(draft May 2011)

What Should Be Classified? Some Guiding Principles

By Steven Aftergood

Every nation, including the most open societies, restricts the public disclosure of information that is deemed to pose a threat to national security. But the actual limits imposed by a system of national security classification are frequently a subject of dispute and frustration. News organizations and public advocacy groups typically favor increased disclosure of national security-related information, while government agencies tend to resist pressure to release more. Is there any way to resolve or mitigate this familiar tension?

There does not seem to be a simple "right" answer about what and how much to classify, particularly since the parties in dispute begin with different criteria and assign different weights to values of security and disclosure. It seems that it would not be possible, say, to program a computer to consistently provide a satisfactory answer to the question whether a particular item of information should be classified or not. There are too many subjective elements involved in the process.

But if there is no universally acceptable right answer to the question of what exactly to classify, it may still be possible to identify wrong answers – i.e. classification practices that most people will agree are erroneous, unnecessary or counterproductive – and to circumscribe the area of continuing disagreement.

This paper attempts to sketch out features of a national security classification system that could be endorsed both by officials and members of the public, by proponents and critics of current classification policies. The first part of the paper proposes some "axioms" that characterize classification policy, at least in the author's view. The second part suggests some practical guidelines that may be inferred from those axioms.

Part I: Some Axioms on Classification Policy

Based on prior experience, several basic elements or aspects of national security classification policy may be identified that can serve to inform and guide classification reform efforts.

1. National security secrecy can serve the public interest.

Not even the most ardent advocates of open government dispute that some secrecy is legitimate and appropriate. "Of course there [are] circumstances, such as diplomatic negotiations, certain intelligence sources and methods, or various time-sensitive military operational secrets, that

warranted strict secrecy," wrote Daniel Ellsberg,[1] who actually withheld four volumes (out of 47) concerning confidential diplomatic negotiations from his historic disclosure of the Pentagon Papers.

2. The application of secrecy depends on subjective judgments.

In the United States, information may be classified only if its disclosure "could reasonably be expected to cause… damage to the national security." But what exactly constitutes "national security"? What is "damage"? What likelihood is needed to warrant a "reasonable expectation"? These terms cannot be defined with sufficient precision to permit them to be applied unambiguously in every case. Instead, government officials are authorized and obligated to use their best judgment about what national security requires. In many cases, other officials and outside observers will reach different conclusions.

3. Independent oversight can compensate for subjectivity in secrecy and help to correct it.

Because of the subjective character of secrecy judgments, it is wise and useful to provide opportunities for independent confirmation – or rejection – of decisions to apply secrecy. If an independent reviewer – even a reviewer from within the government but with a different set of bureaucratic interests -- finds reason to affirm a decision to classify, then the credibility of the decision will be enhanced. If the reviewer finds no such reason, the decision to classify is likely to be unjustified.

This basic principle of independent oversight has been successfully employed in a U.S. government body called the Interagency Security Classification Appeals Panel, which is composed of representatives of six government agencies (Defense, State, Justice, NSC, NARA, ODNI). [2] Among the Panel's functions are to review requests from the public to declassify records that one of the member agencies has previously refused to release. Remarkably, the Panel has ordered the declassification and disclosure of information, at least in part, in the majority of cases that it has considered. In other words, through collective independent oversight, it has overruled the classification judgment of its own member agencies more often than not.

4. Official secrecy tends to expand in scope.

Once established, a system of national security classification does not remain statically in place, but rather it tends to grow in size, scope and complexity. In large part, this is a predictable expression of the nature of bureaucracy, as famously identified by Max Weber: "Every bureaucracy seeks to increase

[1] "Secrets: A Memoir of Vietnam and the Pentagon Papers," by Daniel Ellsberg, Viking Penguin, 2002, at p. 205.
[2] Interagency Security Classification Appeals Panel, official web site: http://www.archives.gov/isoo/oversight-groups/iscap/index.html

the superiority of the professionally informed by keeping their knowledge and intentions secret."[3] There is no comparable bureaucratic imperative to reduce secrecy and promote public disclosure. And so the net result is a continuing growth in secrecy.

5. Official secrecy is susceptible to abuse.

Secrecy makes it possible to circumvent legal, political and moral restrictions on official conduct, and the results are frequently terrible. Even with the best of intentions, government officials may secretly embark on unlawful surveillance, prisoner abuse, unethical human experimentation, and even secret wars. There is ample evidence in the historical record that secrecy can disable external and internal checks on official misconduct.

6. Unnecessary classification should be avoided.

Classification of information should be minimized for several reasons. To begin with, every decision to classify incurs direct and indirect financial costs associated with the protection of such information, including physical security, computer security, personnel security (clearances), and so on. In 2009, the total amount of classification-related costs in the U.S. exceeded a staggering $9.9 billion. [4]

Classification can impose operational penalties by impeding the flow of information to users in government. It obstructs oversight and it deprives the public of information.

Finally, excessive classification dilutes and diminishes the value of classification for legitimate national security functions. "For when everything is classified," in the words of Justice Potter Stewart, "then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion."[5]

For all of these reasons, classification should only be applied where necessary, and nowhere else.

7. Disclosure, not secrecy, may best serve national security in some circumstances.

It would be a mistake to categorically equate secrecy with security. In many cases, disclosure will do more to promote national security than secrecy can. If the American public had been better informed about the threat of terrorism, the 9/11 Commission concluded, the nation would have been

---

[3] Max Weber, *Bureaucracy*, in Essays in Sociology, H.H. Gerth and C. Wright Mills eds. & trans., Oxford Univ. Press, 1946, at pp. 233-34.

[4] Information Security Oversight Office, "2009 Cost Report," available at: http://www.archives.gov/isoo/reports/2009-cost-report.pdf .

[5] New York Times v. United States, Justice Stewart concurring, June 30, 1971, available at: http://www.law.cornell.edu/supct/html/historics/USSC_CR_0403_0713_ZC3.html

better equipped to confront that threat.[6] Public sharing of threat information can help to instill public alertness. Disclosure of vulnerabilities can mobilize public support for corrective measures. Where secrecy sedates public awareness, disclosure can empower the public.

Part II: Principles for Classification

The landscape of secrecy policy sketched above is inherently ambiguous, with competing imperatives for secrecy and disclosure that cannot easily be reduced to a set of classification rules that are clearly applicable in every case. But some instructive inferences may still be drawn.

1. Classified national security information should be protected separately from other types of sensitive information.

There are many kinds of records that are not intended for broad public dissemination, such as tax returns, confidential business information, export controlled data, etc. Some records are withheld because their disclosure would compromise personal privacy. Others would infringe upon intellectual property, or other forms of confidentiality. But national security information is qualitatively different from all of these other categories for several reasons: because its unauthorized disclosure could pose a threat to national security, because of its importance for government oversight and accountability, and because there may be a compelling public interest in its declassification and disclosure.

So, for example, the precise formula for Coca Cola is a tightly held secret that is considered extremely valuable by its owners and protected as such. But it does not belong in the same category as a national security secret. If the "secret" of Coca Cola were ever compromised, the safety and security of millions of people would not be at risk. Its contents are not an integral part of the national security decisionmaking process. It is unlikely that it would ever need to be shared with Congress in the normal course of oversight. And there is no reason why the public should expect or require its eventual "declassification." In short, the practices and procedures that have been developed to regulate the protection, use and ultimate release of national security information are not normally relevant to other types of secrets.

Therefore, in order to preserve the clarity and integrity of the national security classification system, classified records and classification procedures should be maintained separately from other information control regimes.

[6] The 9/11 Commission Report, p. 341.

2. "National security classification" should be applied narrowly only to records pertaining to defense against threats to the nation.

The security of a nation might be said to depend on many factors, from economic vitality to low levels of crime to childhood nutrition. In some diffuse sense, almost every matter of public policy may arguably pertain to a nation's security and well-being. But most of those matters should be excluded from the possibility of national security classification in order to keep the classification system focused on its primary mission and to keep it manageable in size.

In the words of a 1956 U.S. Supreme Court ruling, national security is "intended to comprehend only those activities of the Government that are directly concerned with the protection of the Nation from internal subversion or foreign aggression and not those which contribute to the strength of the Nation only through their impact on the general welfare."[7] It follows that national security classification should be similarly limited.

In practice, U.S. classification policy has overflowed such limits, and national security is now defined in an executive order to include not only "the national defense" but also "foreign relations of the United States" and it may even extend to broad categories such as "foreign government information."[8] Nevertheless, the principle of strictly defining national security is important to the proper application of classification.

Under current U.S. policy, information must fall into one of the following categories in order to even be eligible for classification:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) the development, production, or use of weapons of mass destruction.

---

[7] *Cole v. Young* , 351 U.S. 536, 544 (1956); cited by Arvin S. Quist, "Security Classification of Information," Volume 2, 1993, at p. 30.

[8] Executive Order 13526, "Classified National Security Information," December 29, 2009.

Information in these categories may be classified if its disclosure "could reasonably be expected to cause identifiable or describable damage to the national security."[9]

3. There should be an identifiable reason for each classification decision.

Whenever a decision is made to classify a certain category of information, the classifier should be expected to articulate the justification for classification.

"There should be a definite, identifiable reason or rationale for classifying information or materials," according to a 1993 study of classification policy performed for the U.S. Department of Energy.[10] "If a reason is definite, then it should be expressible. If a reason cannot be expressed or can only be given in vague terms, then the information or material probably should not be classified."

"If specific reasons for classification actions are required, then the classifier will be required to be well informed on what he or she is doing and to carefully think through the classification decision; this will lead to a better classification decision. When a reason that can be examined by others is provided, erroneous reasons (bad classification decisions) are more easily identified. Indicating why specific information is classified enables others to better understand the rationale behind the classification decision."

Current U.S. classification policy requires that classifiers be "able to identify or describe the damage" resulting from unauthorized disclosure, but does not require that they actually do so in fact.[11] Instead, classifiers are asked to choose from a menu of pre-approved justifications for classification and to include a marking on the classified record citing this generic justification.

4. Classification can be justified only by the prospect of real damage to national security.

It must take more than official embarrassment, bad publicity or a loss of international prestige in order to justify national security classification. Classification should be exclusively limited to cases in which real and significant damage to the national security is at stake.

A 1972 executive order on classification gave some concrete examples of the "exceptionally grave damage" that a Top Secret classification could properly be used to prevent. These included: "armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital defense plans or complex cryptologic and communication intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security."

[9] Executive Order 13526, section 1.4.
[10] Arvin S. Quist, "Security Classification of Information," Volume 2, 1993, at p. 15.
[11] Executive Order 13526, Section 1.1.(a)(4).

Even so, the order stated, "This [Top Secret] classification shall be used with the utmost restraint."[12]

4. Information that is in the public domain should not be classified.

Another important limitation on the application of classification is that information that is already in the public domain should not be subject to classification.

It is a perhaps regrettable fact that there is a large body of public information that could contribute to a threat to national security, including design information on weapons of mass destruction, precise locations of sensitive facilities, and so forth. With the passage of time and the emergence of new public tools such as GoogleEarth, previously classified or otherwise restricted information continues to enter the public domain.

But it would not only be futile to attempt to classify such information, it would also tend to compromise the integrity and credibility of the classification system.

5. Information that serves an overriding public need should not be classified.

Sometimes information that meets the criteria for proper classification should nevertheless be publicly disclosed in order to serve a compelling public interest. Such information might include evidence of criminal activity by government officials, matters pertaining to an immediate public safety hazard, and so forth. The case of a public interest override of classification is discussed in a companion paper by Kate Martin.

6. The duration of classification should be set at a minimum.

In order to ensure that the classification system does not expand beyond control and that it is nimble and affordable, classified information should be removed from the system (i.e. declassified) at approximately the same rate at which new information is introduced into the system (classified). This rough equilibrium can best be achieved by setting an automatic declassification date when the information is first classified. Thus, the current U.S. executive order on classification states:[13]

> "At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. […]"
>
> "If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the

[12] Executive Order 11652, "Classification and Declassification of National Security Information and Material," March 8, 1972.
[13] Executive Order 13526, Section 1.5, "Duration of Classification"

sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision."

"An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed."

But in any event, the order states, "No information may remain classified indefinitely." In other words, the classification system must have temporal boundaries as well as limitations on subject matter.

7. Mechanisms to correct classification errors should be built into the system.

Because of the unavoidable subjective elements involved in making classification judgments, along with the tendencies to expand and abuse classification authority, there are sure to be erroneous or unnecessary classification decisions made with some frequency. So there should also be mechanisms built into the system by which such errors can be easily identified and corrected. Such error-correction mechanisms can take many forms, including these:

Systemic oversight: In the U.S. the Director of the Information Security Oversight Office is responsible for monitoring the conduct of the classification and declassification program across the government, and ensuring that government agencies comply with the provisions of the executive order. The ISOO Director has the authority to require the declassification of any information that he determines is classified in violation of the order.

Individual agency oversight: Classification practices within an individual agency can be periodically reviewed by the agency's inspector general, by the Government Accountability Office, or by a congressional committee with relevant jurisdiction.

Classification challenges: The executive order on classification states that government employees (or contractors) who have authorized access to classified information that they believe is improperly classified "are encouraged and expected to challenge" its classification status.

Freedom of Information Act requests: FOIA requests for classified records can prompt a review of their classification, since by law such records can only be withheld from disclosure if they are "properly classified." Decisions to deny access to classified records under FOIA can be challenged in court, though such challenges are only occasionally successful.

Mandatory declassification review requests: MDR requests are another way for members of the public to challenge the classification of a particular record. When faced with the denial of an MDR request, a requester can turn to a government body called the Interagency Security Classification Appeals Panel (ISCAP). What is most remarkable about this process, as mentioned above, is that the ISCAP has ordered the declassification and disclosure, in whole or in part, of the majority of appeals that it has decided upon since 1996.

Fundamental review: The availability of the mechanisms noted above has not been sufficient to prevent overclassification in the U.S. government. So the latest executive order has introduced a new requirement for what it calls a Fundamental Classification Guidance Review.[14] Each classifying agency is required to perform a top-to-bottom review of all of its current classification guidance in order "to identify classified information that no longer requires protection and can be declassified." To ensure a meaningful process, these Reviews are supposed to involve the "broadest possible range of perspectives." The Reviews must be performed periodically and the results must be reported in an unclassified, public form. The first Review is to be completed by 2012.

Conclusion

National security classification can help to protect the public against catastrophic threats, or it can be used as a means of evading public oversight and accountability. It can enable authorized military, diplomatic and intelligence operations, or it can conceal gross misconduct.

The legitimate functions of national security classification can best be preserved -- and its abuses best prevented -- if the system is narrowly focused, limited in scope and duration, and subject to multiple layers of oversight and error correction.

[14] Executive Order 13526, section 1.9; and ISOO Implementing Directive.