Reconciling the public interest in keeping national security information secret and the public interest in an informed citizenry with access to government information.

by Kate Martin

“A popular Government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy, or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.” James Madison Letter to W.T. Barry (1822-08-04).

Introduction: No questions are more important to ensuring democratic government and fundamental human rights than those involving decisions about war and peace and protection of a country’s national security. Inherent in this truism, however, is a fundamental tension in the construction and maintenance of democratic government: democracy and respect for fundamental human rights depend upon public access to government information, while protection of the national security requires some secrecy. The conduct of diplomacy, the maintenance of peaceful relations between states, military activities and intelligence activities all require some measure of secrecy in order to be effective.

Legal regimes allowing the classification and withholding of national security information from public disclosure must recognize these two competing truths, and every democratic government is faced with hard questions about how to do so. There will always be debates about what information should be made public and what information needs to be kept secret at any particular moment in order to protect the security interests of a country. Every administration, including those elected on a liberal platform of commitment to democracy, transparency and accountability, has the tendency to want to hold information close when in power. And there is a long history of abuse by governments claiming that information must be kept secret on national security grounds when the real reason is that they fear the information will be harmful to their political fortunes. At the same time, a government’s political opponents will seek disclosure of information not just to inform public debate and influence public policies, but also to challenge the government and win the next election.

From a larger perspective, the commitment to democratic self-government always requires the acknowledgment that there will be competing views of what is in the public interest and many times, competing public interests. In deciding what

information needs to be kept secret to protect national security interests and what
information should be made public, there are three questions to address to ensure that
the answer to that question is consistent with both democratic self-government and
national security interests.

The first requirement is to determine what categories of information
should properly be considered as information concerning the national security and
therefore eligible for classification. Steven Aftergood’s paper discusses this question
in more detail, but a couple of comments may be useful here. The traditional
understanding of national security encompassed those activities identified in the first
paragraph of this paper, i.e., the conduct of diplomacy, the maintenance of peaceful
relations between states, military activities and intelligence activities. Traditionally
there was also a general understanding that law enforcement activities require secrecy
for some period of time, but national security classification rules were not the way to
protect such information. With the increased focus on domestic counterterrorism
activities, the line between law enforcement and national security activities has
become more blurred. There is also now a legitimate and difficult debate about
extending the traditional understanding of national security to a wider sphere, to
include economic or trade information for example, because economic interests have
become integral to the national security interests of states. There is no doubt that
economic and other matters do have an important impact on the national security
interests of states in this globalized world. But the fact that information relates to
national security interests should not by itself be sufficient to deem it eligible for
classification and withholding from the public. On the contrary, for these new
categories of information, the case needs to be made as to why secrecy is essential to
the success of the enterprise involving the particular information, just as the case has
been made that secrecy is necessary for the categories of information traditionally
recognized as eligible for classification. Secrecy, for example, is essential to the
success of military operations or the recruitment of a foreign intelligence source. The
case for extending classification to new categories of information must also address
the phenomenon, identified by intelligence officials, that secrecy is much rarer in an
increasingly electronic and networked world.

The second requirement is to determine the harm that is likely to result
from disclosure of the information and from keeping the information secret. One test
that is sometimes proposed for resolving whether information related to national
security should be public is whether the public interest in disclosure of that
information outweighs the harm to national security interests that is likely to follow
from disclosure. But this test incorrectly posits a distinction between “public

---

2 See e.g., President Obama’s National Security Strategy, 2010, Page 2. Available at:
3 Spaulding, Suzanne, “No More Secrets: Then What?,” The Huffington Post,
June 24, 2010. Available at: http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-
what_b_623997.html.
4 The Executive Order on Classification in the United States provides: “In some exceptional cases,
however, the need to protect [classified] information may be outweighed by the public interest in disclosure
of the information, and in these cases the information should be declassified.” Executive Order 13292, Sec.
interests” and “national security interests,” when in fact protecting the national security is a critical public interest. What is required instead is a thorough articulation of the varied specific public interests and then a weighing of whether each interest is advanced by either disclosure or secrecy. While that analysis changes with time and may depend on the circumstances at the time and the specific information involved, it can be performed as to categories of information. Thus, the task is to identify categories of information that may be reasonably treated as presumptively secret for some period of time and those categories that should be treated as presumptively open. The effect of applying such a presumption to a particular category would be to require a higher showing of specific facts and circumstances relating to the information at issue to overcome the presumption of either secrecy or disclosure.

The categories of information that should be presumptively secret are outlined in more detail in Steven Aftergood’s paper. They include for example, the names of secret intelligence sources, diplomatic exchanges, secret military technologies and secret intelligence methods—all of which are secret and whose efficacy would be undermined by public disclosure.

The current controversy generated by the release by Wikileaks of thousands of diplomatic cables containing frank exchanges between US diplomats overseas and their colleagues at the State Department in the US offers a case study in the complexity of determining the benefits and harms from both secrecy and disclosure. While such study is beyond the scope of this paper and probably cannot yet be fully assessed, a few comments may be helpful. There is no doubt but that release of the cables has made it more difficult for overseas diplomats to communicate their frank views back home; the resignation of the U.S. ambassador to Mexico is a clear example of disclosure harming the conduct of US foreign relations. And disclosure of the names of individuals living under authoritarian regimes, who met with US personnel on the understanding that such meetings would be kept confidential in order not to prejudice or endanger them is also clearly harmful. On the other hand, Defense Secretary Gates himself acknowledged that foreign governments are well aware that US diplomats do not necessarily share their frank assessments or blunt views with those governments. Such acknowledgment of course is only a statement about the amount of harm from disclosure, it does not outline any public interest flowing from the disclosure. The public interest is harder to see, other than the general interest in knowing what the government is up to. That is harder here, where disclosure seems likely to make the government’s tasks harder. While some have argued that the frank assessments contained in the cables fueled the popular uprisings in the Middle East, such a claim is extremely difficult to verify. It is of course, well known, that diplomats are likely to be more diplomatic in their public statements, than in frank assessments sent back home to the State Department.

3.1(b). As Meredith Fuchs points out, this provision was used to authorize disclosure of an August 6 Presidential Daily Brief item entitled “Bin Laden Determined to Strike in US,” see Report of the National Commission on Terrorist Attacks Against the United States.

5 News reports March 20, 2011.
And many of the particular assessments were also already known. Thus, in the case of disclosure of current cables – as opposed to disclosure of historical cables – the public interest would need to be measured based on the specifics of any new information actually contained in the cables.

This paper will outline categories of information that should be presumptively open. A presumption of openness has been applied, for example regarding the general laws and rules governing military, intelligence or diplomatic activities, even while the activities themselves are frequently secret. Some countries have also adopted a presumption of openness regarding information concerning grave violations of human rights as detailed in the paper by Kate Doyle and Emilene Martinez.

The third requirement is the establishment of rules, and then of processes, institutions and bureaucratic cultures to apply and implement the rules. In writing such rules it is important to keep in mind the principle of indeterminacy and the danger of chilling protected speech and access to information. The former is necessary because rules must of necessity be general and forward looking, when in fact, it is not possible to know in advance the effect of public disclosure of specific information at a specific historical moment. The latter is required, because given the necessary generality of a rule, there must be sufficient flexibility to ensure that disclosures that should be made will not be chilled because the consequences would be too dire to risk. So for example, criminalizing the publication of national security information, which turns out not to be in the public interest is likely to chill the publication of much information that the public needs to know in a democracy. Another key ingredient is the cultivation of an understanding in the executive branch of government that part of its mission is to ensure an informed public and to implement the presumption that government information should be made public, except in a minority of narrowly defined circumstances where secrecy is necessary to prevent some greater harm than the benefit that would result from disclosure.

A couple of general notes. The calculus in balancing the public interests in secrecy and disclosure changes with the passage of time. The calculus is also quite different, when a country is actually at war with its military engaged in hostilities or facing the possibility of imminent war, than when it is at peace. In addition, government information frequently includes information about private individuals, both citizens and foreigners. Whether private individuals’ interests in disclosure or non-disclosure should be weighed in the balancing is frequently addressed by data protection or privacy laws, outside the scope of this paper. However, it is important to note that in most instances where the laws recognize that an individual’s privacy interest may require information to be kept secret, such protection usually extends only to citizens and legal residents of the country and not to foreigners.6

6 See Privacy Act of 1974 which only applies to U.S. citizens and lawful permanent residents. However, the Freedom of Information Act in the U.S. does recognize some privacy interests in non-citizens. See exemption 6 and Supreme Court case re return of Haitians.
Categories of information that should be presumptively open.

In determining the necessary and legitimate scope of government secrecy, it is possible to identify certain categories of information concerning foreign relations, defense or intelligence that are essential for a democratic citizenry to know in order to maintain the democratic character of government and which, also have little, if any likelihood of harming substantial and specific national security interests and objectives when disclosed. These include the following categories of information that should be presumptively open:

- The existence of any particular military, police, security or intelligence agency;
- The laws and rules applicable to intelligence agencies, military forces, police and security agencies, establishing the missions, authorities and limits on authorities of such agencies;
- The gross overall budget for each intelligence agency, military service, police and security agency and as much information about the specific uses of public funds by each such agency as may be disclosed without compromising the operational security of such agencies;
- The names of the officials who head military services, police, and security agencies and secret intelligence agencies; and
- The internal oversight mechanisms for secret intelligence and security agencies, including the names and contact information of individuals with such oversight responsibilities. (Where disclosure of the names poses a substantial risk of bodily harm to such officials, other methods of contacting such individuals should be made available.)

Public knowledge of the structures and powers of government is essential to democratic oversight and accountability of government activities. The fact that police, intelligence and military agencies must operate with some degree of secrecy makes oversight and accountability harder and thus it is even more important that the public be informed about the existence and authorities of such agencies. The budgets for such agencies are important in evaluating whether the proper balance of public funding is being achieved, as well as knowing the potential scope of such secret activities and their cost-effectiveness. At the same time, disclosure of such information is unlikely to impede

---

7 See Security Services in a Constitutional Democracy: Principles for Oversight and Accountability: “Each secret agency shall be established by statute, which should specify the limits of the agency’s powers, its methods of operation and the means by which it will be held accountable. “The fact of existence of every security agency shall be publicly disclosed and the head of each agency shall be publicly identified.”
the operational effectiveness of the agencies by, for example, disclosing useful information to potential enemies because the information is too general to signal more about potential operations than is already likely known as a matter of public record. Similarly, the essence of accountability requires that an individual with overall responsibility for an agency be publicly identified. On the other hand, the identities of individual employees of some agencies, especially intelligence agencies, may be presumed to be properly classified when disclosure would impair their ability to do their jobs and is not essential to providing accountability. (This is a case where depending on the circumstances, that presumption of secrecy may be overridden and an individual employee’s identity disclosed in order to provide accountability for wrong-doing by that person.)

- Judicial opinions.

  The legitimacy of law depends upon it being public and not secret. Not only is secret law an oxymoron, but public understanding and confidence in democratic government depends upon the courts delivering public decisions and opinions. Where cases involve specific information that is properly classified, there should be procedures to limit the necessity for relying on such information in judicial opinions. Those procedures should incorporate the following principles:

  - Where an individual faces criminal charges, information relevant to the defense of that individual should be made publicly available; and

  - Trial evidence offered by the government to prove criminal charges against an individual should be public.

  Additional categories of information, which should be presumptively open, even when national security interests are implicated include:

  - The names and charges against individuals being held in jail; and

  - The location of jails and detention centers.

  Knowing who has been arrested by the government and on what grounds is essential to democratic government. It is also essential to prevent the violation of the fundamental right to be free of secret and arbitrary detention. Any claim that disclosure of such information in a particular case will be harmful to national security should be closely scrutinized with regard to the specificity of the claimed harm, the likelihood and substantiability of the claimed harm and the availability of alternative measure to avoid the harm. For example, governments have claimed that they need to hold individual conspirators in secret in order not to alert fellow-conspirators and allow them to escape before also being arrested. The validity of such claims would turn in part on how long the individual has been held and whether his absence is likely to have been noticed by his fellow conspirators simply due to the passage of time.

---

The laws and practices of government surveillance of its own citizens.

Disclosure of such information is essential to preserving the balance of power between the government and the governed in a democracy. Disclosure is necessary to prevent the government from using its powers of surveillance to chill dissent and punish political opponents instead of using surveillance for the legitimate government work of preventing crime or protecting national security interests. Such disclosures can be made without rendering government surveillance ineffective or leaving the country defenseless against a likely threat.

- Information concerning constitutional violations by the government or government officials.

- Information concerning abuses of power by the government or government officials.

- Information being withheld for the purpose of concealing government wrongdoing.

- Information concerning grave human rights abuses by the government which possesses the information, such as torture, war crimes and crimes against humanity. As stated, this principle is extremely broad and is likely to include specific information, for example about ongoing secret, but lawful, intelligence sources and methods, whose disclosure would prove harmful. Perhaps a more specific formulation would cover Information concerning grave human rights abuses, which needs to be disclosed to give a full public picture of such abuses or to provide necessary evidence needed to establish abuses?

- Information concerning grave human rights abuses by other governments, such as torture, war crimes and crimes against humanity. [Same question]

- Information needed to establish in a court of law or an official commission:
  - Criminal acts -- by government officials;
  - Human rights abuses by current or former government officials; or
  - Grave human rights abuses.

These situations pose especially difficult questions about disclosure versus secrecy when they arise in the context of an ongoing war, armed conflict or insurgency. Governments have a great incentive to claim national security harm in order to avoid accountability for abuses, but at the same time, there may be particular situations where disclosure would be more harmful to national security interests than it would be enlightening about abuses. A recent example where it made sense to override the presumption of disclosure concerning such information was the second batch of photographs of abuses at the then U.S. run prison in Abu Ghraib, Iraq, requested from the U.S. Defense Department. Military generals commanding troops still engaged in
hostilities, concluded that release of the photos would directly incite additional violence against U.S. troops. At the same time, it was unlikely that release of the photos would add anything significant to public knowledge about the abuses, given the public release of other photos and other information, and no specific case was made that release of the additional photos was important to pursuit of accountability for the abuses.

- The fact that a nation possesses nuclear weapons and a description of the extent of those weapons.
- The location of armed nuclear weapons.

*Whether this information should be presumptively public, especially the second, is controversial.*

- The deployment of armed forces or others authorized to engage in hostilities.
- Treaties or other international agreements obligating the country to use military force in defense of other countries.
- Government waivers resulting in decisions not to comply with international obligations in the interest of national security.

*These represent fundamental decisions on war and peace, which should be decided in a democratic process, which by definition requires full public knowledge.*

*Some notes about possible tests for determining whether disclosure is more or less likely to serve the public interest.*

The usual tests articulated by Executive branches of government for keeping information secret either don’t recognize the necessity of considering competing public interests advanced by both disclosure and secrecy or simply call for the weighing of the two. See for example, the U.S. Executive Orders on classification. It may be difficult to articulate a more specific test which can be generally applied, but there have been some efforts which bear looking at. In the United States, Supreme Court Justices (but not the Court itself) have articulated two possible tests in addressing when the government may enlist the courts to order non-disclosure of specific information. They wrote that disclosure must be allowed except where:

“publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea . . . “

Justice Brennan at 726-27:

or

---

“disclosure . . . will result in direct, immediate, and irreparable damage to our nation or its people.” Justice Stewart at 730.

Both Justices were writing in the Pentagon Papers case, where the Court refused the government’s request to stop the publication of a Defense Department study of the Vietnam War while the war was ongoing. *New York Times vs. US*, 403 U.S. 713 (1971).

There are other specific questions that should be asked when weighing the public benefit of disclosure versus secrecy, including:

- How does the existence of war or internal conflict affect this calculus? Is it different during peacetime? Given the current terrorist threats, a more nuanced consideration of war versus peace is probably needed than was the case in the 1940’s for example.

- How does the existence of other publicly reported information, even when not officially confirmed, impact the likelihood and scope of any possible harm from disclosure. Does it matter how widely the information has been reported, does the named source of the information or whether its reliability has been challenged matter?

**What structural protections are necessary to protect the right of access to information and guard against excessive secrecy?**

A Freedom of Information law requiring the government to release information will never be adequate by itself, in part because laws must by their nature be written in generalities, laws are always imperfect, and they exist and are applied in a broader public and political context. Thus, additional structural protections are required to protect the right of access and insure that proper consideration is given to the public interest in disclosure as well as the potential harm therefrom.

Some of these additional structural protections could include the following:

- A practice and understanding that certain kinds of national security information will be made public even if not required by a Freedom of Information law, (there are many examples in the U.S.);

- An institutional commitment to public access outside the executive branch, e.g., in the legislature and the judiciary; and

- Protections for freedom of speech by public officials and freedom of the press which allow for a genuine tug of war as to public disclosure. Sanctions for unauthorized disclosure must not be so severe as to chill the disclosure or reporting of information whose disclosure is in the public interest.

April 2011