CHAPTER ONE

OPEN GOVERNMENT

INTRODUCTION

A growing preoccupation with secrecy has affected all three branches of government in the two years since September 11. A series of legal and policy decisions has made it more difficult for Congress, the courts, and the American public to oversee the operations of the executive branch. Despite signs of increased concern about these changes by Congress in recent months, the normalization of secrecy shows little sign of abating.

This chapter examines how a framework of increased secrecy has developed – encompassing both specific initiatives and a more general pattern of less openness about the way important executive branch decisions are made. The chapter details both of these phenomena and illustrates the consequences of these changes for the values promoted by open government. Finally, it addresses the types of responses needed – particularly given that, in the absence of a formal declaration of war or a traditional, focused external threat, the current security climate may persist indefinitely.

LEGAL BACKGROUND

> *A popular Government without popular information, or the means of acquiring it, is but a Prologue to a Farce or Tragedy; or, perhaps both.*[1]
>
> **James Madison**

In the democracy envisioned by Madison, effective checks against arbitrary power flow from a government structure in which each branch of government shares information about its activities with the others, and in which the people themselves have access to information about the way government works. Government has always had vital interests in keeping some information secret – protecting intelligence sources and methods and ensuring the safety of military operations among them. But the past half century in particular has seen the creation of an elaborate system of rules designed to protect government's most important secrets – a system that increasingly has encroached on Madison's vision that the operations of the U.S. government would be open to its people.

Most of the rules of this secrecy system have been set forth in a series of executive orders, beginning with President Harry S. Truman in 1951 and continuing through President George W. Bush earlier this year.[2] Through these directives, the executive branch has established standards for how "national security information" should be classified, the different categories of information eligible for classification, and the general grounds on which government secrets should be established and maintained.

Not long after the first such executive order was issued, a special committee convened by President Eisenhower's Secretary of Defense warned that the classification system was already "so overloaded that proper protection of information which should be protected has suffered," and that "the mass of classified papers has inevitably resulted in a casual attitude toward classified information, at least on the part of many."[3] Partly in response to such concerns,[4] Congress passed the Freedom of Information Act (FOIA) in 1966 and strengthened it substantially in 1974.[5] FOIA established a presumption that executive branch documents would be available to the public subject only to carefully defined exceptions, and that judicial review would be available as a check on agency decisions to withhold information. In signing FOIA into law on July 4, 1966, President Lyndon Johnson emphasized its chief objective: "This legislation springs from one of our most essential principles: a democracy works best when the people have all the information that the security of the nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest."[6]

THE NEW NORM OF GOVERNMENT SECRECY

> *Much the same way the indiscriminate use of antibiotics reduces their effectiveness in combating infections, classifying either too much information or for too long can reduce the effectiveness of the classification system, which, more than anything else, is dependent upon the confidence of the people touched by it. While there is always a temptation to err on the side of caution, especially in times of war, the challenge for agencies is to similarly avoid damaging the nation's security by hoarding information.*[7]
>
> **J. William Leonard**,
> Director, Information Security Oversight Office
> National Archives and Records Administration

There is some historical precedent for the expanded government secrecy of the past two years; the first and second World Wars and the early years of the Cold War all saw some level of expansion. But the scope of executive branch initiatives to restrict access to information since September 11 has been broader than in the past. More than during previous periods of heightened security concern, the post-September 11 executive has made secrecy – rather than disclosure – its default position.

According to data collected by the Information Security Oversight Office of the National Archives and Records Administration (ISOO), the number of classification actions by the executive branch rose 14 percent in 2002 over 2001 – and declassification activity fell to its lowest level in seven years.[8] Both in limiting the disclosure of basic information and in denying the public access to executive decision-making processes, the new normal is a democracy with diminished ability to check the exercise of government power, and increased risk of missing information vital to security.

Restricting the Flow of Information

For nearly four decades, and especially since its enhancement in 1974, FOIA has played a central role in expanding public access to executive information, subject to a series of nine carefully delineated exceptions.[13] Beginning before September 11 and accelerating in the two years since, the administration has sought to restrict FOIA both by (1) expanding the reach of existing statutory exemptions, and (2) adding a new "critical infrastructure" exemption. While the effects of the latter initiative remain unclear, recent court cases on the expansion of existing exemptions verify the extent of the threat to openness posed by the new restrictions.

THE FREEDOM OF INFORMATION ACT

As the U.S. Supreme Court explained in 1973, FOIA "seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable public right to secure such information from possibly unwilling official hands."[9] Under FOIA, "any person" may file an application for access to any document, file, or other record in the possession of an executive agency – without demonstrating any need for the information requested.[10] An agency must release the information requested under FOIA unless it falls within one of the statutory exemptions. If the agency decides to withhold the information, the applicant can challenge that decision in court – where the agency bears the burden of showing that its refusal was legitimate.[11] Courts have generally shown some deference to an agency's determination that a certain exception applies, but such determinations "must be clear, specific, and adequately detailed; they must describe the withheld information and the reason for nondisclosure in a factual and non-conclusory manner; and they must be submitted in good faith."[12]

The Ashcroft Directive

In October 2001, Attorney General John Ashcroft issued a new directive to the heads of executive agencies that announced two key changes in previous executive branch practice. First, it encouraged the presumptive refusal of any FOIA request over which departments and agencies could exercise discretion. Second, it reversed previous Justice Department policy to defend an agency's refusal to release information only where release would result in "foreseeable harm"; instead, the department would now defend any refusal to release information as long as it had a "sound legal basis."[14]

This was anything but a temporary, emergency approach limited to the immediate aftermath of September 11. Subsequent memoranda, including from White House Chief of Staff Andrew Card, further encouraged agencies to use FOIA exemptions to withhold "sensitive but non-classified" material – a loosely-defined category of information (discussed in more detail below) that could include information voluntarily submitted to the executive from the private sector. As one such memorandum explained:

> All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful

> consideration to all applicable FOIA exemptions. . . . In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552 (b)(4).[15]

Recent court decisions have bolstered the administration's success in expanding the reach of FOIA exemptions. In *American Civil Liberties Union v. U.S. Department of Justice*, the district court denied the ACLU's request for information concerning how often the Justice Department had utilized its expanded surveillance and investigative authority under the PATRIOT Act.[16] To prevent disclosure, the administration invoked FOIA Exemption 1, which permits the withholding of information specifically authorized by an executive order to be kept secret in the interests of national defense or foreign policy.[17] While the court acknowledged the plaintiffs' arguments that the disclosure sought would not harm national security because it would not involve any particular records or other information on current surveillance,[18] it determined that plaintiffs could not "overcome the agency's expert judgment that withholding the information is authorized . . . because it is reasonably connected to the protection of national security."[19]

Of perhaps greater significance is *Center for National Security Studies v. U.S. Department of Justice,* in which a divided three-judge panel of the U.S. Court of Appeals for the D.C. Circuit upheld the executive's assertion that FOIA Exemption 7(A) could be used to withhold the names of those detained in the course of investigations following September 11, as well as other information about the detainees, such as the locations, dates, and rationale for their detention.[20] In contrast to earlier rulings requiring that the executive's explanation for withholding information be reasonably specific,[21] the majority broadly deferred to the executive branch in accepting its assertion that disclosure of the requested information could be expected to interfere with law enforcement proceedings – explaining simply "we owe deference to the government's judgments contained in its affidavits."[22]

This change in approach greatly concerned dissenting Judge David Tatel, who warned that "the court's uncritical deference to the government's vague, poorly explained arguments for withholding broad categories of information . . . eviscerates both FOIA and the principles of openness in government that FOIA embodies."[23] Judge Tatel acknowledged that some of the requested information without question should be exempt from disclosure, but added that the request should not be denied in its entirety:

> This all-or-nothing approach runs directly counter to well-established principles governing FOIA requests . . . the government bears the burden of identifying functional categories of information that are exempt from disclosure, and disclosing any reasonably segregable, non-exempt portion of the requested materials.[24]

Judge Tatel called for a more particularized approach to identifying – and explaining – how the information pending release could negatively affect national security. As Judge Tatel noted, requiring executive agencies to "make the detailed showing the FOIA requires is not second-guessing their judgment about matters within their expertise," but rather applying the law

as it was intended – and ensuring that the judicial branch retains a "meaningful role in reviewing FOIA exemption requests."[25]

"Critical Infrastructure" Exemption

In November 2002, Congress passed an expansive "critical infrastructure" exemption introduced by the administration as part of the Homeland Security Act of 2002.[26] The new exemption provides that all information submitted to the Department of Homeland Security (DHS) that is "not customarily in the public domain and related to the security or critical infrastructure or protected systems" is not subject to disclosure under FOIA.[27]

While this new exemption has not yet been utilized to deny access to information under FOIA, and DHS has been slow to publish implementing regulations, it is potentially far-reaching and appears broad enough to withhold a wide range of both private and governmental information. Indeed, proposed regulations to implement the exemption broadly state the type of information that may be restricted and also fail to require that those providing the information substantiate their claim that it falls within the "critical infrastructure" category.[28]

The administration has argued that the new exemption is necessary to facilitate information sharing; chemical and other firms had claimed that they would be reluctant to provide information to the government if they thought it would become public. However, FOIA already contains clear exemptions for confidential business information, as well as national security information.[29] Further, while the intention of the new exemption obviously is to enhance security, to the extent that it prevents disclosure of information showing wrongdoing or ineptitude by private parties it could weaken incentives for private entities to address ongoing or potential problems.

Finally, the new exemption could limit public access to critical health, safety, and environmental information submitted by businesses to the executive – for example, the status of a safety problem at a nuclear power plant, or a chemical facility producing toxic materials and located in a densely populated urban neighborhood.[30] This risk is particularly troubling because "critical infrastructure" information cannot be used against the submitting party in any civil action provided it was submitted in good faith. Even if the information reveals that a firm is violating health, safety, or environmental laws, DHS cannot bring a civil action based on that information.[31]

The potential danger posed by the still-unused "critical infrastructure" exemption has greatly concerned some members of Congress. Senator Patrick Leahy (D-VT), for example, warned that the exemption represented the "most severe weakening" of FOIA to date.[32] To address such concerns, Senators Leahy, Carl Levin (D-MI), Joseph Lieberman (D-CT), James Jeffords (I-VT), and Robert Byrd (D-WV), and Representatives Barney Frank (D-MA) and Tom Udall (D-NM), introduced the Restoration of Freedom of Information Act of 2003 earlier this year.[33]

The "Restore FOIA Act," as its proponents have termed it, narrows the definition of "critical infrastructure" information to focus on records directly related to the vulnerabilities of

and threats to such infrastructure, and limits the exemption to include only information the government could not have obtained without voluntary submission by private firms.[34] It allows for disclosure of records an agency receives independently from DHS and requires that DHS make available any portion of an exempted record that can be segregated. It removes the exemption of communication of "critical infrastructure" information from open meeting requirements. Finally, it removes the prohibition on using "critical infrastructure" information against the submitter in a civil action.[35]

In short, the new legislation is intended to address concerns such as those expressed by Mark Tapscott, the Director of the Heritage Foundation's Center for Media and Public Policy, who noted that without such narrowing and clarification the provision "could be manipulated by clever corporate and government operators to hide endless varieties of potentially embarrassing and/or criminal information from public view."[36]

Classifying New Information: A Presumption of Secrecy

Executive Order 13292

Executive Order 13292 (E.O. 13292), issued by President Bush on March 28, 2003, represents another example of the expanding default to secrecy – easing the burden on executive officials responsible for deciding whether to classify in the first instance, and making it more difficult for the public to gain access to information.

The latest in a series of presidential orders dating back over half a century to govern the classification (and procedures for later declassification) of national security information,[37] E.O. 13292 modifies the order issued by the previous administration in 1995 in certain important respects.[38] While the new order preserves some important elements of its predecessor, including the interagency classification review panel that has prompted increased declassification of older documents,[39] it promotes greater secrecy by: (1) allowing the executive to delay the release of certain documents; (2) giving the executive new powers to reclassify previously released information;[40] (3) broadening exceptions to declassification; and (4) lowering the standard under which information is exempted from release – from requiring that it "should" be expected to result in harm to that it "could" be expected to have that result.[41]

Perhaps most important, E.O. 13292 removes a provision from the 1995 executive order mandating that "[i]f there is significant doubt about the need to classify information, it shall not be classified."[42] This seemingly minor deletion has the effect of changing the "default" setting from "do not classify" to "classify" – likely promoting the classification of more documents, with attendant costs for both government operations and public knowledge. As Thomas Blanton, Executive Director of the National Security Archive, notes, E.O. 13292 thus sends "one more signal . . . to the bureaucracy to slow down, stall, withhold, stonewall."[43]

Executive Order 13292 builds upon other efforts to make it easier to classify a wider range of information. In three separate executive orders, the current administration expanded the authority to classify documents to include the Secretary of Agriculture, Secretary of Health and Human Services, and Administrator of the Environmental Protection Agency (EPA).[44] While

those officials already had means of protecting information, they previously had not had the original classification authority typically vested in officials at departments and agencies engaged in core national security activities.

Homeland Security Information: "Sensitive but Unclassified"

> *We're talking about the safety and security of people who would be better protected by this report . . . . This is just bad public policy. If there's something that needs to be redacted, take it out.*[45]
>
> **David Heyman**,
> Center for Strategic and International Studies
> (on the Defense Department's decision to keep secret his report
> on public preparation for bioterrorism attacks)

A little-noticed provision of the Homeland Security Act of 2002 may prove to be a significant barrier to congressional and public access to a wide range of information. Ironically, this provision, which requires the president to prescribe and implement procedures to "identify and safeguard homeland security information that is sensitive but unclassified," is contained in the section of the act on "information sharing."[46]

This open-ended language, enacted with little debate or scrutiny, gives the executive branch wide discretion to withhold vast amounts of information even without the need to do so through formal classification. Most of the provision's terms, including "sensitive but unclassified," are not defined. And "homeland security information" is defined so broadly with respect to counterterrorism activities as to potentially encompass a wide range of information extending well beyond what traditionally has been classified under executive orders for national security purposes.[47]

Moreover, unlike the "critical infrastructure" information provision of the act discussed above, there is no "savings clause" – a provision that would require information that falls within this potentially sweeping category to be revealed if another statute or regulation mandates such disclosure.[48] In other words, the sweeping language of the Homeland Security Act could trump disclosure provided for under a previously enacted law. Finally, the provision grants full control over managing and sharing such "homeland security information" to the president, who is required only to submit a report to Congress on the section's implementation by November 25, 2003.[49]

How the executive branch will implement this provision remains unclear. One recent example that might prove illustrative involves the Defense Department's refusal over the past year to release an unclassified report on lessons learned from the anthrax attacks in late 2001. That report, the outgrowth of a December 2001 meeting organized by the Center for Strategic and International Studies and funded by the Department's Defense Threat Reduction Agency, included recommendations for improving the nation's preparation for future bioterrorism attacks.[50] However, the Defense Department determined that the report should be treated as "For

Official Use Only" (a category of restricting access to unclassified information analogous to "sensitive but unclassified") and refused to release any portion of it to the public.

The "homeland security information" provision represents a sweeping new delegation of authority to expand secrecy well beyond formal classification procedures in a manner that is likely to further impair Congress' oversight responsibilities. Whether Congress will step in to try to mitigate this potential remains uncertain.

Withdrawal of Information Previously Released

The administration also has removed information previously available to the public from government websites. The deletions have extended beyond highly sensitive materials that may have been posted inadvertently to also reach general program information. For example, the Federal Aviation Administration removed data from its website regarding enforcement actions against air carriers. And the EPA removed risk management plans that provide important information about the dangers of chemical accidents and emergency response mechanisms. These actions were taken despite the fact that such information may be important for those planning to fly and those living near chemical plants; in the case of the information withdrawn by the EPA, the FBI had explicitly stated that its availability presented no unique terrorist threat.[51]

Limiting Congressional Oversight

Open and transparent procedures for making government decisions are crucial for congressional and public oversight and, in turn, an understanding of the terms and consequences of the policy decisions that emerge. Just as the developments summarized above demonstrate a growing presumption of information secrecy, the increase in secrecy surrounding the processes of executive branch decision-making reveals a default instinct to remove such processes from public view. This has been evidenced in the past year by the secrecy surrounding consideration of provisions to expand the PATRIOT Act, efforts to withhold information in the congressional report on September 11 intelligence failures, and the denial of access to meetings of key DHS private sector advisors.

The PATRIOT Act and the Justice Department

> *We want to make sure that what we pass in Congress works the way we wanted it to, and that the money is spent the way we intended. We need a maximum flow of information to make the separation of powers work.*[52]
>
> **Senator Charles Grassley (R-IA)**

The past year has been marked by several clashes between senior members of Congress and the administration over access to information on the implementation of the PATRIOT Act. Following denials by the Justice Department of information he considered relevant, House Judiciary Committee Chairman James Sensenbrenner (R-WI) threatened to subpoena documents relating to the act's implementation – prompting the Justice Department to respond to some of

the committee's questions.[53] The Department initially answered 28 of the 50 questions from the committee, but indicated in most responses that the information was classified.[54] When Senator Patrick Leahy, ranking member on the Senate Judiciary Committee, then submitted 93 questions, including the 50 already posed by the House Judiciary Committee, the Justice Department responded to only 56 of them in a sequence of three letters – though it shared certain other information with the intelligence committees.

The Justice Department and the FBI had also repeatedly refused to provide Judiciary Committee members with a copy of the secret Foreign Intelligence Surveillance Act (FISA) Court's May 17, 2002 opinion rejecting the Department's proposed implementation of the PATRIOT Act's FISA amendments,[55] and criticizing aspects of the FBI's past performance on FISA warrants.[56] (FISA and its implementation are discussed in detail in Chapter 2.) In response, in February 2003, Senators Leahy, Grassley, and Arlen Specter (R-PA) introduced the Domestic Surveillance Oversight Act of 2003, intended as one means of reasserting a portion of Congress' oversight authority.[57] The bill modifies FISA by adding to its public reporting requirements. It directs the attorney general to include, in an annual public report on FISA, the aggregate number of U.S. persons targeted for any type of order under the act, as well as information about the total number of times FISA is used for criminal cases or law enforcement purposes.

Expressing the importance of greater oversight regarding the changes adopted in the PATRIOT Act more generally,[58] Senator Leahy explained:

> Before we give the government more power to conduct surveillance on its own citizens, we must look at how it is using the power that it already has. We must answer two questions: Is that power being used effectively, so that our citizens not only *feel* safer, but *are in fact* safer? Is that power being used appropriately, so that our liberties are not sacrificed?[59]

These remarks came in the context of a series of moves by the Justice Department to restrict Congress' access to information in its oversight capacity. For example, on March 27, 2003, the Department issued a directive telling its employees to inform the Department's Office of Legislative Affairs "of all potential briefings on Capitol Hill and significant, substantive conversations with staff and members on Capitol Hill. . . . We will assist in determining the appropriateness of proceeding with potential briefings."[60] Senator Grassley attacked the directive as "an attempt to control information."[61] Senator Leahy noted that "the administration's overwhelming impulse has been to limit the flow of information, and that has made congressional oversight of this Justice Department a never-ending ordeal."[62]

Indeed, the March directive came on the heels of controversy regarding the development and drafting of the "Domestic Security Enhancement Act of 2003," commonly known as "PATRIOT II."[63] Its provisions, including those expanding the authorization of secret arrests, the expedited loss of U.S. citizenship, and deportation powers, raise profound human rights and civil liberty concerns. Although rumors of a draft had circulated for months prior to its leak in early February 2003, Justice Department officials repeatedly had denied that they were preparing any new legislation. As late as February 3, just four days before the draft was leaked,

Department officials assured Senator Leahy's staff that the Justice Department was not drafting any such proposals. At a hearing before the Committee on March 4, 2003, Senator Leahy told Attorney General Ashcroft bluntly: "Somebody who reports directly to you lied . . . and I think that this is not a good way to do things. . . . I think it shows a secretive process in developing this."[64]

Faced with strong reactions from other members of Congress and the press, Attorney General Ashcroft continued to deny that the administration had planned to present a "PATRIOT II" proposal to Congress – only acknowledging that the administration was continuing to "think expansively" about the relevant issues and not ruling out the prospect that certain proposals might be submitted to Congress at some future time. At the same time, he appeared to rule out the possibility of any advance consultation with the committees of jurisdiction, stating at a March 4 Senate Judiciary hearing: "Until I have something I think is appropriate, I don't know that I should engage in some sort of discussion."[65]

The administration has not acknowledged the concerns about process – including whether given the substantial interest in the implementation of the PATRIOT Act there should have been consultation with Congress on the issues under consideration. Despite the controversial provisions being considered, the draft apparently was forwarded only to Vice President Cheney (in his capacity as President of the Senate) and Speaker of the House Dennis Hastert (R-IL).[66]

House Judiciary Committee Chairman Sensenbrenner expressed concerns about the scope of the proposal and the lack of congressional consultation: "[A]s I stressed during legislative consideration of the PATRIOT Act, my support for this legislation is neither perpetual nor unconditional. I believe the Department and Congress must be vigilant."[67] Despite this, recent reports suggest that the Justice Department continues to work on a version of similar legislation behind closed doors[68] – consistent with calls by the president and attorney general for expanded powers to arrest, detain, and seek the death penalty.[69] While controversy over "PATRIOT II" may make it too difficult to submit the bill as a single integrated package, pieces of the leaked draft – coupled with other proposals – may be introduced separately in the coming months. Senator Orrin Hatch (R-UT) is expected to introduce one such bill, the VICTORY Act, in the fall of 2003.[70] One provision of this bill would grant the Justice Department the authority to seize private records in terrorism investigations through the use of administrative subpoenas, bypassing the federal courts (as discussed in Chapter 2).[71] President Bush publicly endorsed this proposal in a speech at the FBI Academy on September 10, 2003, claiming that current law posed "unreasonable obstacles to investigating and prosecuting terrorism."[72]

In August 2003, just after the draft of the VICTORY Act became public, Attorney General Ashcroft launched a campaign aimed at convincing the American people of the need for the Justice Department's expanded powers under the PATRIOT Act.[73] Ironically, that campaign has been closed to the public.[74] Although the attorney general has been traveling the country to shore up support for the PATRIOT Act, in nearly every city he has visited so far he addressed only a pre-screened group of law enforcement officers in closed sessions.[75] And following each speech, the attorney general has refused to take questions, even from newspaper journalists trying to report on what he said.[76]

FACA and the Department of Homeland Security

An additional limit on oversight has been through the exemption of advisory committees constituted by DHS from the Federal Advisory Committee Act (FACA). Enacted in 1972, FACA is intended to limit the ability of interest groups to influence public policy by making Congress and the public aware of the composition and activities of advisory committees set up by the executive branch. Such advisory committees often serve as the primary instrument for outside input into executive branch decision-making. FACA mandates that such committees announce their meetings, hold them in public, provide for representation of differing viewpoints, and make their materials available. The act also provides exemptions on the basis of national security for shielding from disclosure certain information and activities.[77]

Under Section 871 of the Homeland Security Act however, DHS advisory committees are exempt from FACA's requirements, and the committees thus may meet in secret.[78] As a result, their activities and reports will be shielded from scrutiny, regardless of the subject matter under review or the interests of the advisory committee members. This broad carve-out, which covers advisory committee engagement with components of DHS previously located in other departments where they were subject to FACA requirements, extends well beyond the focused exemptions that already existed in FACA and could have been utilized by DHS.

In an effort to address this carve-out, Senator Robert Byrd offered an amendment to require disclosure of the recommendations of DHS advisory committees, as well as information on the members of such committees. Senator Byrd expressed concern about the exemption from public disclosure in light of what he termed "the specter" of a "conflict of interest" – saying the amendment would help build greater public confidence in the security efforts of DHS. The amendment was rejected on a largely party-line vote of 50-46.

The September 11 Report and the Withholding of Selected Information

> *My judgment is that 95 percent of that information could be declassified, become uncensored, so the American people would know.*[79]
>
> **Richard Shelby (R-AL)**,
> Former Senate Intelligence Committee Chairman

A highly publicized dispute over the classification of Congress' own work product further highlights the tension between the branches concerning restrictions on the release of information. Following the completion of a lengthy joint report of the House and Senate intelligence committees on the intelligence failures leading to the September 11 attacks, an administration working group coordinated by the CIA redacted more than two-thirds of the report's text – including some sections that had already been discussed publicly. Recognizing the implications for effective oversight and understanding of what had gone wrong prior to September 11, a bipartisan group of committee members protested the reach of the CIA's classification process and threatened to use for the first time an obscure, 26-year old Senate rule (Senate Resolution 400) to declassify the document themselves over administration objections.[80] Faced with this

bipartisan threat, the administration scaled back the scope of information that it insisted be redacted.[81]

Despite this, when the report finally was released in mid-July 2003, controversy erupted over key sections that remained classified. While acknowledging the importance of keeping certain information classified to protect intelligence sources and methods, members of Congress raised new concerns about the redaction of other parts of the report. Former Senate Intelligence Committee Chairman Richard Shelby stated that he thought certain sections had been classified for the wrong reasons, referring specifically to a 28-page section dealing with alleged foreign support for terrorism.[82] House Minority Leader Nancy Pelosi (D-CA), also involved in the September 11 inquiry as a senior member of the House Intelligence Committee, emphasized the difficulty in disseminating its findings:

> It took us nine months to do our entire investigation. . . . It took six and a half months to . . . get this declassified version out. . . . They do not want to reveal information that should be available to the public. . . . We need to protect the American people in the future. This secrecy does not serve that purpose.[83]

As of August 2003, 46 senators had signed a letter to the president, circulated by Senators Charles Schumer (D-NY) and Sam Brownback (R-KS), requesting that the White House declassify additional portions of the report.[84] Senate Resolution 400 requires a majority vote to disclose such information over administration objections.[85] In early August, the Democratic members of the House Permanent Select Committee on Intelligence, led by Representative Jane Harman (D-CA), endorsed additional declassification of the portions of the report withheld, saying that "there is a compelling national interest" in doing so, and expanded declassification "will not compromise important intelligence activities."[86] This left open the prospect for a battle between Congress and the executive – and possible unilateral legislative action to release portions of the still-classified sections if a compromise cannot be reached.

The Courts' Deference to Secrecy

Among the most troubling examples of expanded secrecy has been the sustained effort of executive branch officials to close certain immigration proceedings that have traditionally been open – an effort that began immediately after September 11 and has continued in the two years since. Ten days after the September 11 attacks, Chief Immigration Judge Michael Creppy issued a directive requiring immigration judges to implement a full information blackout on any case deemed of "special interest" by the Justice Department.[87] The so-called "Creppy Directive" closes hearings involving such "special interest" detainees and also prohibits court administrators from listing the cases on dockets or confirming when hearings will be held. The restrictions prevent detainees' families and members of the news media from attending the hearings.

In *North Jersey Media Group, Inc. v. Ashcroft*, the U.S. Court of Appeals for the Third Circuit, reversing the district court below, accepted the "credible, although somewhat speculative" national security concerns that the attorney general had used to justify this blanket directive.[88] The court acknowledged that it was "quite hesitant to conduct a judicial inquiry into the credibility of these security concerns," given a tradition of "great deference to Executive

expertise."[89] A dissenting judge accepted the general concept of deference in national security cases, but rejected the Creppy Directive's blanket closure approach and called for reinstituting the authority of immigration judges to conduct a case-by-case analysis.

The U.S. Court of Appeals for the Sixth Circuit reached a very different conclusion in *Detroit Free Press v. Ashcroft*[90] – acknowledging the principle of deference to the executive on national security issues, and the interests asserted by the government for closure, but holding that there is a First Amendment right of access to deportation hearings and that a blanket closure of such hearings was impermissible. In its ruling, the court noted the important role that public access plays in ensuring that procedures are fair and government does not make mistakes.[91]

Despite this split of appellate authority, the U.S. Supreme Court has declined to review the decisions.[92] As it stands, openness advocates may look to the Sixth Circuit in *Detroit Free Press*, and the dissent in *North Jersey Media Group*, both of which criticized the Creppy Directive for not requiring particularized decisions, narrowly tailored so as to restrict only information that would damage national security.

The Question of Security

> *Law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed American public.*[93]
>
> **Eleanor Hill**,
> Staff Director of the Joint U.S. House-Senate Intelligence Committee

While Congress has often yielded quickly to the executive's insistence on secrecy since September 11, some members have begun efforts to recapture some of the access to information that existed prior to the terrorist attacks – giving cause to question whether the new norm of secrecy can be sustained. Some of this stepped-up legislative attention has arisen out of the recognition by members, including many who traditionally have deferred to the executive branch on matters of national security, of the rapid increase in the scope of secrecy and its consequences for their own oversight activities and capabilities.

One example is illustrative. In testimony in May 2003 before a commission investigating the events of September 11, Rep. Porter Goss (R-FL), Chair of the House Permanent Select Committee on Intelligence, testified that "we overclassify very badly . . . there's a lot of gratuitous classification going on," adding that the "dysfunctional" classification system remains his Committee's greatest challenge.[94] Chairman Goss endorsed the efforts made in the 1990s by the late Senator Daniel Patrick Moynihan, who had chaired a two-year bipartisan commission investigating government secrecy that raised concerns about overclassification and issued recommendations to narrow the scope and duration of government secrets. While he had not previously identified himself with those efforts, Chairman Goss now suggested that perhaps they did not go far enough.[95]

Members of Congress with strong security credentials are also recognizing that where secrecy is used to cover up procedural deficiencies within either the government or private sector, it can permit security vulnerabilities and other dangers to go unnoticed and unaddressed, in turn making it harder to correct any errors.[96] And they understand that secrecy can breed increased distrust in governmental institutions. As Senator John McCain (R-AZ) noted in testimony in May 2003: "Excessive administration secrecy on issues related to the September 11 attacks feeds conspiracy theories and reduces the public's confidence in government."[97]

As many of these members are realizing, too much secrecy may well result in *less* security. A system that, in the words of the Director of the Information Security Oversight Office, is often "not perceived as being discerning" with respect to what should be secret in turn carries the risk of reduced accountability – and missed opportunities for needed information sharing both within the government and with the American people.[98]

RECOMMENDATIONS

1. Congress should pass a "Restore FOIA" Act to remedy the effects of overly broad provisions in the Homeland Security Act of 2002, including by narrowing the "critical infrastructure" exemption.

2. Congress should remove the blanket exemption granted to DHS advisory committees from the open meeting and related requirements of the Federal Advisory Committee Act.

3. Congress should convene oversight hearings to review the security and budgetary impact of post-September 11 changes in classification rules, including Executive Order 13292 provisions on initial classification decisions, and Homeland Security Act provisions on the protection of "sensitive but unclassified" information.

4. Congress should consider setting statutory guidelines for classifying national security information, including imposing a requirement that the executive show a "demonstrable need" to classify information in the name of national security.

5. The administration should modify the "Creppy Directive" to replace the blanket closure of "special interest" deportation hearings with a case-specific inquiry into the merits of closing a hearing.