, the information holder is probably better positioned to assess the availability of alternate sources of information and the vulnerability of sources to detection and countermeasures. However, the potential recipient is in the better position to assess whether the information in question, or the information that might be provided to her in the future, is or will be useful. The problem is that the information holder makes that decision for her. As a result, the information holder always runs the risk of providing too much or too little information to the potential recipient. The problem can be ameliorated to some extent by communication between the holder and the recipient, but it never completely disappears.

The amount of disclosure required can be context-specific. James Steinberg argues that counter-terrorism requires a more open system where information is shared among a broader set of actors, because potential targets are diffuse and attacks take place on the local level.[114] In his view, the security structure built in response to the Cold War is ill-fitted for this new climate.[115] That architecture placed a high premium on information security and included tight background checks, rigid compartmentalization, and allowed the agency that developed a

113. *See supra* text accompanying notes 33-35.

114. *Intelligence and Nat'l Sec. Policy: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* (Oct. 14, 2003) (statement of James B. Steinberg, Vice President & Director, Foreign Policy Studies Program, Brookings Institution), *available at* http://govinfo.library.unt.edu/911/hearings/hearing4/witness_steinberg.htm.

115. *Id.*

particular item of information to control its dissemination.[116] "This system assumed that it was possible to know a priori who 'needed to know' and that the risk of inadvertent or malicious disclosure was greater than the benefit from wider information sharing."[117] There have been some attempts at reform, but the problem remains large and intractable.[118]

In this regard, the system Steinberg complains of is immense and expensive. In Fiscal Year 2005, for example, various agencies classified about 14.2 million items of information as top secret, secret, or confidential.[119] That same year information security activities cost

116. *Id.*

117. *Id.*; *see also* CLARK, *supra* note 54, at 98 ("The major penalty compartmentalization imposes on the intelligence business is that it restricts critical review of the analytic product."). The 9/11 Commission attributes the failure to recognize or take advantage of these opportunities to a number of factors, many dealing with the failure to share information. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 353, 355-56 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf [hereinafter THE 9/11 COMMISSION REPORT]. In another example, Laura Donohue argues that practical cooperation on the international level to prevent the funding of terrorist organizations is impeded by government reluctance to share evidence with other states to substantiate why certain individual's and entities' assets should be blocked, out of a fear of disclosing sources and methods. Laura K. Donohue, *Anti-Terrorist Finance in the U.K. & U.S.*, 27 MICH. J. INT'L L. 303, 381 (2006); *see also* HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE AND THE SENATE SELECT COMMITTEE ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. Rep. No. 107-351 & H.R. Rep. No. 107-792, at xvii (2002) [hereinafter SENATE AND HOUSE SELECT COMM. REPORT] (finding that the failure of the CIA to recognize significant information being collected about potential terrorist activity led in turn to a failure to take precautions that might have prevented the attacks).

118. In response to concerns about the failure of agencies to share relevant information, the government proposed a series of initiatives known as the Federal Enterprise Architecture, which are designed to improve information-sharing among agencies. For a description and critical evaluation of the program, see Peng Liu & Amit Chetal, *Trust-Based Secure Information Sharing Between Federal Government Agencies*, 56 J. AM. SOC'Y INFO. SCI. & TECH. 283 (2005). Provisions of the Intelligence Reform and Terrorism Prevention Act provide for greater horizontal sharing of intelligence among agencies. 6 U.S.C.A. § 485 (West 2008). The President followed the recommendations of the 9/11 Commission for greater information sharing through executive order. Exec. Order No. 13,356, 69 Fed. Reg. 53599 (Aug. 27, 2004).

119. INFORMATION SECURITY OVERSIGHT OFFICE, REPORT ON COST ESTIMATES FOR SECURITY CLASSIFICATION ACTIVITIES FOR 2005, 3 (2005), *available at* http://www.archives.gov/isoo/reports/2005-cost-report.pdf [hereinafter REPORT ON COST ESTIMATES] This represented a nine percent decrease from 2004, but the ISOO states it remains cautious as to whether this represents a trend. *Id.*

approximately $7.7 billion.[120] There may be so many secrets that it is impossible to track them all, let alone evaluate whether information should continue to remain secret. The result is a bias in favor of secrecy to play it safe, thus resulting in an increasing amount of classified information. And because a large number of government agencies produce such information, huge coordination problems arise, which in turn are exacerbated by interagency rivalries endemic to any bureaucracy. Secrecy becomes it own justification, unmoored from any valid reasons for its existence.[121]

Joseph Stiglitz identifies four reasons why the government is unable to craft policies that result in Pareto improvements.[122] First, the government is unable to make credible commitments because it can always change its mind.[123] This inability to make commitments creates another set of inefficiencies, which is the "cost of creating next-best credibility-enhancing mechanisms."[124] Second, because of imperfect information, bargaining results in inefficient outcomes, and since policymakers know bargaining is a dynamic process, some will hold out and wait for a better deal in subsequent rounds.[125] Third, Stiglitz argues destructive competition exists where political competitors raise the costs of their opponents.[126] Fourth, people lack knowledge of the consequences of change and misunderstand the nature of policy decisions; politicians mistakenly believe they are in a zero-sum game.[127] "[T]here is often a generalized skepticism about proposals offered by an adversary that leads politicians to think that anytime an adversary makes a proposal, it must involve the adversary benefiting at their expense."[128]

---

120. *Id.* at 2-3. These costs included those incurred for personnel security, physical security, information security, professional training, and security management and planning. *Id.* at 1-2. Cost estimates from the CIA are not included because that information is classified. REPORT ON COST ESTIMATES, *supra* note 119, at 3.

121. The irony is that the large number of secrets, coupled with modern communications technology, such as electronic mail, increases the likelihood secrets will be disclosed.

122. Joseph Stiglitz, *The Private Uses of Public Interests: Incentives and Institutions*, 12 J. ECON. PERSPECTIVES 2, 7-15 (1998).

123. *Id.* at 8-11.

124. *Id.* at 10. These are strategies designed to make it costly for the government to change its mind. According to Stiglitz, such strategies raise transaction costs, which makes change difficult, thereby preventing Pareto improvements. *Id.*

125. Stiglitz, *supra* note 122, at 11-12.

126. *Id.* at 12-13. For Stiglitz, destructive competition arises under conditions of imperfect competition in which firms gain an advantage not by producing a better product at lower cost, but by raising the costs of its competitors. *Id.*

127. *Id.* at 13-14.

128. Stiglitz, *supra* note 122, at 13.

In Stiglitz's view, secrecy exacerbates these problems in several ways.[129] Those who were barred from the commitment process on grounds of secrecy are justified in trying to change the outcome, because they have no reason to trust that their interests were considered.[130] Indeed, it is unlikely the interests of those excluded from the process will be considered as fully as those included, which increases the incentives of excluded groups to overturn the results of the process.[131] As a related matter, secrecy worsens the costs of positional goods and destructive competition in government.[132] "It short-circuits the consensus process and makes it more likely that outcomes will lead to a greater divergence between winners and losers."[133] "Third," he continues, "by making information scarce, it contributes both to the perception and reality of asymmetrical information, and puts into play a dynamic which is more likely to lead to biased and unrealistic information."[134] As Stiglitz puts it: "In a world of secrecy, you will always suspect that some interest group is taking advantage of the secrecy to advance their causes over yours. . .."[135]

Rhodri Jeffreys-Jones puts the matter this way:

> In keeping certain information hidden from foreign powers, the director of the CIA must necessarily refrain from instructing (and may even actively deceive) the American people and all but a few of their elected representatives. But as dissimulation is a well-known strategy of the shadier type of politician, and as it might also signify an attempt by a particular president to expand his powers at the expense of Congress, arguments about the need for secrecy often meet with a cynical reception.[136]

Jeffreys-Jones uses the term "dissimulation," but one need not go that far to understand that administrations can use secrecy to engage in what Habermas calls "steering."[137] The role secret intelligence plays in

129. *Id.* at 15.
130. *Id.*
131. *Id.*
132. Stiglitz, *supra* note 122, at 15.
133. *Id.*
134. *Id.*
135. *Id.*
136. JEFFREYS-JONES, *supra* note 84, at 3.
137. Pat Holt argues that the Reagan administration exaggerated intelligence reports from Central America to support its policies there. According to Holt, the congressional oversight committees were aware of these exaggerations but were constrained from revealing them for security reasons. Similarly, the Johnson administration misrepresented the encounter between

decision-making becomes more complex because of the ways in which information can be used through framing, persuasion, and media priming[138] to manipulate people into assenting to public policies. An argument that secrecy is needed to protect sources and methods might have no basis in reality, or it might be just one of several reasons why the government might want to keep a particular item of information secret. Secrecy can of course be used to cover up activities or mistakes that would be criticized by the public. Stiglitz argues, for example, that secrecy in government most often "serves as a cloak behind which special interests can most effectively advance their interests, outside of public scrutiny."[139] Many have argued national security concerns rarely motivate most government secrets.[140]

One result is that government can shift the costs of inaccurate or incomplete information from itself to the larger society. Sometimes this shift is obvious. For example, until legislation was enacted in 2007, the annual budget for the intelligence community was classified, known only to the executive branch, select members of Congress, and high officials in the intelligence community, and even under the new law, the President can waive public disclosure of the budget on national security grounds.[141] A secret budget makes it possible for the government to

---

the United States and North Vietnam in the Gulf of Tonkin, which led in part to passage of the Tonkin Resolution. HOLT, *supra* note 4, at 14.

138. *See generally* James M. Druckman, *On the Limits of Framing Effects: Who can Frame?*, 63 J. POL 1041 (2001) (discussing the limitations of the framing effect).

139. Stiglitz, *supra* note 122, at 16.

140. *See, e.g., id.* at 15-16; *see also* United States v. N.Y. Times Co. et. al., No. 71 Civ. 2662, 1971 WL 224067, ¶ 17 (S.D.N.Y. Jun. 17, 1971) (Frankel Aff.).

> [T]he Government and its officials regularly and routinely misuse and abuse the "classification" of information, either by imposing secrecy where none is justified or by retaining it long after the justification has become invalid, for simple reasons of political or bureaucratic convenience. To hide mistakes of judgment, to protect individuals, to cover up the loss and waste of funds, almost everything in government is kept secret for a time and, in the foreign policy field, classified as "secret" and "sensitive" beyond any rule of law and reason. Every minor official can testify to this fact.

*Id.*

141. LOWENTHAL, *supra* note 54, at 42, 205- 207. Section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 335 (2007), requires the Director of National Intelligence to disclose to the public the aggregate amount appropriated by Congress for intelligence purposes at the end of each fiscal year. Beginning fiscal year 2009, the President may waive or postpone the disclosure

spend too little or too much on intelligence collection, and the ability to mask the costs of such collection removes important incentives to allocate efficiently scarce resources for that purpose.[142] To take another example, if for secrecy reasons intelligence users are denied access to information needed to verify the accuracy of intelligence upon which a policy decision is based, there is less reason for intelligence producers to make sure such intelligence is accurate in the first place. But perhaps the most costly impact of secrecy is lack of trust. Since secrecy enables the government to shift costs, the public is justified in taking what the government has to say with a grain of salt, and in the end may reject a proposal that would actually benefit it.

### *C. The Lessons of Secrecy for Democracy*

As discussed in Part II, democratic concepts and deliberative principles do not always provide definitive guidance on the uses of secrecy. In this Part III, however, I have shown that although the protection of sources and methods is often a compelling reason for secrecy, it is not always so. Much is publicly known about these sources and methods, and to some extent, the need for secrecy is not uniform among all sources and methods because some are less vulnerable to detection or evasion, or both, than others. Further, the protection of sources and methods is only as important as the intelligence derived from them, which in turn is only as important as the role intelligence plays in policymaking. Finally, the dynamics of information asymmetries are such that secrets result in inefficiencies and perverse incentives in the collection, processing, and dissemination of intelligence, which ultimately results in shifting the costs of inaccurate or incomplete information to the public. The upshot is that the secrecy argument shares aspects of reality and unreality, as does democracy as idea and institution.

---

requirement if he provides a statement to the respective Senate and House select committees on intelligence that such disclosure would "damage national security." *Id.* sec. 601(b). The President must detail the reasons for a waiver or postponement; such reasons can be in classified form. *Id.* For a general discussion of Presidential certifications and determinations, see Mark A. Chinen, *Presidential Certifications in U.S. Foreign Policy Legislation*, 31 N.Y.U. J. INT'L L. & POL. 217 (1999).

142 Even under the 2007 legislation, since only the aggregate amount of money budgeted for intelligence must be disclosed, *supra* note 141, the public and most members of Congress will not be able to assess these more detailed allocations.

## IV. DEMOCRACY AND SECRECY IN VARIOUS CONTEXTS

### *A. Framing the Democracy v. Secrecy Debate*

Given the foregoing discussions of democracy and secrecy on their respective merits, how might the two inform each other? As an initial matter, to conceive of democracy in terms of freedom from coercion, meaningful consent, deliberation, or accountability is to do so on very broad terms that sometimes do not give much purchase. However, if intelligence derived from protected sources and methods, is, although the product of experts, necessarily tentative, and about which there are varying degrees of confidence, and which comprise only one of several factors decision-makers take into account, then the debate about democracy and secrecy is much more complex than a collision between the ideals of a political system and the realities of national security and its demands. The attack on Pearl Harbor was certainly real, as were the attacks on the World Trade Center and the Pentagon. But equally real was the internment of Japanese Americans and, as of this writing, the deaths of thousands of American soldiers and many more Iraqi civilians—events set into motion at least in part on intelligence assessments that were either ignored[143] or eventually proved groundless.[144]

Such results would be of concern to any country, let alone a democracy. If they do nothing else, the broad democratic concepts discussed in Part II highlight or locate areas of concern that merit higher scrutiny of the secrecy argument. There are undoubtedly times when the secrecy argument will prevail. However, the conclusions drawn from Part III indicate that the secrecy argument should not always carry the day.

---

143. J. Edgar Hoover and others argued that there was no national security reason for relocating Japanese-Americans. TETSUDEN KASHIMA, PERSONAL JUSTICE DENIED: REPORT OF THE COMMISSION ON WARTIME RELOCATION AND INTERNMENT OF CIVILIANS 186-88 (1996).

144. COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT 45 (2005) *available at* http://www.wmd.gov./report/wmd_report.pdf [hereinafter COMM'N ON THE INTELLIGENCE CAPABILITIES] (concluding Iraq was not engaged in the production of weapons of mass destruction at the time of the invasion); SELECT COMMITTEE ON INTELLIGENCE, POSTWAR FINDINGS ABOUT IRAQ'S WMD PROGRAMS AND LINKS TO TERRORISM AND HOW THEY COMPARE WITH PREWAR ASSESSMENTS, S. REP. NO. 109-331 (2d. Sess. 2006) (reaching the same conclusion with respect to weapons of mass destruction and finding there were no meaningful links between the Iraqi government and Al Qaeda).

## *B. Situations of Strict Scrutiny*

### *1. Decisions of National Moment*

One area in which the secrecy argument must be given particular scrutiny is when the country is making decisions of national moment, such as the decision to go to war. It goes without saying that the use of force is costly in terms of lives, resources, and reputation. Yet, as was true on the eve of World War II, the argument that sources and methods must be protected appears most persuasive against the backdrop of looming armed conflict.

One cannot overstress, however, that short of an armed attack or a declaration of war by an adversary, the decision to use force will always turn on judgments with varying degrees of certainty about an adversary's intentions and activities. In this context, the question arises whether any source or method and the information flows either is designed to protect is worth the human, economic, and reputational costs of engaging in armed conflict in error. This is particularly salient because, as discussed in Part II, the kind of intelligence used to justify the use of force is the predictive intelligence or general assessment of an adversary's plans that the intelligence community itself urges should not be taken as unqualified truth.

In these contexts, democratic concerns come to the fore: because the stakes are so high and citizens will bear the brunt of a decision to use force, this is precisely when meaningful consent by citizens is most required and when their representatives need to give compelling reasons for incurring the costs of war. In this kind of decision, "citizens are capable of judging as well as officials, and if they are less informed, it is the fault of the officials who conceal critical information."[145] If the reasons for engaging in conflict are based on secret judgments of the intelligence community, those who are making the case for armed conflict must be prepared either to disclose the information needed to assess the reliability of such intelligence or to have their claims heavily discounted.

145. AMY GUTMANN & DENNIS THOMPSON, DEMOCRACY AND DISAGREEMENT 97 (1996).

*2. Decisions Impacting Individuals and Government Compliance with Law*

It is probably in the area of civil liberties that the effects of secrecy in decision-making are the most poignant and painful, evoking Kafkaesque images of persons who find themselves subjected to absurd and nightmarish treatment. Here the coercive force of government becomes most salient and thus justifies careful scrutiny of the secrecy argument when used in this context. Yet, the post 9/11 use of extraordinary renditions, severe interrogation tactics, indefinite detention, and warrantless surveillance find their justification, in part, as sources and methods needed to prevent further attacks. How are such justifications to be assessed?

The literature on the impact of government policies on civil liberties and human rights after 9/11 is voluminous,[146] and it is beyond the scope of this Article to discuss all of the issues raised by these practices, particularly as they relate to individuals. That democracies must protect counter-majoritarian interests is of course an important part of democratic accounts. In the national security context, the issue is often framed as a tension between counter-majoritarian and majoritarian interests or between Kantian and utilitarian understandings of justice. I limit my discussion here, however, to the view that a democratic constitution reflects decisions about the community's values and about how it will conduct itself, even in times of conflict. In a constitution, the majority has pre-committed itself to preserving certain counter-majoritarian interests. The same is true with laws that emerge from that constitution. Thus, although it may be that the U.S. Constitution is not (to use what is becoming a worn-out phrase) a suicide pact, something vital to democracy is lost if widely held substantive values expressed in the Constitution and other law, which are meant to strike a balance between security and liberty, are ignored. As Jon Elster notes: "If the

146. Several authors have discussed and criticized post 9/11 administration policies regarding detention, interrogation and torture. *See, e.g.*, José E. Alvarez, *Torturing the Law*, 37 CASE W. RES. J. INT'L L. 175 (2006); David Luban, *Liberalism, Torture, and the Ticking Bomb*, 91 VA. L. REV. 1425 (2005); Deborah N. Pearlstein, *Finding Effective Constraints on Executive Power: Interrogation, Detention and Torture*, 81 IND. L.J. 1255 (2006); Jeremy Waldron, *Torture and Positive Law: Jurisprudence for the White House*, 105 COLUM. L. REV. 1681 (2005). On the history of civil liberties in times of national crisis, see GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME, FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM (2004).

framers try to prevent the constitution from becoming a suicide pact, it may lose its efficacy as a suicide prevention device."[147]

These concerns often arise in the courts, since they decide what the law is, but the secrecy dilemma also bedevils relations here. The state secrets doctrine is one example.[148] Under that doctrine, the government can ask the court to protect certain information as privileged state secrets. If the court decides such information is privileged, the court will exclude it from consideration. If there is enough non-privileged evidence to enable the parties to make their respective cases, the court can allow a case to proceed; but if there is not, the court will dismiss the case, often on grounds of lack of standing or ripeness.[149]

A recent decision illustrates the problems raised by the doctrine. In *El-Masri v. United States*, the U.S. Court of Appeals for the Fourth Circuit used the state secrets doctrine to affirm the dismissal by a federal district court of a challenge to the CIA's extraordinary rendition policy.[150] The plaintiff, a German citizen, alleged the CIA had

147. JON ELSTER, ULYSSES UNBOUND: STUDIES IN RATIONALITY, PRECOMMITMENT, AND CONSTRAINTS 174 (2000) (emphasis omitted).

148. For recent discussions of the doctrine, see Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249 (2007); Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007); William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85 (2005). The dilemma shows itself in other contexts, such as the use of secret evidence in military commissions. Military Commissions Act, § 3, 10 U.S.C. §§ 948a-950 (2006). There, a military judge may protect from disclosure "the sources, methods or activities by which the United States obtained the evidence" against the defense, if the military judge finds such information to be classified. *Id.* § 949j(c)(2). In such an instance, the military judge *may* require the trial counsel to provide, "to the extent practicable, an unclassified summary" of such sources, methods, or activities. *Id.* The same procedure is followed for exculpatory evidence. *Id.* § 949j(d)(1). In respect to Freedom of Information Act ("FOIA") requests, in *CIA v. Sims*, 471 U.S. 159 (1985), the Supreme Court held that the names and institutional affiliations of persons who participated in CIA-sponsored research on the use of biological, chemical, and radiological materials to alter human behavior were not subject to FOIA disclosure. In doing so, the Court found that the Director of Intelligence had broad power to protect "sources and methods" as required by Section 102(d)(3) of the National Security Act and rejected a narrower, functional definition of intelligence sources that focused on whether confidentiality was needed to obtain the type of information desired. *Id.* at 168-69; *see also* Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public's Right to Know about the CIA*, 17 STAN. L. & POL'Y REV. 353, 375-80 (2006) (arguing that provisions of the Intelligence and Reform and Terrorism Prevention Act curtail the reach of Sims).

149. The modern doctrine arose from United States v. Reynolds, 345 U.S. 1 (1953). There the U.S. Supreme Court denied on state secrecy grounds access to certain documents related to the crash of a B-29 bomber that was testing secret electronic equipment. For recent discussions of the doctrine, see Weaver & Pallitto, *supra* note 148, at 87; Chesney, *supra* note 148; Frost, *supra* note 148.

150. El-Masri v. U. S., 479 F.3d 296 (4th Cir. 2007), *cert. denied*, 128 S. Ct. 373 (2007).

transported him from Macedonia to Afghanistan, where he was detained and subjected to cruel, inhuman, and degrading treatment.[151] The CIA claimed the state secrets privilege, and the appeals court relied on two declarations by the Director of the CIA—one unclassified and the other classified—which stated that there was a danger state secrets would be revealed if the litigation went forward.[152] According to the appeals court, the classified CIA declaration "detailed the information the United States sought to protect, explained why further court proceedings would unreasonably risk . . . disclosure, and spelled out why such disclosure would be detrimental to the national security . . . ."[153] The appeals court relied on the government's claims in the confidential declaration and did not engage in its own in camera review of the evidence at issue to determine whether the privilege was warranted.[154] The court found the case could not proceed on publicly available information, in part because in the court's view, the government would not be able to craft an adequate defense without disclosing information "regarding the means and methods by which the CIA gathers intelligence."[155]

The court was able to justify its decision in part because an individual plaintiff was involved. At the end of its opinion, the court acknowledged that the "successful interposition of the state secrets privilege imposes a heavy burden on the party against whom the privilege is asserted."[156] When the privilege is imposed, however, the

151. *Id.* at 300.

152. *Id.* at 309-10.

153. *Id.* at 301.

154. *Id.* at 306, 311-12.

155. *El-Masri*, 479 F.3d.at 309. According to the appeals court, such information might include the fact and details of his detention; testimony from personnel involved; the identities of participating countries, if any; information about how CIA operations are specified; how the CIA makes personnel assignments; and the production of witnesses whose identities are classified. *Id.* at 309-10.

156. *Id.* at 313. As a related matter, it appears the appeals court had some misgivings about basing its decision on information given in the classified declaration, to which the plaintiff had no access. *Id.* at 312. The appeals court wrote: "That El-Masri is unfamiliar with the [c]lassified [d]eclaration's explanation for the privilege claim does not imply . . . that no such explanation was required, or that the district court's ruling was simply an unthinking ratification of a conclusory demand by the executive branch." *Id.* The problem with that response, of course, is that in camera and ex parte examinations of "evidence" and arguments undermines a fundamental principle of the adversarial system, that the parties, not the judge, are responsible for framing their respective cases and marshalling evidence for them. WILLIAM BURNHAM, INTRODUCTION TO THE LAW AND LEGAL SYSTEM OF THE UNITED STATES 82 (4th ed. 2006).

plaintiff's "personal interest in pursuing his civil claim is subordinated to the collective interest in national security."[157]

This is not an unprincipled argument, but it is far from conclusive. Whether a person has been deprived of due process or has been subjected to unlawful treatment is not just an individual concern. Several commentators have criticized the state secrets doctrine as a common-law creation having no basis in the Constitution, and argue that it undermines aspects of the Constitutional structure. William Weaver and Robert Pallitto argue that overuse of the doctrine since the Carter Administration, and the almost unquestioning deference of the courts when the privilege has been evoked, threatens the independence of the judiciary.[158] Amanda Frost argues that the doctrine diminishes the power of Congress to establish the jurisdiction of courts and to oversee the executive branch.[159] Louis Fisher points out, in addition to the criticisms posed by other commentators, that the provenance of the doctrine is itself questionable.[160]

If these authors are correct, the doctrine also exacts costs on national security writ large. As Richard Betts argues:

> One may accept that decentralization, separation of powers, and checks and balances make democracy constitutionally antistrategic. But one may also assume that the procedural norms of constitutional democracy are, at least for the United States, the highest national security value, ranking above particular substantive values that come and go in policy.[161]

Why might this be so? Betts does not put it in these terms, but apart from the structural protections that might be jeopardized by the overreaching of one political branch, it is because, as discussed earlier, given the high degree of delegation in modern democracies, sometimes the only claims to legitimacy a government has in the eyes of citizens with little to no real power (particularly where national security is involved), are that the government has taken into account their interests, it can provide plausible reasons for the actions it takes, and is itself

157. *El-Masri*, 479 F.3d at 313.

158. Weaver & Pallitto, *supra* note 148, at 87.

159. Frost, *supra* note 148, at 1959.

160. LOUIS FISHER, IN THE NAME OF NATIONAL SECURITY: UNCHECKED PRESIDENTIAL POWER AND THE *REYNOLDS* CASE (2006). Fisher points out decades after the Reynolds decision, the documents originally sought in that litigation were declassified, and contained no secrets. *Id.* at 165-207. He concludes that the government deceived the courts into believing records of the accident were important to national security.

161. Betts, *supra* note 100, at 41.

guided by law. If the government does otherwise, it risks jeopardizing support for the very national security measures it seeks to take,[162] as well as the system of government those measures are supposed to protect.

For example, in 2005, Congress passed the Detainee Treatment Act (DTA), which prohibits the use of cruel, inhumane, and degrading treatment of detainees held by the United States. [163] The legislation reflects a value judgment that certain interrogation methods violate human dignity and are off-limits, even after 9/11. In this context, very little weight should be given to secrecy arguments when Congress or the courts are asked to determine whether such legislation is being obeyed. This follows not only because civil liberties are involved, but also because it is vital to the functioning of a government to determine whether enacted law is being implemented and whether it is effective.

This is not to say, if the arguments I made in Part II are correct, that the issues are simple. Consider a situation in which someone alleges before a court that the government has subjected him to an interrogation method expressly prohibited by the DTA. Assume a video recording proves unequivocally the prohibited method was used, but it also records other lawful interrogation methods that would be disclosed if the video recording is used in evidence. Under those circumstances, it would not be surprising for the government to argue in a confidential pleading that, although it neither confirms nor denies that the video recording does in fact capture the proscribed method, it can confirm that a number of classified interrogation techniques and methods would be disclosed if the video recording is used in evidence.[164] Given the history of court deference to the government in these cases, it would be equally unsurprising for a court to agree with the government, find that the video recording is privileged under the state secrets doctrine, and conclude either that the person who has made the allegations therefore lacks standing, or that the matter is not yet ripe for adjudication.

---

162. *See* Marc J. Hetherington, *The Political Relevance of Political Trust*, 92 AM. POL. SCI. REV. 791 (1998) (discussing the link between trust in government and the success of government policies).

163. Pub. L. No. 109-148, § 1003(a), 119 Stat. 2680, 2739 (2005) (codified at 42 U.S.C. § 2000dd (2006)).

164. For a discussion of interrogation techniques and their effectiveness, see INTELLIGENCE SCIENCE BOARD, NATIONAL DEFENSE INTELLIGENCE COLLEGE, EDUCING INFORMATION, INTERROGATION: SCIENCE AND ART: FOUNDATIONS FOR THE FUTURE (2006), *available at* http://www.fas.org/irp/dni/educing.pdf (an anthology of articles on the subject).

An outcome like this is difficult to assess given the amorphous nature of both democratic principles and the secrecy argument. On the one hand, as I have just discussed, one can argue that legislation prohibiting the interrogation method in question results from democratic values and processes and should be honored as such. Yet the same democracy, by prohibiting some methods, implicitly allows others, some of which would be disclosed if the video recording comes to light. Moreover, one could argue that court determinations about whether secret information is privileged—particularly when courts view evidence in camera—[165]represent the kind of partial secrecy suggested by Thompson, which is tolerated in a deliberative democracy. Finally, applying the state secrets doctrine in such circumstances would allow the government to shield discovery of prohibited intelligence activities by mixing them with permitted activities, but the government probably does in fact use an array of sources and methods that cannot be easily separated in a way that would allow the method in question to be disclosed for evaluation without disclosing permissible intelligence sources or methods.

On the other hand, every time a court privileges certain evidence as a state secret, there is a good chance it is misapplying the precautionary principle. This is because neither the choice to grant the privilege nor to deny it is risk free. Granting the privilege might indeed protect a legitimate source or method of intelligence. But it will also undermine both the individual's and the polity's interest in the vindication of her constitutional rights or legislative protections, or both, and could endanger the constitutional structures and the values they embody. Additionally, while on balance the government is in the better position to assess the harm to the country caused by a particular disclosure, the court is in a just as good or better position to determine the harm caused by not allowing the case to proceed. Further, given the current state of the doctrine, where even in camera inspection of classified information is prohibited, the claim to privilege could have no basis in fact.[166]

165. In this regard, however, the *El-Masri* court stated it was prevented from making its own direct determination of the evidence because of the *Reynolds* case. El-Masri v. United States, 479 F.3d 296, 312 (4th Cir. 2007). According to the *Reynolds* court, once a judge finds information is privileged, the judge herself should not review such information even alone in chambers. United States v. Reynolds, 345 U.S. 1, 10 (1953).

166. In light of the larger issues implicating the balance of powers, the prohibition of in camera inspection of allegedly privileged evidence is incomprehensible. The *El-Masri* court, aware of concerns that the state secrets doctrine cedes excessive power to the executive branch, argued that it is the very determination of privilege by a court that prevents the state

Finally, the court could take these risks to protect a source or method that is already known, that needs no protection because it is resistant to countermeasures, or that may be unproven, unreliable, or that may lead to intelligence that in the end will go unheeded or play only a small role in policymaking.[167]

---

secrets doctrine from lapsing into "a surrender of judicial control over access to the courts." El-Masri v. United States, 479 F.3d 296, 312 (4th Cir. 2007). Even if it is possible to move past the circularity of that reasoning, it is surprising that a court would rely solely on arguments made in confidential declarations from the executive branch. Legislation proposed in early 2008 attempts to address some of these concerns. The State Secrets Protection Act, S. 2533, 110th Cong. (2008), sets out procedures for invoking the state secrets privilege. Under the proposed legislation, if the United States invokes the privilege, a federal court is empowered and required to hold an in camera hearing, at which the United States must provide all evidence that the United States claims is protected. *Id.* § 2. If the court determines that the item of evidence is subject to the privilege, it will not be used in evidence. *Id.* In that case, however, subject to certain requirements, the court must order the United States to provide a non-privileged substitute for the privileged evidence. *Id.* If the United States refuses to do so, the issue in question will be decided in the non-government party's favor. S. 2533, 110th Cong. § 2 (2008). A federal court may dismiss a claim or counterclaim on the basis of the state secrets act only if it determines first, that it is impossible to provide a non-privileged substitute that would provide a "substantially equivalent opportunity" to litigate the claim or counterclaim; second, that the dismissal would not "harm national security;" and third, that continuing with the litigation without the privileged evidence "would substantially impair the ability of a party to pursue a valid defense to the claim or counterclaim." *Id.*

167. Some of these issues are at stake in the on-going controversy over the CIA's destruction of video recordings of interrogations of two detainees suspected of ties with Al Qaeda. In the video recordings, the detainees are being subjected to severe forms of interrogation. *See* Mark Mazzetti, *C.I.A. Destroyed 2 Tapes Showing Interrogations*, N.Y. TIMES, Dec. 7, 2007, at A1. Such harsh techniques are believed to include waterboarding, in which the subject is made to feel as if he is drowning. These harsh forms of interrogation have been criticized as forms of torture, although the administration denies this. Several commentators have discussed and criticized these interrogation techniques. *See, e.g.*, George J. Annas, *Human Rights Outlaws: Nuremberg, Geneva, and the Global War on Terror*, 87 B.U. L. REV. 427 (2007); Dawn E. Johnsen, *Faithfully Executing the Laws: Internal Legal Constraints on Executive Power*, 54 UCLA L. REV. 1559, 1571-72 (2007); Steven A. Saltzburg, *A Different War: Ten Key Questions about the War on Terror*, 75 GEO. WASH. L. REV. 1021, 1045 n.100 (2007). Although the U.S. military is prohibited from engaging in harsher forms of interrogation, the CIA is not, even though the CIA is reported to have halted waterboarding in 2003. Scott Shane, *House Passes Restrictions on Interrogation Methods*, N.Y. TIMES, Dec. 14, 2007, at A18 (reporting that intelligence officials state waterboarding has not been used since 2003). The CIA argues that the tapes were destroyed in part to protect interrogators and their families from reprisals. *See* Mazzetti *supra*. However, CIA officers involved in the decision are reported to have said that "a primary factor was the legal risks that officers shown on the tape might face." Mark Mazzetti & Scott Shane, *Tapes' Destruction Hovers over Detainee Cases*, N.Y. TIMES, Mar. 28, 2008, at A1. In 2008, President Bush vetoed legislation that would have prohibited the CIA from using certain harsh interrogation techniques. Steven Lee Meyers, *Bush Vetoes Bill on C.I.A. Tactics, Affirming Legacy*, N.Y. TIMES, Mar. 9, 2008, at A1.

### C. *Assessing Political Branch Decisions and Oversight*

Given the problems that emerge in the judicial branch when secrets are involved, more intense focus falls on the political branches because they are responsible for setting and executing the national security policy with which secrets are so intertwined. An incident in 2006 illustrates some of the difficulties here. That fall, the Senate Select Committee on Intelligence issued a report on postwar findings on Iraq's purported WMD programs and links to terrorist organizations.[168] As discussed earlier, claims that Iraq was developing weapons of mass destruction and that it was linked to terrorist organizations were the primary reasons given for invasion, claims subsequently proved to be false. The report compared the post-war findings on these issues with the erroneous pre-war assessments, and classified information was used in making the report.[169]

---

Concerns about the use of secret information against individuals also arise in the holding of detainees at Guantanamo Bay. In Boumediene v. Bush, 128 S.Ct. 2229 (2008), the U.S. Supreme Court found that aliens held as enemy combatants at Guantanamo were entitled to habeas corpus protection. *Id.* at 2240. In its holding the Court rejected arguments that the system whereby Combatant Status Review Tribunals determine (subject to review by the U.S. Court of Appeals for the District of Columbia Circuit) whether an individual is a lawfully held enemy combatant, provided an adequate substitute for the writ. *Id.* at 2274. The Court reasoned in part that the procedures followed by the tribunals allowed for "considerable risk of error" in the findings of fact, in part because of the "constraints upon the detainee's ability to rebut the factual basis for the Government's assertion that he is an enemy combatant." *Id.* at 2238. Such constraints included the government's ability to use secret information against the detainee. *Id.*, at 2238.

Following the Court's decision in *Boumediene*, the D.C. Circuit overturned the finding of a Combatant Status Review Tribunal that a detainee was an enemy combatant. Parhat v. Gates, 532 F.3d 834, 850 (D.C. Cir. 2008). The evidence used to support the government's case against the detainee came from four U.S. intelligence documents, redacted from the public version of the opinion. *Id.* at 844-45. The court stated that the documents described events and relationships as having "reportedly" occurred, or "suspected of" having taken place. *Id.* at 846. "But in virtually every instance," the court criticized, "the documents do not say who 'reported' or 'said' or 'suspected' those things. Nor do they provide any of the underlying reporting upon which the documents' bottom-line assertions are founded, nor any assessment of the reliability of that reporting." *Id.* at 846-47. The court noted that the government might be able to submit information in forms that would protect the identity of a valuable source, but the court could not rubber-stamp as factual government assertions without evidence to support them. *Id.* at 849-50.

168. SELECT COMMITTEE ON INTELLIGENCE, POSTWAR FINDINGS ABOUT IRAQ'S WMD PROGRAMS AND LINKS TO TERRORISM AND HOW THEY COMPARE WITH PREWAR ASSESSMENTS, S. REP. NO. 109-331 (2d. Sess. 2006).

169. *See id.* at 4-8.

The committee acknowledged that a balance must be struck between the need to protect sources and methods and the need for transparency of intelligence activities.[170] At the same time, however, the committee protested the intelligence community's decision to keep certain portions of the report's findings and conclusions secret:

> In its decision to keep this information from the public, the Intelligence Community was unable to demonstrate to the Committee that disclosing the redacted information would compromise sensitive sources and methods or otherwise harm national security. The Committee concludes that the Intelligence Community's decision to classify this information is without justification.[171]

Decision-makers were not persuaded by arguments that certain classified information would jeopardize sources and methods if made public. However, the committee allowed the classification decision to stand, thus depriving the rest of Congress and the public of information that would have helped it assess the wisdom of a decision of national importance.

The relationship between the legislative and executive branches in the area of national security is complex and difficult, as is the relationship between these branches and the intelligence community. Congress has occasionally asserted its powers in matters relevant to foreign and national security policy, but over time, the executive branch has come to dominate the conduct of foreign affairs.[172] Nowhere is this dominance clearer than in the area of intelligence.[173] Most concede the

---

170. *Id.* at 7.

171. *Id.* at 8.

172. This is part of a more general trend in which the office of the Presidency has grown in importance, particularly since the Roosevelt Administration. *See, e.g.*, Michael A. Fitts, *The Paradox of Power in the Modern State: Why a Unitary, Centralized Presidency May Not Exhibit Effective or Legitimate Leadership*, 144 U. PENN. L. REV. 827, 841-45 (1996) (describing the rise of the modern presidency and theoretical justifications for centralization of power in the president). The "dominance" of the executive over Congress in respect of intelligence matters should not be over exaggerated. Barrett finds that in the 1950s, Congress, through a select few, had fairly regular contact with the intelligence community since its modern post-War incarnation. BARRETT, *supra* note 73, at 459-61. Although Congress in the 1950s deferred to the Executive branch in the conduct of foreign affairs and national security policy, it was not completely silent. It actually overrode the Eisenhower administration by appropriating more than requested for missile development. *Id.* at 279-80. And, Congress could be just as assertive in foreign affairs, pressing for covert operations. *Id.* at 95-112.

173. *See, e.g.*, ANDREW, *supra* note 34 (discussing the use of intelligence by U.S. presidents). Such executive interest goes back to the time of Washington, who had a keen

intelligence community is primarily responsible to the executive branch and that the executive branch should set the agenda for the intelligence community's activities. Accordingly, the executive branch is seen as playing a major role in overseeing them.[174] Under the executive umbrella, the intelligence community views itself as playing a unique role because it serves the needs of several agencies by providing them with intelligence relevant to policymaking within the appropriate competencies of the various agencies.[175] At its inception, it was intended to be independent of the various departments and uninvolved in policymaking so that it could provide as objective information as possible[176] although, of course, the line between policymaking and intelligence analysis often blurs.[177]

These relationships between the intelligence community, the President and other executive agencies become more complex because Congress also is involved. Congress uses intelligence in three activities: in the exercise of its Constitutional powers, such as control over the budget and the regulation of foreign commerce; in attempts to exert influence in foreign relations, defense and, national security, areas that overlap with executive concerns; and in its oversight over the intelligence community as part of its more general role of ensuring that the executive meets its responsibility of executing the laws.[178] As might

---

appreciation for intelligence and the need to keep them secret. *See, e.g.*, Letter from George Washington to Colonel Elias Dayton (July 26, 1777), *in* 8 THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745-1799, at 478-479 (J. Fitzpatrick ed. 1933), *available at* http://etext.virginia.edu/washington/fitzpatrick/.

174. For a discussion of Executive branch oversight of the intelligence community, see HOLT, *supra* note 4, at 200-07; LOWENTHAL, *supra* note 54, at 191-95.

175. LOWENTHAL, *supra* note 54, at 4.

176. MICHAEL WARNER & J. KENNETH MCDONALD, CENTER FOR THE STUDY OF INTELLIGENCE, U.S. INTELLIGENCE COMMUNITY REFORM STUDIES SINCE 1947, at 4 (2005), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/US%20Intelligence%20Community%20Reform%20Studies%20Since%201947.pdf. Warner and McDonald write that in 1945, the view of many policymakers was that "the President and his key advisers needed a control variable against which to test the intelligence and policy advice coming from the departments. Only a free standing intelligence agency could provide such a perspective." *Id.*

177. *See* SHULSKY & SCHMITT, *supra* note 74, at 133-41 (discussing the close relationship between policy-making and intelligence analysis).

178. Snider, *supra* note 94, at 95.

be expected, the lines between these three activities also blur in practice.[179]

The intelligence community has supported Congress in each of these roles through a series of informal arrangements.[180] A great deal of intelligence is shared with Congress on a regular basis.[181] According to Alfred Cumming, Congress is given access to most forms of finished intelligence, including the National Intelligence Estimates.[182] The CIA

---

179. For example, much of Congress's "oversight" of the CIA in the 1950s took place through the appropriations committees, which of course represent Congress's budgetary power. BARRETT, *supra* note 73, at 19-21.

180. *Id.* at 49-50, n.10. (citing CIA statement that "[i]t is all very well . . . to state that both Congress and the Bureau of the Budget must understand that the Central Intelligence Agency must be given, in effect, a blank check and a free hand. In practice, the Central Intelligence Agency must justify its demands with some reason and logic and must reassure both of those bodies that the Central Intelligence Agency is, at least, somewhat careful with government funds and does its best to guard against waste and fraud").

181. Congressional authority to have access to confidential intelligence stems from its constitutional powers to make the laws and to oversee the executive branch. Snider, *supra* note 94; KATE MARTIN, CENTER FOR NATIONAL SECURITY STUDIES, CONGRESSIONAL ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION 1-2 (2007), *available at* http://www.americanprogress.org/issues/2007/03/pdf/congressional_oversight_report.pdf. Moreover, the President is charged with the duty of making sure that Congress is "kept fully and currently informed of the intelligence activities of the United States." 50 U.S.C. § 413 (2006). The executive branch has argued that it has the exclusive right to the production and management of classified information. Christopher H. Schroeder, Memorandum Opinion for the General Counsel Central Intelligence Agency, 20 Op. Off. Legal Counsel 402, 404 (Nov. 26, 1996) (arguing that the president has "ultimate and unimpeded authority" over national security information). These arguments have arisen when individuals in the intelligence community provide information to Congress without authorization. *Id.* at 405; *see also Disclosure of Classified Information to Congress, Hearings Before the Select Committee on Intelligence of the U.S. Senate,* 105th Cong. (2d Sess. 1998) (containing testimony regarding Congressional access to intelligence information from members of the intelligence community). Members of Congress do not receive security clearances as such. *See* Schroeder, *supra*, at 406. However, each of the House and Senate Select Committees on Intelligence—committees with primary authority for the oversight of the intelligence community—have in place rules for the protection and dissemination of classified information. *See* H.R. Comm. on Rules, Rule X(11) (H.R. Select Comm. on Intelligence rules); Rules of Procedure for the H. Permanent Select Comm. On Intelligence, 110th Cong., Rules 12-14; *see also* S. Res. 400, 94th Cong., 2d Sess. (1976) (as amended by S. Res., 95th Cong., 1st Sess. (1977), S. Res. 445, 108th Cong., 2d Sess. (2004), and S. Res. 50, § 8, 110th Cong., 1st Sess. (2007)) (setting out rules for the Senate Select Committee on Intelligence); Rules of Procedure for the S. Select Comm. on Intelligence, Rule 9 (establishing additional procedures for the treatment of classified information). The committees give security clearances to staff members in consultation with the Director of National Intelligence. Rules of the House of Representatives, R. X(11)(e), 110th Cong., 1st Sess. (2008), *available at* http://www.rules.house.gov/ruleprec/110th.pdf.

182. Memorandum from Alfred Cumming, Specialist in Intelligence and National Security, Foreign Affairs, Defense and Trade Division, to Sen. Dianne Feinstein on Congress

estimates that in 2004 it gave Congress 4000 publications.[183] The intelligence community also briefs various committees of Congress, usually behind closed doors. There were about 1000 such briefings in 2004.[184] Some intelligence, however, is not routinely shared with Congress. This includes the identities of foreign agents; the methods of intelligence gathering and analysis; raw, unanalyzed intelligence; and certain reports specifically tailored for members of the executive branch, such as the President's Daily Brief.[185]

Although much information is provided to Congress, most of it is shared with a relatively small number of members. From the beginning, Congress chose an elite model of oversight, in which a small set of powerful members of Congress would be given access to intelligence.[186] Since the reforms following the Church hearings in the mid-1970s, oversight of the intelligence community takes place through select committees on intelligence in both houses of Congress, whose deliberations are often conducted in closed sessions to which other members of Congress are not given ready access.[187] Of course, the committee structure is not unique to intelligence; it is part of Congress as a whole and is an attempt to capture the efficiencies of specialization even in a representative body. In the area of intelligence, however, the committee structure is also intended to protect classified information. As such, it is an example of Thompson's partial secrecy.[188]

---

as a Consumer of Intelligence Information, at 9 (Dec. 14, 2005), *available at* http://fas.org/sgp/crs/intel/congress.pdf.

183. *Id.* at 9 n.38.

184. *Id.*

185. *Id.* at 5-6.

186. BARRETT, *supra* note 73, at 22.

187. In the case of the House Permanent Select Committee on Intelligence, a representative who is not a member of the committee must go through a multi-stage approval process before he may sit in on a closed or executive session or gain access to classified information, with the possibility such approval will be denied. Rules of Procedure for the H. Permanent Select Comm. on Intelligence, 110th Cong., Rule 14(f); *see also* Frederick M. Kaiser, Protection of Classified Information by Congress: Practices and Proposals, CRS Report RS20748, at 4 (2006), *available at* http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RS20748_01112006.pdf (arguing that the House select committee requirements and procedures for granting non-committee members access to classified information are the most exacting). The Senate Select Committee on Intelligence also imposes similar restrictions on access to classified materials and closed meetings. Rules of Procedure for the S. Select Comm. on Intelligence, Rules 9.5-9.10.

188. *See supra* text accompanying notes 43-47.

Much, therefore, hinges on the ability of a relatively small number of members of Congress to evaluate claims based on intelligence. As Shulsky and Schmitt point out, the committee structure is highly problematic from a democratic perspective: "[T]he notion of congressional oversight conducted secretly contains a self-contradiction: One wants to obtain the benefits of legislative deliberation on intelligence matters, but one rules out from the start the major method of such deliberation—full and open public debate."[189]These problems are exacerbated by institutional dynamics. Amy Zegart argues that the fact the national security agencies are comprised of large bureaucracies, their housing in the executive branch, and the motivations of Congress, weigh against effective Congressional oversight.[190] She points out that national security agencies differ from domestic agencies because for the most part they are not supported by interest groups, which results in less Congressional interest in overseeing these institutions.[191] Secrecy itself makes oversight difficult.[192] Further, the pre-eminence of the executive branch in the formation of foreign and security policy leads to weak oversight.[193] Finally, she acknowledges that there are members of Congress who take an interest in foreign affairs and national security, but in her view, such members are rare and tend to support the president's primacy in foreign affairs.[194]

These kinds of problems are evident in the pre-invasion intelligence assessments debacle. The executive branch has been heavily criticized for its reliance on a National Intelligence Estimate issued in late 2002, which found incorrectly that Iraq was actively engaged in a nuclear weapons program.[195] Based on their examination of publicly available documents, Joseph Cirincione and his co-authors conclude that before 2002, the intelligence community appears to have had a generally accurate picture of the state of Iraqi nuclear and missile programs, but overestimated the development of its biological and chemical warfare

189. SHULSKY AND SCHMITT, *supra* note 74, at 146.

190. AMY B. ZEGART, FLAWED BY DESIGN: THE EVOLUTION OF THE CIA, JCS, AND NSC (1999).

191. *Id.* at 26.

192. *Id.* at 27.

193. *Id.* at 31.

194. ZEGART, *supra* note 190, at 32-33.

195. COMM'N ON THE INTELLIGENCE CAPABILITIES, *supra* note 144, at 45.

programs.[196] They argue the shift in assessments after 2002 is consistent with the argument that the intelligence reports were being influenced by political considerations.[197]

Others have argued that the executive branch manipulated assessments to achieve political ends,[198] but what is interesting for purposes of this discussion is the response of committees charged with overseeing the intelligence community. In an article written in 2005, Bob Graham, the chair of the Senate Select Committee on Intelligence during 9/11 and the lead-up to the Iraq invasion, wrote that the 2002 National Intelligence Estimate was prepared at the request of the Senate, not the executive branch.[199] According to Graham, the classified version of the 2002 NIE was very troubling because the document was full of qualifications, which prompted Graham to ask that a public version be released.[200] However, that version was much more unequivocal in its assertions about the Iraqi programs.[201] Graham's assessment of the reliability of the estimate jibes well with that of Ciricione and his co-authors. Based on their reading of portions of the classified version released to the public in 2003, Cirincione and his co-authors point out there were a number of red flags that should have signaled that the accuracy of the NIE was in question.[202] The October NIE had some forty caveats, atypical for an NIE, which, as discussed earlier, is meant to reflect the collective judgment of the intelligence community.[203] Moreover, agencies within the intelligence community, the State Department Bureau of Intelligence, and Research and the Department of Energy disputed the claim that Iraq had restarted its nuclear program.[204]

Senator Graham shares that doubts about the accuracy of claims made in the report (and his corresponding doubts about the strength of

196. JOSEPH CIRINCIONE, ET. AL., CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, WMD IN IRAQ: EVIDENCE AND IMPLICATIONS 50 (2004), *available at* http://www.carnegieendowment.org/files/Iraq3FullText.pdf.

197. *Id.*

198. *See, e.g.*, MELVIN A. GOODMAN, INTERNATIONAL POLICY REPORT, USES AND MISUSES OF STRATEGIC INTELLIGENCE (Jan. 2004), *available at* http://www.ciponline.org/nationalsecurity/reports/jan04goodman.pdf; Paul L. Pillar, *Intelligence, Policy, and the War in Iraq*, 85 FOREIGN AFFAIRS 15 (2006).

199. Bob Graham, *What I Knew Before the Invasion*, WASH. POST, Nov. 20, 2005, at B07.

200. *Id.*

201. *Id.*

202. CIRINCIONE, *supra* note 196, at 14.

203. *Id.* at 17.

204. *Id.* at 22.

the executive branch's case for the invasion) led him to vote against the resolution authorizing the use of force in Iraq.[205] He writes, "I was able to apply caveat emptor. Most of my colleagues could not."[206] The issue is what Senator Graham means by "my colleagues" and "could not." Is he referring to his colleagues on the Select Committee? At least in theory, the members of the select committees are supposed to have the expertise needed to oversee intelligence matters. One would have expected those members to detect the same qualifications in the classified NIE Senator Graham spotted, as well as the inconsistency in tone between the classified and public versions of the NIE.[207] Or is he referring to his colleagues in the Senate as a whole? Here again secrecy rears its ugly head. "While Graham . . . could complain that the administration's and [the director of the CIA's] own statements contradicted the classified reports they had read, they could not say what was actually in those reports." [208] Either answer reveals significant weaknesses in the current system of oversight. Given what I have discussed in Part III about the nature of NIE assessments,[209] it is alarming that regular members of Congress were not given access to the classified version.

As it stands, the committee structure exacerbates a situation in which the executive branch enjoys an informational advantage vis-à-vis Congress as a whole, with all of the inefficiencies created by information asymmetries discussed earlier. There will be other times when the executive branch will urge a policy based on classified information to which the legislative branch as a whole does not have access, or which is not capable of independent verification.[210] When such an informational asymmetry exists, unless Congress trusts the executive branch as it urges a particular policy decision, one would expect Congress to discount justifications for the policy based on secrets and use the best public information available to reach its decision.

---

205. Graham, *supra* note 199.

206. *Id.*

207. Ultimately, five members of the Senate Intelligence Committee, including Graham, voted against the resolution. *See* John B. Judis & Spencer Ackerman, *The Selling of the Iraq War: The First Casualty*, NEW REPUBLIC, June 30, 2003, at 14.

208. *Id.*

209. *See supra* text accompanying notes 77-96.

210. This may occur despite the fact that legislation requires the President to report to Congress certain national security activities. For a discussion of such laws, see Cumming, *supra* note 59.

Such a discount could lead to inefficiencies because sometimes Congress will decide something based on a presumption that an assertion is not true when in fact it is, but just as often a discount would prevent the opposite result. Further, the "threat" of a discount could have at least two more effects. As an initial matter, it gives voters a metric with which to hold their representative accountable. If, in the face of an information asymmetry, a representative does not apply a discount, the question is "why not?" As I have just discussed, a representative might be satisfied with meaningful assertions of the executive branch, which serve as a proxy for the classified information to which she is being denied access. But if not, the failure to apply a discount would call into question a representative's judgment.[211] In addition, the prospect of such discounts might also encourage the executive branch to perform a balancing test. It will have to weigh whether it is more important for national security to persuade the legislative branch to act (which entails providing verifiable information that could risk the disclosure of sources and methods) against protecting those sources and methods by not sharing such information (thereby taking the risk the legislature will not act because the executive's assertions will be discounted).

Here, however, is another place where the elusive nature of democratic concepts comes into play. Richard Posner argues that one reason the executive branch should take the lead in national security matters is because the legislature is rarely accountable for such decisions.[212] It is hard to trace a national security outcome to any one legislator. In Posner's view the power to act should rest with the person who can be held responsible, i.e., the president.[213] It may be, however, that no one is accountable. In a study of the impact of memory on political preferences, Mark Joslyn argues the fact that people cannot remember their prior political positions results in support for the status

211. The committee system complicates this situation. Suppose a representative who is not a member of a select committee is being told by a government official that the state of the world is X, but will not provide verifying information. The rational representative would discount the official's statement. But suppose further that the representative is being told by his colleague, who is a member of a select committee, that the state of the world is X, but the committee will not provide verifying information. *See supra* note 187. The representative would presumably discount this statement as well, but then, who is the representative to believe? Further, given what we know about the nature of intelligence assessments, one can ask those on the standing committees whether they, at a minimum, assessed the level of confidence the intelligence community has in assertions being made in favor of a particular policy.

212. *See* POSNER, *supra* note 53, at 174-75.

213. *Id.*

quo.[214] In a survey taken prior to the first Gulf War, most respondents stated that they favored peaceful means to resolving the conflict in the Gulf. After the invasion, most of those respondents incorrectly remembered they had favored military action before the war.[215] Joslyn thus concludes that memories of policy preferences are subject to decay, and over time, such memories are reconstructed, not recalled.[216] These reconstructions are impacted by perceived current public opinion, even if this leads to an inaccurate recollection of one's prior position.[217] As a result, a person who fails to recall the sharp differences between his personal policy preferences and those the government actually adopted is likely to support the status quo by voting for the incumbent.[218] Although it has been argued that the 2006 election was a referendum on Iraq, when it comes to national security, there might be a lack of accountability with respect to either branch. If citizens are uninterested in these kinds of matters, or public opinion is so easily manipulated, then secrecy concerns fade from view.[219]

## V. CONCLUSION

The argument for secrecy to protect sources and methods reflects an inner logic that continues to play itself out more than sixty-five years after Pearl Harbor, and particularly after 9/11. That this society is a democracy means we can flag instances when the interplay between that inner logic and our collective and individual lives raises concerns about coercion or interference with democratic processes. However, whether we locate the core of democracy in widely held values or in our methods

214. Mark R. Joslyn, *The Determinants and Consequences of Recall Error about Gulf War Preferences*, 47 AM. J. POL. SCI. 440 (2003).

215. *Id.* at 441.

216. *Id.*

217. *Id.* at 442.

218. Joslyn *supra* note 214, at 442. In Joslyn's view, exposure to such public opinion comes largely through the media. *Id.* at 443. "Significant exposure to the news media, greater trust in government, and low education signaled individuals so ripe for manipulation that their memories could be replaced by recollections more consonant with government's position." *Id.* at 445. Joslyn then shows that postwar misrecall of Gulf War preferences was a predictor of voting for the incumbent president. *Id.* at 447.

219. James Druckman argues, for example, that citizens delegate to credible elites the task of choosing among possible frames through which policy decisions can be viewed. At the same time, consistency with those frames serves as a kind of check on elites. *See* Druckman, *supra* note 138.

for achieving consensus, democratic concepts do not always tell us when the logic of secrecy should be replaced with other equally valid logics.

At the same time, when the sources and methods argument is evaluated in light of the sources and methods themselves, the kinds of intelligence it is designed to cultivate, the role such intelligence plays in decision-making, and the dynamics secrecy sets into motion, the argument's underlying logic becomes less inexorable and the argument itself untenable. This means it is entirely appropriate to subject the argument for secrecy to very high scrutiny when our representatives consider decisions of national moment, or when the judiciary is being asked to determine whether government is obeying the law. At the very least, we know some of the questions that must be asked of proponents of secrecy, and we can hold persons accountable for failing to ask those questions. But in the end, whether the secrecy argument will carry the day depends on whether citizens wish to enter the debate in the first place.

.