Decisions Without Democracy

by David Banisar

Preface by Bob Barr and John Podesta

People For the American Way Foundation

OpenTheGovernment.org
Americans for Less Secrecy, More Democracy

Government Secrecy:
Decisions Without Democracy

BY DAVID BANISAR

People For the American Way Foundation is an energetic advocate for the values and institutions that sustain a diverse democratic society, and which are threatened by the political rise of the religious right. PFAW Foundation seeks to protect fundamental rights and freedoms guaranteed under the Constitution, sustain an independent judiciary and mobilize activists to support progressive causes.

www.pfaw.org
People For the American Way • 2000 M Street, NW,
Suite 400 • Washington, DC 20036
Telephone: 202-467-4999 or 800-326-7329 • pfaw@pfaw.org
Donations to People For the American Way Foundation, a nonprofit 501(c)(3) organization, are tax deductible

OpenTheGovernment.org
Americans for Less Secrecy, More Democracy

OpenTheGovernment.org is a coalition of consumer and good government groups, environmentalists, journalists, library groups, labor and others united to make the federal government a more open place in order to make us safer, strengthen public trust in government, and support our democratic principles.

www.openthegovernment.org
OpenTheGovernment.org, 1742 Connecticut Avenue N.W., 3rd Floor, Washington D.C. 20009 202-332-OPEN (6736)
A project of the Fund for Constitutional Government.
All donations are tax-deductible to the maximum allowable by law.

Foreword

Excessive secrecy is the enemy of public accountability and democratic governance. Unfortunately, it is becoming standard operating procedure for many government officials. Vice President Dick Cheney's recent insistence that his office is not subject to secrecy regulations that apply to the executive branch is just the latest evidence of a systematic campaign to keep information about government activities out of the hands of the American public.

Freedoms of Information laws are grounded in the recognition that knowledge about the government's actions is the necessary first step in oversight and accountability. Most Americans recognize the need to safeguard national security information from improper public disclosures that would damage the national interest. But national security has become a blanket excuse to withhold information from the public as well as from Congress, especially in the aftermath of the 9/11 terrorist attacks.

The National Security Archive has documented widespread agency mismanagement and obstruction which lead to delays as long as 17 years in responding to public Freedom of Information Act requests. Only one in four agencies is complying with the Electronic Freedom of Information Act a decade after it passed.

Of course, the right to know is also undermined by the release of information that is inaccurate or misleading. At the federal level, politics increasingly trumps sound science: reports on key environmental issues are altered by political appointees; information about HIV/AIDS is manipulated to promote a particular ideological viewpoint; and federal employees are muzzled from sharing their expertise.

The misuse of secrecy and the manipulation of science and other information undermine the public's right to know and the health of our democracy. And they threaten the health of the public as well: a fire at a chemical plant situated near a neighborhood could pose a serious threat to residents' health, but it is difficult for individuals to learn the most basic information about hazards to which their families may be exposed.

The preface to this report, written by Republican Robert Barr and Democrat John Podesta, reflects that the importance of the public's right to know is not a partisan issue; it is a fundamentally American issue.

Over the years, regardless of the political party in charge, our three organizations have challenged excessive government secrecy and offered ideas to protect the public's right to know. For example, in 1987, People for the American Way, OMB Watch, the Benton Foundation, and the Advocacy Institute launched a public education campaign to draw attention to the ways in which government was withholding information from the public. One element of that campaign was the publication by People for the American Way of Government Secrecy: Decisions Without Democracy, a primer on secrecy that serves as the model for this publication.

OMB Watch and National Security Archive followed Government Secrecy with a retreat at the Blue Mountain Center in New York in the early 1990s that established principles for advancing the public right to know that have guided the public interest community for more than a decade.

But today the foundation of democratic accountability is being steadily eroded. At the same time that technology has given us new tools for linking government information in ways that could empower citizens, policies and procedures at the federal, state, and local levels serve as barriers to fulfilling the promise. And public confidence in the openness of the federal government is shrinking, as documented in a recent poll by the Association of Newspaper Editors.

Our three organizations are part of OpenTheGovernment.org, a broad-based coalition that brings together journalists, librarians, academics, individual citizens, advocacy groups, and professional associations committed to strengthening and protecting our right to know. This primer is just one step in engaging the public in a campaign to make our government more transparent and accountable to the public. "We the people" must exercise our rights to strengthen, if not preserve, democracy. We encourage you to get involved by visiting the website (www.openthegovernment.org) to learn what you can do.

We want to thank David Banisar, the author of this publication, for his excellent work. Patrice McDermott, the director of the OpenTheGovernment.org, and Emily Feldman, the policy associate, shepherded the process from start to finish. They did a wonderful job. This project would have not started had not Conrad Martin of the Fund for Constitutional Government suggested the idea. The Steering Committee for OpenTheGovernment.org provided invaluable assistance in establishing the themes of this book: the expansive and myriad secrecy we confront; and the opportunities that a more digital government presents to us for greater participation, openness, and accountability. Special thanks goes to Elliot Mincberg while he was with People for the American Way, Steve Aftergood, Marge Baker, Mary Alice Baish, and Charles Davis who served as a panel to provide the ongoing advice, guidance and review that led to this strong report.

Gary D. Bass
Executive Director, OMB Watch
and co-chair, OpenTheGovernment.org

Thomas S. Blanton
Executive Director, National Security Archive
and co-chair, OpenTheGovernment.org

Ralph G. Neas
President, People for the American Way
and partner, OpenTheGovernment.org

July 2007

Preface

by Bob Barr and John Podesta

Twenty years ago, People for The American Way published the first "Government Secrecy" primer. At the time, our founding principles of openness and accountability were being strained under the decades-long Cold War with the Soviet Union. Presidents of both parties repeatedly invoked security to justify greater secrecy, very often in ways that did not reflect legitimate security concerns but rather served what Arthur Schlesinger, Jr. called in his preface "the Imperial Presidency."

Today, we face a new security threat, but the Imperial Presidency is back. In the aftermath of the 9/11 terrorist attacks, the current administration has laid claim to a dramatic expansion of executive power, sometimes with congressional approval, as with the PATRIOT Act, and sometimes through legally dubious assertions, as with the National Security Agency's domestic surveillance program.

At the same time, the administration has routinely withheld information that should be made public, thereby insulating itself from democratic accountability. As this primer documents, secrecy has been advanced in a myriad of ways, including excessive classification, brazen assertions of "executive privilege" and "state secrets," new control markings to restrict "sensitive but unclassified" information, and new limits on Freedom of Information Act requests.

The government should, of course, keep certain kinds of information secret. Our laws recognize the need to protect national security information, such as intelligence sources and military plans, for example, as well as personally identifiable data, such as information provided on tax returns. But the secrecy claims asserted by the administration go far beyond what is contemplated by the law—and far beyond what is healthy for democracy, which depends on an informed citizenry.

Citizens deprived of relevant information cannot participate in their government's decisions or hold their leaders accountable. Without this check, government officials are more likely to make decisions contrary to the public interest, abuse their authority, and engage in corrupt activities. In words that ring prophetic today, James Madison warned in 1822, "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."

The administration's embrace of secrecy comes frustratingly at a time of great opportunity for government openness. The Internet and other new information technologies make it far easier and cheaper for government to disseminate information and interact with the public. Through government Websites, for example, citizens can now access the Congressional Record, track environmental pollution in their neighborhoods, and comment on regulatory proposals. Instead of building on this foundation, however, the executive branch is retrenching—in a host of cases, government information previously available through the Internet has been removed.

This primer by David Banisar on behalf of OpenTheGovernment.org and People for the American Way clearly documents the expansion of secrecy and the dangers posed to democracy. In doing so, it provides ammunition to reclaim the open and balanced system of government set forth in our Constitution and Bill of Rights. It is now up to all of us to make our voices heard. ❖

Preface to the 1987 Edition

by Arthur Schlesinger, Jr.

Secrecy is the bane of democracy because it is the enemy of accountability. The framers of the American Constitution designed a system of government intended to bring power and accountability into balance. The secrecy system, as it has been nurtured by the executive branch over the last forty years and with special zeal over the last seven years, is the indispensable ally and instrument of the Imperial Presidency.

Now no one can question the right of the state to keep certain things secret. Weapons technology and deployment, diplomatic negotiations, intelligence methods and sources, and military contingency plans are among the areas where secrecy is entirely defensible. Secrecy is defensible too in certain domestic areas: personal data given the government on the presumption it would be kept confidential—tax returns, personnel investigations and the like; and official decisions that, if prematurely disclosed, would lead to speculation in land or commodities, preemptive buying, higher governmental costs and private enrichment.

But the contemporary state has extended the secrecy system far beyond its legitimate bounds. In doing so, the target is far less to prevent the disclosure of information to enemy governments than to prevent the disclosure of information to the American Congress, press and people. For governments have discovered that secrecy is a source of power and an efficient way of covering up the embarrassments, blunders, follies and crimes of the ruling regime.

When governments claim that a broad secrecy mandate is essential to protect national security, they mostly mean that it is essential to protect the political interests of the administration. The harm to national security through breaches of secrecy is always exaggerated. The secrecy system has been breached since the beginning of the republic—from the day in 1795 when Senator Mason of Virginia enraged President Washington by giving the secret text of Jay's Treaty to the Philadelphia Aurora, or the day in 1844 when Senator Tappan of Ohio enraged President Tyler by giving the secret text of the treaty annexing Texas to the New York Evening Post. No one has ever demonstrated that such leaks, or the publication of the Pentagon Papers either, harmed national security. No one can doubt that these disclosures benefited the democratic process.

The republic has survived great crises—the War of 1812, the Civil War, the First and Second World War— without erecting the suffocating structure of secrecy the Reagan administration proposes today. One wonders what greater crisis justifies the extreme measures taken and contemplated by the Reagan administration since 1981. The consequences for American democracy of the cult of secrecy may be dire. For the secrecy system not only safeguards the executive branch from accountability for its incompetence and its venality. Worse, it emboldens the state to undertake rash and mindless adventures, as the Iran-contra scandal sadly reminds us. "Though secrecy in diplomacy is occasionally unavoidable," wrote James Bryce, who was not only an acute student of comparative government but also a distinguished diplomat, "it has its perils...Publicity may cause some losses, but may avert some misfortunes." Perhaps President Reagan will one day regret that the press had not exposed

his secret intentions toward Iran in time to block his ill-considered policy, as President Kennedy regretted that the New York Times had not played up its story on the exile invasion of Cuba. "If you had printed more about the operation," he told a Times editor, "you would have saved us from a colossal mistake."

Because the secrecy system is controlled by those on whom it bestows prestige and protection, it has long since overridden its legitimate objectives. The religion of secrecy has become an all-purpose means by which the American Presidency seeks to dissemble its purposes, bury its mistakes, manipulate its citizens and maximize its power. This People For the American Way report by Steven L. Katz is a meticulous and dispassionate account of the growth and widening reach of the secrecy system and of the danger it poses to American democracy. It is not too late for Congress to bring the secrecy system under control and redress the balance between presidential power and presidential accountability.

The issue is hardly new. "Executive secrecy," John Taylor of Caroline, the philosopher of Jeffersonian democracy, wrote in 1814, "is one of the monarchial customs, plausibly defended, and certainly fatal to republican government...How can national self government exist without a knowledge of national affairs? or how can legislatures be wise or independent, who legislate in the dark upon the recommendation of one man?" ❖

December 1987, New York

Acknowledgements

The Steering Committee for OpenTheGovernment.org provided invaluable assistance in establishing the themes of this book: the expansive and myriad secrecy we confront; and the opportunities that a more digital government presents to us for greater participation, openness, and accountability. A smaller editorial committee provided ongoing advice, guidance and review that led to this strong report.

Recognition must also be given to the staff of OpenTheGovernment.org who shepherded the process and assisted with the proof-reading and copy-editing.

OpenTheGovernment.org is most grateful for the generous support of the Angelina Fund, CS Fund, Educational Foundation of America, HKH Foundation, Knight Foundation, Open Society Institute, Philanthropic Venture Fund, and Warsh-Mott Legacy, which made this publication possible.

We would like to acknowledge our partners in OpenTheGovernment.org, many of whom have labored in these fields for many years and all of whom continue to work to push back secrecy and advance openness and accountability in our government:

American Association of Law Libraries, American Booksellers Foundation for Free Expression, American Library Association, American Society of Newspaper Editors, Association of American Publishers, Association For Community Networking, Association of Research Libraries, Bill of Rights Defense Committee, Californians Aware, Center for American Progress, Center for Democracy and Technology, Center for National Security Studies, Center for Progressive Reform, The Center for Public Integrity, Common Cause, Electronic Frontier Foundation, Electronic Privacy Information Center, EnviroJustice, Environmental Defense, Essential Information, Federation of American Scientists, First Amendment Foundation, Florida First Amendment Foundation, Free Expression Policy Project, Friends Committee on National Legislation, Fund for Constitutional Government, Good Jobs First, Government Accountability Project, Humanist Society of New Mexico, Human Rights First, Illinois Community Technology Coalition, Indiana Coalition for Open Government, Institute for Defense and Disarmament Studies, James Madison Project, League of Women Voters, Liberty Coalition, Mine Safety and Health News, Minnesota Coalition on Government Information, National Coalition Against Censorship, National Coalition for History, National Committee Against Repressive Legislation, National Freedom of Information Coalition, National Security Archive, National Security Whistleblowers Coalition, New Jersey Work Environment Council, Northern California Association of Law Libraries, NPOTechs, OMB Watch, PEN American Center, People For the American Way, Political Research Associates, Positive Financial Advisors, Inc, Project On Government Oversight, Public Employees for Environmental Responsibility, ReadtheBill.org, ReclaimDemocracy.org, Reporters Committee for Freedom of the Press, Society of American Archivists, Society of Professional Journalists, Southeastern American Association of Law Libraries, Special Libraries Association, Sunlight Foundation, Taxpayers for Common Sense, Transactional Records Access Clearinghouse, U.S. Public Interest Research Group, Washington Coalition for Open Government, Working Group on Community Right-to-Know.

Executive Summary

Openness is an American value. It promotes democracy and good government. It reduces corruption and ensures that rights are respected and protected. In the past six years, the basic principle of openness as the underpinning of democracy has been serious undermined. The Administration has taken an extreme view of the power of the presidency. In its view, its powers to operate are largely unchecked by the Congress, courts, states or the public.

Existing laws on openness have been undermined while secrecy is increased. The Administration has issued executive orders placing limits on the Freedom of Information Act and Presidential Records Act, expanded the power to classify information for national security reasons, and created a whole range of new categories of "sensitive" information. Classification of information has nearly doubled while efforts toward declassification have largely been stopped and many records were secretly reclassified. Thousands of records have disappeared off of public web sites. The State Secrets privilege has been regularly invoked in shutting down court challenges.

Congress and the public have been misled about important issues. Government decision-making leading up to and following the invasion of Iraq has been rife with misinformation and secrecy. Key evidence relating to the presence of chemical and biological weapons was misrepresented and key information withheld from Congress and the public. Once the initial invasion was over, information about contracts activities and costs that shows millions of dollars have been lost in fraud and mismanagement has been systematically hidden. Records relating to abuses in prisons were classified. The photos of the caskets of dead soldiers, bringing home the severity of the war, were prohibited from being released.

The public health has been threatened. In 2006, the Environmental Protection Agency approved changes limiting the collection of information about how much chemical waste they released into the environment. In 2004, the National Highway Traffic Safety Administration restricted the amount of information on the safety of automobiles that would be released to the public.

Dozens of whistleblowers who have revealed information about misconduct in federal agencies have been fired, lost their security clearances or been transferred to lesser jobs. Scientists have faced new restrictions on their ability to speak to the press about scientific issues. Employees at NASA were censored from speaking about global warming. The EPA decreed that whistleblower protections under environmental laws no longer applied to workers. Journalists have also been investigated and jailed for refusing to identify the sources of their information.

At the same time, advances in digital technology have increased the amount of information and the speed at which it is available. Federal laws, regulations and structures are available online. Information that was

once difficult to obtain is now available at the click of a button.

The new digital technologies also offer unprecedented opportunities for organizations and citizens to obtain and use information to monitor the government and affect government policy. E-government allows for easier access to services and some governance such as rulemaking.

However, digital information is not a panacea. Problems continue with technology distribution and education to ensure that all persons have equal access to government information. Information can also disappear in the blink of an eye. Thousands of pages were abruptly removed from federal web sites following 9/11. Long term strategies for collecting, archiving and maintaining information are not yet fully developed.

It is now time for Congress to take charge. Oversight is needed to ensure that laws are enforced. Many need revisions to replace the policies that have been put in place in the last six years with more openness. Others need to be updated to recognize changes in law, society and technology in the past decade. ❖

1

Openness: an American Value

Liberty cannot be preserved without a general knowledge among the people, who have a right, from the frame of their nature, to knowledge…and a desire to know; but besides this, they have a right, an indisputable, unalienable, indefeasible, divine right to that most dreaded and envied kind of knowledge, I mean, of the characters and conduct of their rulers.[1]

–JOHN ADAMS, 1765

The liberties of a people never were, nor ever will be, secure, when the transactions of their rulers may be concealed from them.[2]

–PATRICK HENRY, 1788

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.[3]

–JAMES MADISON, 1822

American democracy is based, in the words of Thomas Jefferson, on government "deriving their just powers from the consent of the governed." It has been long recognized that openness is essential to ensuring that government is working on behalf of its citizens. Individuals have the right to know, either directly from officials, or through organizations, the media or their elected representatives, how government is operating to ensure it is on their behalf. The information held by the government is owned by the American people and only held in trust for them by the government and its officials.

Openness has many benefits for both citizens and governments. It promotes trust and efficient government, it reduces mismanagement and corruption, and it promotes rights, fairness and the rule of the law.

THE BENEFITS OF OPENNESS

Openness limits misinformation and promotes awareness and trust in government. Government officials are less able to mislead the public for political reasons if the system is open and information is widely available. As noted by President Nixon in 1972, "Fundamental to our way of life is the belief that when information which properly belongs to the public is systematically withheld by those in power, the people soon become ignorant of their own affairs, distrustful of those who manage them, and---eventually---incapable of determining their own destinies."[4] Public awareness of the information and reasons behind decisions can improve support and reduce misunderstandings and dissatisfaction. The public can also better participate in the process when they have information about the activities of

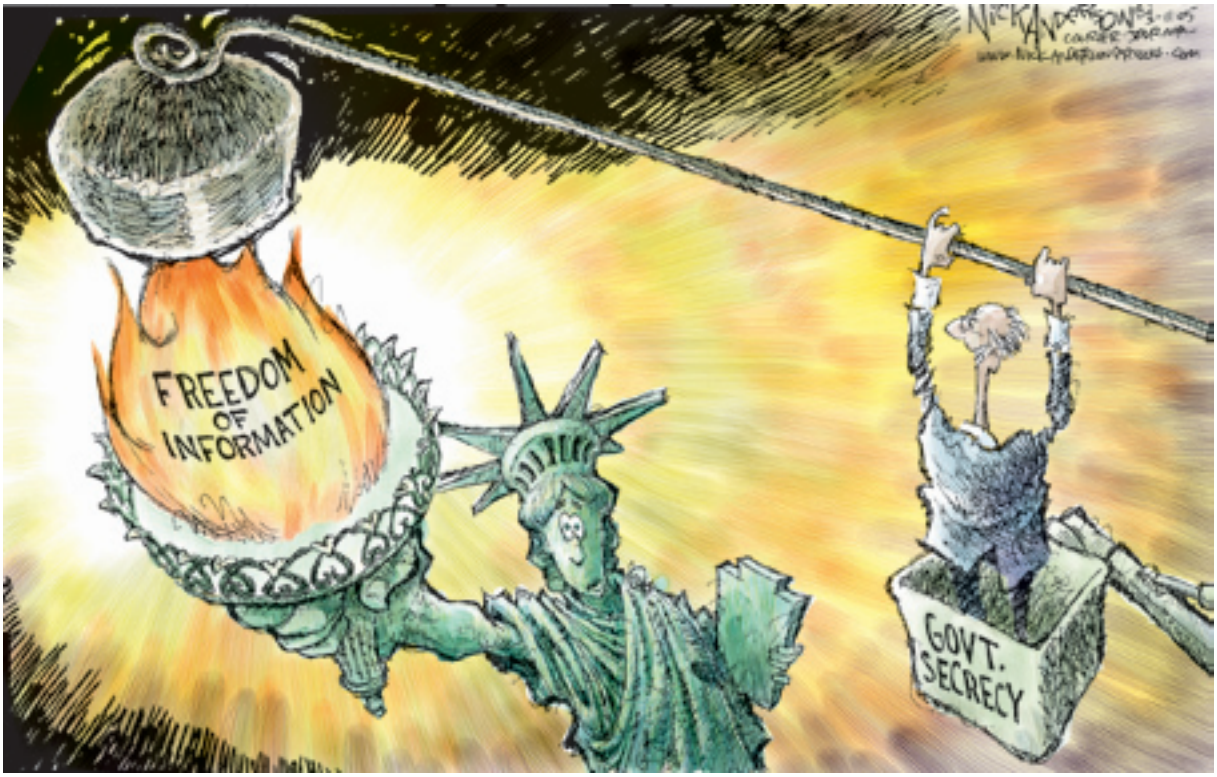
the government. Confidence in the government is also improved if it is known that the decisions will be predictable.

Openness fights corruption and mismanagement. As the future President Woodrow Wilson said in 1913, "Everybody knows that corruption thrives in secret places, and avoids public places, and we believe it a fair presumption that secrecy means impropriety. So, our honest politicians and our honorable corporation heads owe it to their reputations to bring their activities out into the open."[5] Billions of dollars are spent every year by the federal government. Openness in public spending makes it possible for representatives and citizens to monitor their government actions and publicize poor spending. The public controversy over "The Bridge to Nowhere" and other earmarks show that public rebuke is often more powerful than the Congressional appropriations process. Billions misspent and wasted in Iraq and in the cleanup of Katrina have been revealed; armed with this knowledge, citizens can demand meaningful reforms from their government. Billions have been recovered by whistleblowers in the past ten years.

Openness prevents abuses. As Justice Louis Brandeis said, "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[6] Government officials are less likely to abuse their power if they believe the abuse wil be exposed. At a minimum, officials will stop abuses, once they become public. The revelations of abuses of detainees in Iraq and of domestic surveillance in the U.S. show that the spotlight of public scrutiny can force changes when internal administrative processes and Congressional oversight fail.

Openness promotes government efficiency. Openness allows government agencies to better share information and learn lessons. Sharing reduces redundant efforts and allows better analysis. Overspending and double spending can be reduced. The 9/11 Commission found that the lack of sharing among government agencies was one of the reasons the plot was able to succeed.

Openness helps individuals protect themselves. An open system of law allows individuals to know their rights and responsibilities. Each year, millions of veterans access their records held by the federal government to help determine their disabilities. Local citizens and municipalities can better protect themselves from chemical hazards. Openness could have helped the dozens who have died in the aftermath of 9/11 due to respiratory problems around the site of the World Trade Center.



Openness promotes scientific innovation and development. Information sharing between scientists and others allows for greater innovation. Many of the most significant technical developments in the past thirty years, including the Internet, have come out of open scientific research sponsored by the government. These developments have substantially benefited the U.S. economically. Today, many areas of new scientific development such as genetics are based on government- sponsored projects. Information sharing can also be a benefit in protecting the national defense, as sharing can lead to faster breakthroughs in areas such as cures or developments of immunizations for the flu virus and other biological threats.

Openness can be used as an alternative to regulations. Over half of the release of toxic materials – millions of tons of pollutants – have been reduced due to public availability of information on pollutants.[7] Consumers are better able to make decisions on products when information, such as safety and reliability, are made available.

Openness improves the stability of markets. Millions of investors use the public filings of companies to evaluate their financial worthiness. Money can then be invested in well-managed companies with innovative ideas rather than only those with the best public relations and slickest brochures. The markets can also act more fairly. Better general access to financial information makes secret deals and monopolies more difficult.

THE HISTORY OF OPENNESS IN THE U.S.

As the initial statements show, many of the founding fathers recognized the power of information in promoting democracy. Along with a free press, government openness was seen as a necessity to promote trust.

Our system of government was not totally open originally and in many areas, such as foreign relations, there was great secrecy imposed by the executive branch. But there are many early examples of the openness of activities on the federal level. In 1813, Congress initiated the beginnings of the Federal Depository Library Program by requiring copies of its Journals to be sent to university and state libraries. As far back as 1816, the salaries of the employees in federal agencies were being published. Congress too opened its proceedings almost from the beginning and published them. In 1860, it created the Government Printing Office, which opened the day of Abraham Lincoln's inauguration. From the beginning, the judicial system was based on the English principle that an open court would ensure fairness and limit abuses.

The states have been at the forefront of providing information to citizens about their activities. Most states have provided information about local and police activities for over a century. In Wisconsin, the legislature in 1849 adopted a law on the openness of country records and meetings.[8] In Louisiana, the 1940 Public Records Act set up the first comprehensive system for the archiving and access to public records. Today, the states are still at the forefront as "laboratories of democracy," with many still trying innovative new ideas to promote openness later adopted by the federal government.

The development of the federal administrative state in the early 20th century led to a great concern about the transparency and accountability of the newly-created powerful federal administrative agencies. Within a short period of time, many large agencies were created and issued thousands of pages of orders and regulations with little organization. Even individuals working at the highest levels of government found it difficult or impossible to keep track of all of them. And for the regulated public, this new body of "executive legislation" was inaccessible and virtually hidden. [9]

In 1935, a case[10] that went to the Supreme Court revealed that the section of a rule under which a company was being prosecuted was omitted from the publication of the regulation. Soon thereafter, the Congress enacted a law ordering the creation of the Federal Register to publish all regulations in a systematic way.[11]

In 1946, the Administrative Procedures Act (APA), which was intended to regulate the activities of the agencies, was adopted. The law provided for a limited to right of access for those who were affected by agencies' decisions. A permissive provision in the law encouraged agencies to make more information about their activities available. Most, however, took a restrictive view and did not disclose information.

Starting in 1950s, Congress, led by Congressman John Moss (D-CA), began investigating the right of access and found that agencies did not make much information available. A campaign led by media organizations resulted finally in the 1966

Freedom of Information Act (FOIA). For the past 40 years, this Act, subsequently amended several times to enhance openness and supplemented with other laws, has stood as the pinnacle of openness for the public.

It has been supplemented by laws such as: the Government in the Sunshine Act to ensure that meetings of federal agencies headed by a collegial body, such as the Federal Communications Commission, are open to the public and minutes or transcripts are kept of the meetings; the Federal Advisory Committee Act which ensures that committees that advise the federal government are composed fairly and hold open meetings; and the Privacy Act, which allows individuals to obtain and correct their personal information in records held by federal bodies.

As new technologies have made the provision more easily available and increased demand by citizens to know more, the trend toward more openness has continued. In 1993, Congress enacted a law to require that the Federal Register be published in electronic form. In 1996, the Congress adopted the Electronic Freedom of Information Act to extend the FOIA to electronic records and to provide for more use of electronic resources. More recently, efforts to improve electronic government have increased both access to information and increased participation. ❖

2

The Darkening Cloud

Behind closed doors, there is no guarantee that the most basic of individual freedoms will be preserved. And as we enter the 21st Century, the great fear we have for our democracy is the enveloping culture of government secrecy and the corresponding distrust of government that follows.[12]

–FORMER SENATOR DANIEL PATRICK MOYNIHAN 2000

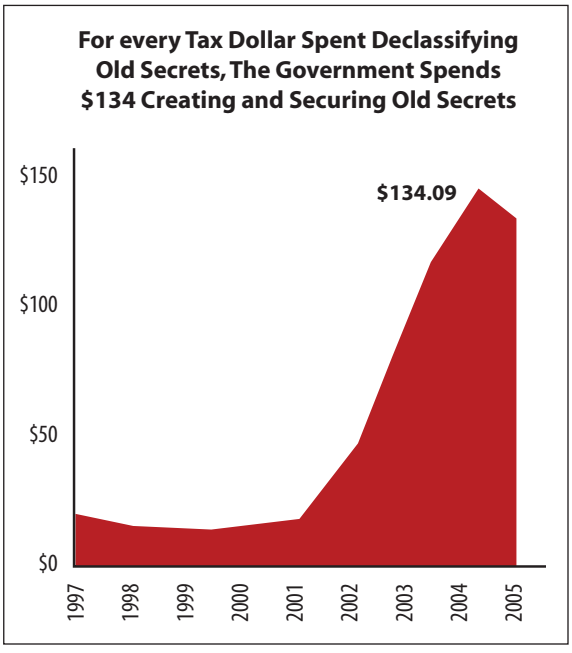
In the past six years, the basic principle of openness as the underpinning of democracy has been seriously undermined and distrust of government is on the rise.

The Administration has taken an extreme view of the power of the presidency. In its view, its powers to operate are largely unchecked by the Congress, courts, states, or the public. The number of secrets generated has substantially increased, while release of information has declined. New categories of semi-secret "sensitive" information proliferate while laws on access to information are undermined or ignored. Whistleblowers and journalists are threatened with jail while billions of dollars are squandered on secret contracts or incompetence. Scientists are gagged while propaganda and misinformation are released from the highest offices.

IT'S A SECRET: CLASSIFIED AND SEMI-CLASSIFIED INFORMATION

Classified information

The system of protecting information for national security reasons is out of control. Information is classified at an astounding rate. On an average day of the year, nearly 40,000 items (such as documents, files, or videos) – 15 million in 2004 and 14.2 million in 2005 – are classified by government officials and private contractors. This number has been increasing for the last ten years – up from 3.5 million in 1995; it has substantially increased in the last six years.



Problems with the classification system have been long recognized. In 1994, Congress approved the creation of the Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan. The Commission issued a detailed report in 1997 that found that the system for classified information was severely broken:

The result today is a system which neither protects nor releases national security information particularly well. Substantial concerns exist with respect to both the ability of the classification system to protect secrets effectively and the adequacy of the procedures in place to make information available to those outside the Government.[13]

The biggest problem is the prevalence of mis-classification and over-classification. It is estimated that between 10 percent and 90 percent of all documents are over-classified. Lee Hamilton, the Vice-Chair of the 9/11 Commission said that 70 percent of the classified information that he saw during the Inquiry was "needlessly classified." Reviews by the Government Accountability Office have found numerous problems with the classification levels and markings employed in agencies.[14]

Even government officials admit there are serious problems. Carol Haave, the Deputy Under-Secretary of Defense, testified in a Congressional hearing in 2004 that she believed that 50 percent of information was over-classified. At the same hearing, William Leonard, Director of the Information Security Oversight Office thought it was even higher. He noted that over-classification was "disturbingly increasing, where information is being classified that is clear, blatant violation of the order."[15] Former Central Intelligence Agency (CIA) Director (now Secretary of Defense) Robert Gates testified to the 9/11 Commission "We overclassify very badly."[16]

The U.S. Executive Order on Classification

The rules for classification of information for national security reasons are set by the U.S. Executive Order 12958 on Classified National Security Information originally issued by President Clinton in 1995 and amended by President Bush in 2003.[17] The Order sets out procedures on the classification of information including who can classify, under what standards they can do so, for how long information can be classified, and a process for its eventual declassification and release. There are a limited number of people who are authorized to create classified information (around 4,000 total) and they must mark each time why it is classified and for how long it needs to be protected.

There are eight categories of information that are eligible for classification:

(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), 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, which includes defense against transnational terrorism;
(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, which includes defense against transnational terrorism; or
(h) weapons of mass destruction.

Depending on the sensitivity of the information, there are three levels of classification:

- Top Secret - where unauthorized disclosure could be reasonably expected to cause exceptionally grave damage to the national security.
- Secret - where disclosure could be expected to cause serious damage to the national security.
- Confidential - disclosure could be expected to cause damage to the national security.

The E.O. prohibits the classification of information to "conceal violations of law, inefficiency, or administrative error, prevent embarrassment to a person, organization or agency, retain competition, or prevent or delay the release of information that does not require protection in the interest of national security information." It also prohibits the classification of basic scientific information not clearly related to national security. In practice, however, these prohibitions have often been unsuccessful, with information such as the report on the abuses from the Abu Ghraib prison being classified to prevent its release.[18]

The default period for information to be classified is ten years unless the person who issues the classification can identify an earlier date or event that would cause it to be available sooner, or makes a specific determination that it is sensitive to a later date. Since the adoption of the Clinton order, ap-

proximately fifty percent of all information is set for declassification in 10 years or less.

Changes to the Order by President Bush

The 2003 Bush Amendment (E.O. 13292) left the structure of the Clinton order mostly intact but significantly changed the presumptions about classification. It removed the requirement that, if there were a significant doubt about classification, it should not be classified. Expert Harry Hammit describes it as a "when in doubt, classify" standard. Other changes include:

- Set presumption that information in categories "shall" be considered for classification rather than "may" be classified.
- Expanded categories to include Information infrastructure, WMD, and terrorism.
- Allowed for easier reclassification of information.
- Removed presumption of 10 years for classification if no date can be determined.
- Eliminated requirement that each agency make plans for declassification.
- Extended the deadline for automatic declassification to December 2006.
- Allowed the CIA Director, unless overruled by President, to block decisions by the Interagency Security Classification Appeals Panel (ISCAP) to declassify information.
- Expanded protection of information provided by foreign governments.

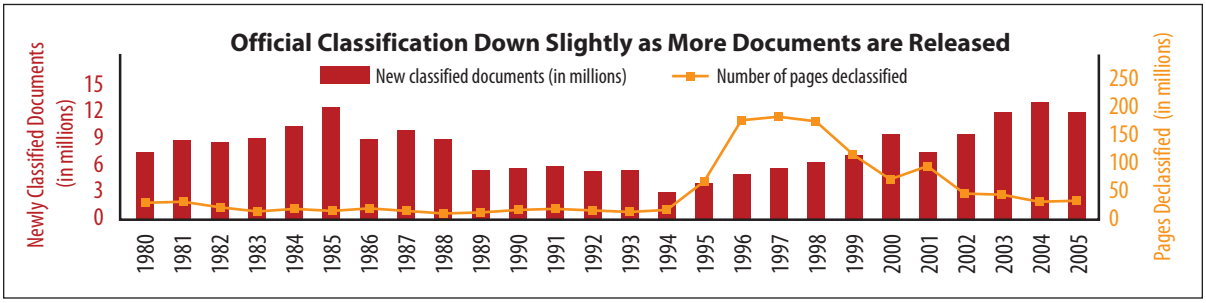
Declassification

The other, equally important, side of protecting classified information is ensuring that it is declassified and released once it is no longer sensitive. The Clinton Executive Order required, and the Bush order retained the requirement, that all information 25 years and older that has permanent historical value be automatically declassified, starting in December 2006 (originally set for 2000), unless it is specifically exempted and is subject to outside review. The Order created a new standard by placing the burden on the government agency to justify why the information should not be declassified, rather than why it should be.

The result of the order was the massive systematic review by agencies of their records. Between 1995 and 2001, one billion pages were reviewed and declassified, 200 million pages in 1997 alone. Since the beginning of the Bush Administration, that effort significantly declined, dropping below 30 million pages in 2004 and 2005.

Limited efforts have also occurred to declassify information in special areas where there was a compelling interest. Congress enacted two specialized laws on the access to files relating to the assassination of President John F Kennedy (following the movie JFK),[19] and to Nazi and Japanese war crimes[20] held by government agencies, including the intelligence services. Both Acts created review boards to collect and examine documents and decide on their release. Over four million pages were released, including thousands of previously classified records under the JFK Act.[21] Over eight million documents have been released under the war crimes laws.

However, the Administration has also often used selective declassification for political means. President Bush secretly declassified sections of a National Intelligence Estimate that supported its claims of weapons of mass destruction in Iraq. These were leaked to reporters by the Office of the Vice-President.[22] The Attorney General went before the 9/11 Commission with what Senator Leahy called a conveniently declassified memo to attack a Commissioner. In 2004, Secretary of State Rice quoted from a selectively declassified 2001 memo prepared for the National Security Council by then-counter-



Source: Information Security Oversight Office Compiled by OpenTheGovernment.org & National Security Archive

terrorism czar Richard Clarke.[23] It has also used it to stymie Congressional oversight of the Foreign Intelligence Surveillance Act and anti-terrorism policy.

A bill was introduced in the 109th Congress which would require notification to the Intelligence Committees when information was declassified.[24] In the 110th Congress, the House Intelligence Committee has already announced plans to investigate the practice of selective declassification.[25]

Now you see it, now you don't: Secret Reclassifications

As noted above, the Bush amendments to the Clinton Executive Order make it easier to reclassify information. Under the Clinton Order, information could not be reclassified if it had been declassified and released to the public. Now, information can be reclassified if the head of the agency determines that it is in the interest of national security, "the information may be reasonably recovered" and the Director of the Information Security Oversight Office (ISOO) is notified.

In 2006, it was discovered that over fifty-five thousand pages of records were secretly reclassified at the National Archives and the Presidential libraries under an agreement with the CIA and other agencies.[26] Many were documents that had never been classified in the first place or were already published by the State Department. Some were over 60 years old, such as the Korean War era assessments by the CIA that China was not likely to intervene in Korea two weeks before China entered the war. An ISOO audit of the files found that over one third were not even eligible for classification. It also found a "significant number of instances when records that were clearly inappropriate for continued classification were withdrawn from public access."[27] The U.S. Archivist apologized for the secret agreements, stating "There can never be a classified aspect to our mission. Classified agreements are the antithesis of our reason for being."[28]

The Administration is not the only party at fault in promoting excessive secrecy. In 1998, Congress ordered that the Department of Energy withdraw from public availability all of its recently declassified documents that might be related to the design of nuclear weapons, to ensure that improper declassification did not take place.[29] In all, the Department withheld and reviewed over 200 million pages. Only 6,640 pages containing classified information were found, mostly long-public material about the previous locations of weapons that are no longer sensitive. Many documents that were previously public were withheld, such as a 1971 Congressional briefing by Secretary of Defense Melvin Laird on Theatre Nuclear Forces and Strategic Forces, the numbers of weapons and bombers in the 1960s and 1970s, and agreements with the Canadian government from the 1960s.[30] The review has cost $22 million and delayed efforts by the DOE to continue its declassification effort.

Watching the Watchers: oversight of the classification system

The Information Security Oversight Office (ISOO)

An intelligent system of classification needs independent oversight to ensure that it is working. Under the Executive Order, the Information Security Oversight Office, a division of the National Archives, has general responsibility relating to the development and oversight of protections on classification and declassification of information. Its duties include:

- Implementing Directives, Instruction and Regulations
- Liaison, Inspections and General Oversight
- Statistical Collection, Analysis and Reporting
- Recommending Policy Changes

Each year, the ISOO collects statistics on the classification and declassification of information the previous year and presents a public document on the amount of classification and its estimated costs.

The ISOO's powers are limited, however. It audits and makes recommendations on agencies classification practices; the agencies, however, are not required to follow its guidelines and recommendations. This is why Senator Moynihan's Commission on Protecting and Reducing Government Secrecy recommended the creation of a National Declassification Center.

Missing in Action: The Public Interest Declassification Board

In 2000, Congress approved the creation of the Public Interest Declassification Board.[31] The board functions are to:

- Advise the President and other executive branch officials on classification and declassification process;
- Promote public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and significant U.S. national security activities;
- Provide recommendations to the President on declassification of information of extraordinary public interest; and
- Review and make recommendations to the President with respect to any Congressional request on declassification of information.

The board was the only recommendation of the Commission on Protecting and Reducing Government Secrecy that was adopted. To date, it has not been of much use. The board remained in a legal vacuum for over five years while the White House delayed appointing members and providing funding for it. It was not until 2005 that the President appointed members and it began to hold meetings.

Now that it is finally in place, the Board has already taken a very limited view of its own powers. In September 2006, members of the Senate Intelligence Committee asked the Board to review two committee reports on Iraq intelligence that had been classified by the Administration. The Chairman, L. Britt Snider, a former CIA Inspector General, responded that it could not review the classified documents unless it was asked to do so by the President. It recently announced that it plans to move ahead unless it hears from the President.

Go Away: The State Secrets Privilege

Another justification invoked by the government to deny access to information is the claim that the information is privileged as involving state secrets. The privilege was first recognized by the Supreme Court in a 1953 case where the widows and families of several civilians killed in the crash of an Air Force airplane conducting experiments sued under the Federal Torts Claims Act.[32]

The sources of the privilege are nebulous. It has been attributed to pre-constitutional powers, separation of powers, executive privilege and others.[33] Its scope is not well defined. In many cases, it allows the government to prevent courts from even evaluating the information before ruling on the merits. Some courts treat it as absolute and dismiss cases as soon as the privilege is invoked; others have rejected that view and demanded access to the records to ensure that they are actually state secrets.[34]

Over the years, the government has used this privilege controversially in many cases to shut down lawsuits against it and prevent having to defend against them. A recent review of the cases in the Po-

litical Science Quarterly notes "At present, it is costless for the president to assert a secrecy privilege: the overwhelming odds are that the assertion will be successful, and even if unsuccessful, the process of overturning claims of privilege is lengthy and the only potential cost of excessive claims of national security is in bad publicity."[35] Tom Blanton, Director of the National Security Archive, is more direct in his criticism: "State secrets privilege continues as a kind of the neutron bomb of whistleblower litigation. It leaves no plaintiff standing."

In the past six years, the privilege has been invoked over 20 times by the federal government to end court cases. These include:

RENDITIONS. Khaled El-Masri, a German citizen who was taken by the CIA in Macedonia and sent to Afghanistan where he was tortured for six months. El-Masri sued the CIA for an apology. The case was dismissed after the court ruled that the state secrets privilege was absolute. It was also successfully invoked in the case of Maher Arar, a Canadian on his way through New York back to Canada, who was sent to Syria where he was tortured. His case was also dismissed.

ILLEGAL SURVEILLANCE. In separate cases brought by the American Civil Liberties Union (ACLU), Electronic Frontier Foundation and the Center for Constitutional Rights on the warrantless surveillance by the National Security Agency, the government has invoked the state secrets privilege to demand that all of the cases be dismissed. In at least one case, the court has rejected the privilege.

WHISTLEBLOWERS. The privilege has been used to prevent former FBI translator Sibel Edmonds from challenging in court her dismissal from the FBI after revealing numerous problems with the translation division. The FBI's Inspector General found that she was improperly terminated and that her allegations were never properly investigated. She was also prevented from testifying in a civil suit brought by the families of victims of 9/11.

Keep away: It's Sensitive (but not classified)!

The growth in secrecy has not been limited just to classified information. In the past six years, there has been substantial growth in categories of information designated as "sensitive" and therefore restricted. Some of these categories have statutory authorization but, for the most part, these designations are made internally by each agency and have no legal authority.

While categories designating information sensitive have existed for at least thirty years in some form or another, their use appears to have dramatically expanded since March 2002 when White House Chief of Staff Andrew Card issued a memorandum to all agencies requiring review of their information with an eye to protect "information that could be misused to harm the security of our nation and the safety of our people," and urged the agencies to view FOIA exemptions broadly.[36] It is estimated that there are now more than 100 different designations for categories of sensitive information.

Some of the recent uses of sensitive information include:

- The prosecution of a Miami-based Transportation Security Administration (TSA) employee caught stealing baggage was dropped and local police officials are not allowed from publicly reporting on incidents in airports without permission of the TSA.[37]
- The DC government was not allowed to see information on trains that are allowed to travel through the District carrying hazardous cargoes.
- The Nuclear Regulatory Commission (NRC) attempted to suppress a report by the National Academy of Sciences that it did not agree with.
- Federal Energy Regulatory Commission (FERC) refused to share information about the safety of a proposed Liquid Natural Gas plan with the Connecticut Attorney General because it was Sensitive Energy Information.[38]
- Department of Homeland Security (DHS) cited it when it refused to name the new DHS ombudsman.[39]
- The TSA withheld information about information circulars that had been published in the 9/11 Commission report as sensitive, only releasing them after it was directly pointed that it was published in the 9/11 Commission report.

Currently, there are no government-wide procedures on how sensitive information is to be designated, who can impose it, how it is to be reviewed for release or its withholding appealed. A report sponsored by the Department of Defense noted in 2004 that the "status of sensitive information outside of the present classification system is murkier than ever ... Sensitive but unclassified data

is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used."[40] Representative Henry Waxman describes "sensitive" as, "a code word for embarrassing to senior officials".

The lack of standards results in overuse of the designations and greater restrictions on information both for internal use and for public availability. A 2006 Government Accountability Office review found over fifty different categories of information designated as sensitive, ranging from Sensitive Homeland Security Information, Sensitive but Unclassified, Law Enforcement Sensitive, to For Official Use Only.[41] The GAO found that, in different agencies, similar information was often being designated for control using different labels and procedures. It also found that few agencies provided adequate guidance, training or internal controls. The GAO concluded that "the lack of such recommended internal controls increases the risk that the designations will be misapplied. This could result in either unnecessarily restricting materials that could be shared or inadvertently releasing materials that should be restricted." Within departments such as Justice, the GAO found numerous procedural problems due to lack of formal policies, inadequate training, and poor oversight. In the FBI, any employee or contractor could designate information as sensitive even though the FBI had no guide and did not provide adequate training.[42]

A 2006 review by the National Security Archive of 37 major agencies and components found little consistency across government agencies.[43] Only eight of the agencies had legal authority to designate information as sensitive, while 24 were only following their own internal guidelines. Eleven had no policy at all. Nearly one-third of the policies allowed any employee to designate information as sensitive, but they did not set policies on how the markings could be removed, and only seven total set restrictions on how they can be designated. The review also found that policies set after 9/11 were "vague, open-ended or broadly applicable" compared with those before.

Even though the designations often have no official standing, agencies are more restrictive in many cases with such information when it is requested under FOIA.[44] The National Security Archive found that at least half of the agencies subject the information to greater review and more restrictions when requested under FOIA; only two made any attempts at ensuring that the restrictions were balanced with the public's right to know.[45]

The designation is also being used to create de facto secret laws. The 2002 Homeland Security Act allows the Department of Homeland Security to designate dozens of categories of information as sensitive. This includes DHS regulations that authorize requiring showing ID to get on a plane and who can be searched. Republican Congresswoman Helen Chenoweth-Hage was refused access onto a plane after she demanded unsuccessfully to be shown the legal authorization for being searched. When asked why the regulations were not shown, a TSA spokesman said "Because we don't have to ... That is called 'sensitive security information.' She's not allowed to see it, nor is anyone else."[46] In another case involving the no-fly list, a District Court found that the TSA used "frivolous claims of exemption" in designating the security policies as sensitive.[47]

In December 2005, the White House issued a memorandum ordering government-wide standardization of "procedures and standards for designating, marking, and handling SBU information."[48] Agencies were required to conduct reviews of their procedures for sensitive information and report to the Director of National Intelligence. An inter-agency working group led by the DNI was due to issue guidance by the end of 2006, but there are reports that it has been delayed due to controversy among agencies on which headings should be kept. A report in June 2006 from the DHS and DOJ was reported to be rejected by the White House because it "lacked substance".[49]

Congress has shown some recognition that sensitive information needs to be limited. In 2002, Congress required the President to come up with a government-wide definition of homeland security information.[50] The standards were never issued and might have been pre-empted by the December 2005 memorandum. In 2005 and 2006, a number of House and Senate Committees held hearings on Sensitive Security Information (SSI) and "Pseudo-classification." In 2006, Congress approved an amendment to the Department of Homeland Security Appropriations Act requiring that the DHS amend its regulations to review SSI information when requested under FOIA, declassify SSI for most information that is over three years old unless the DHS secretary "identifies a rational reason why the information must remain SSI," and allow access to

SSI by parties to lawsuits who need to access for the lawsuit, subject to restrictions on further disclosure.[51] These changes were not expected to make a substantive improvement to the overall problem, though, because of the limitation of the strictures to the DHS.

Propaganda and Dis-information

The dissemination of truthful information is essential to allow for an informed electorate and Congress. This has also been systematically disregarded in the past six years. The Administration has selectively released information, actively deceived Congress and the public, secretly hired journalists and released "news" videos and other similar activities.

Following 9/11, the White House instructed the EPA to tell the public that the air around Ground Zero was "safe," even though the EPA had not conducted full testing. The EPA's Office of the Inspector General issued a critical report in 2003, finding that the White House had "convinced EPA to add reassuring statements and delete cautionary ones."[52] The Mount Sinai Medical Center found that 70 percent of ground zero responders had some form of respiratory problem.[53] At least 75 police and firefighters have been found to have developed cancer and several have died.[54]

The administration has also engaged in active deception of Congress. When Congress was debating the cost of the changes to Medicare bill in 2004, it was told by the Administration that the total was going to be $395 billion. However, the Chief Actuary of Health and Human Services (HHS) was aware that the actual cost was over $720 billion and was told not to inform Congress of the actual cost. The White House claimed that it has a constitutional power to withhold information.[55]

Under federal law, spending money for "publicity or propaganda purposes" is prohibited.[56] However, there has been a series of incidents where the government has been paying for news articles or influencing journalists. In 2002, the Pentagon proposed the creation of an Office of Strategic Influence to influence media outlets to favor the United States. It was widely reported that the office would engage in misinformation and planting of stories in foreign media and on the Internet. The proposal was quickly killed off by the Pentagon following public outcry. However, in 2005, the LA Times revealed that U.S. military was secretly paying to have stories planted in the Iraqi press.[57]

The Education Department secretly paid conservative commentator Armstrong Williams $240,000 to promote the No Child Left Behind Act. The HHS produced videos that were intended to look like news stories promoting changes to Medicare which were unknowingly run on 40 television stations. The Governmental Accountability Office found that this was "covert propaganda" prohibited by law.

CLOSING DOORS

The Freedom from Information Act: Limiting the FOIA

The Freedom of Information Act (FOIA) is one of the most important pieces of legislation in ensuring that information is available to the public.[58] It has two principal functions. First, it requires that government agencies publish information about their activities. Second, it gives a legal right to any person to request information from federal government agencies. The FOIA sets a presumption that all persons have a right to know information about what the federal government is doing and the government has a legal obligation to tell them, subject to a few limited exemptions. Over 4 million requests were made in 2005 under the FOIA and the vast majority (over 90 percent, mostly personal files) were responded to in full.

The FOIA was signed by President Lyndon Baines Johnson on July 4, 1966 and went into effect in June 1967 after a fifteen year campaign by media and members of Congress to reduce secrecy in federal agencies. Prior to the FOIA coming into effect, agencies used a variety of different excuses, including an obscure 1798 "Housekeeping Statute" and a misreading of the Administrative Procedures Act, to deny access to information. The FOIA was substantially amended in 1974 over the veto of President Ford, in 1986, and in 1996 with the Electronic FOIA (E-FOIA) amendments.

The FOIA only applies to agencies of the executive branch of the federal government such as the Department of Homeland Security, the Environmental Protection Agency, the Department of Defense and the Department of Health and Human Services. It does not apply to the Congress, the federal courts, offices directly under the President such as the National Security Council, private contractors or state government bodies.[59] Any individual, without regard to interest, legal status or geographic location, can request records from the agencies.

There are nine exemptions under the FOIA. They are for:

- Classified information relating to the national defense or foreign policy;
- Internal personnel rules and practices of an agency;
- Information made secret by another statute;
- Confidential trade and business secrets;
- Internal and inter-agency communications;
- Personal information;
- Law enforcement;
- Financial institutions;
- Well and geologic information.

Most of these exemptions are discretionary (agencies may, but are neither required to release nor withhold information requested). The presumption overall is for the release of information and agencies can withhold it only if there is a good reason. The 1986 amendments to the law also allow agencies to refuse to confirm to existence of records if the information would interfere with a current secret criminal investigation, records about informants, and some classified and secret FBI intelligence or terrorism files.

A person denied information can first appeal internally to the agency to reconsider. A lawsuit can also be filed in the federal District court where the requestor resides or the U.S. District Court in Washington, DC. Several hundred law suits are filed each year.

For fees purposes, requestors can be broken down into three categories – commercial; educational or noncommercial scientific and news media (including public interest groups); and other. Commercial-use requestors are required to pay for all search, review and duplication costs; news media and representatives of scientific or educational organizations are required to pay for duplication of records of more than 100 pages. Requestors who are not commercial, news media, scientific or educational requesters are required to pay search costs for more than 2 hours and duplication costs for more than 100 pages.

Attempts by agencies to use the fees as a barrier have been increasing. The CIA in October 2005 began demanding search fees from public interest groups and the news media if it determined that the information requested was not "important enough news" to justify a waiver.

E-FOIA

In 1996, the U.S. Congress adopted the Electronic FOIA (E-FOIA) Act, the most significant amendment to the FOIA since 1974. The primary goal of the E-FOIA was to improve how agencies handled electronic information related to FOIA requests. This included a specific recognition that requests for electronic information were to be treated in the same way as requests for physical documents, and greater obligations for publishing information online and accepting electronic requests.

However, the requirements have not been fully implemented more than ten years after the adoption of the Act. Many agencies still do not have adequate web sites with Electronic Reading Rooms or accept electronic requests for information.

Problems

The chilling of FOIA in the Bush Administration began nearly from its outset. In October 2001, Attorney General John Ashcroft issued a memo on FOIA that substantially undermined the presumption of openness.[60] The memo encouraged agencies to limit disclosure of information, ordering them to "carefully consider" interests including national security, business information, and personal privacy before allowing the release of any information. The agencies were told that the Justice Department would defend them in court except in the most extreme cases. The DOJ then issued guidance suggesting expanded views on exemptions such as privacy and internal agency rules and practices. This substantially changed the presumption of the previous order issued by Attorney General Reno. That order created a presumption of openness and stated that the DOJ would only defend agencies if a "foreseeable harm" existed, not if there were only a substantial legal basis (the standard under the 2001 order).

Following the 2001 memo, studies have found that the number of exemptions cited expanded greatly. The use of the privacy exemption has been especially aggressive.

Delays - Waiting until kingdom come

One of the most significant problems with the FOIA is the often long delays that occur in agencies providing information to requestors. The FOIA requires that agencies respond to requestors within 20 working days. However, there are no set dead-

lines for actually making the information available, rather the information must be provided "promptly". In some cases, requestors can wait years for the information that they requested. A review by the National Security Archive in 2006 found that the oldest request was 17 years old. The GAO found that the backlog of agencies requests had also increased from 2002 to 2005 by 14 percent.[61]

In part, this is a resource issue. Many agencies have not provided for enough resources to ensure that requests are responded to in a timely manner. But agencies know that unless a lawsuit is filed, they do not have to respond in a timely manner and many use that as a means to deny access.

Oversight

Another significant problem with the FOIA is the lack of a central authority to monitor and enforce it. Many U.S. states such as Connecticut, Florida, Hawaii, and New York (and over forty other countries) have appointed a Commission or ombudsman which has this task. The office can also play a proactive role in providing guidance and training to assist agencies.

The best the U.S. has is the FOI and Privacy Office in the Department of Justice. The DOJ provides guidance to agencies but its actual authority is limited to some administrative functions on annual reports. The Department also defends agencies who are sued but, under the Ashcroft memorandum, its duty is to defend in nearly all cases.

Proposals for Improvements

In the past several years, Congress has again been discussing improvement to the FOIA. Hearings were held and a number of bills were introduced and discussed by Committees in the House and the Senate in the 109th Congress.[62]

In December 2005, President Bush issued an executive order requiring agencies to improve their administration of FOI.[63] The order requires that each agency establish "citizen centered" policies that require that requestors are treated "courteously and appropriately" and agencies operate in a "results-oriented" manner. Specifically each Agency was required to:

- Designate a senior official as Chief FOIA Officer with overall power over agency compliance and implementation;
- Conduct a review of FOI operations and draft a plan for improvements including review of the use of information technology and reducing backlogs;
- Establish one or more FOIA Requester Service Center(s);
- Designate a FOIA Public Liaison to work with requestors.

It was widely suspected that the executive order was issued to undermine Congressional efforts to adopt amendments to the FOI to improve operations. Most of the requirements such as Chief FOI officers and Liaisons were already in place, and it does not address problems such as the 2001 Ashcroft memo that sets the default at withholding information rather than releasing it.

In October 2006, the Attorney General released the first report based on the implementation plans. The report presented a very rosy view of the Executive Order, calling it a "first of its kind FOIA executive order" and "the most significant administrative development in its history" and lauding it as an international standard. The order was described as having "an immediate and widespread positive effect on the operations of the federal agencies". It recommended minor changes to the administration including a meeting of Chief FOIA Officers, improvement of acknowledgement letters, a review of forms and better use of technology. A review of the same reports by the National Security Archive was much less cheery, saying that the review "fails to provide an honest assessment of where agencies' FOIA programs stand today." The review noted that many agencies have still not implemented the 1996 E-FOIA amendments; many plans rely on uncertain funding; there is a lack of recognition of the resources needed to resolve longstanding backlog problems; and there is a lack of any cross-agency authority for FOI.[64]

In March 2007, the House passed the "Freedom of Information Act Amendments of 2007" (H.R. 1309), and the "OPEN Government Act" (S. 849) was introduced in the Senate. S. 849 has passed out of the Judiciary Committee and is awaiting floor time for debate and a vote.

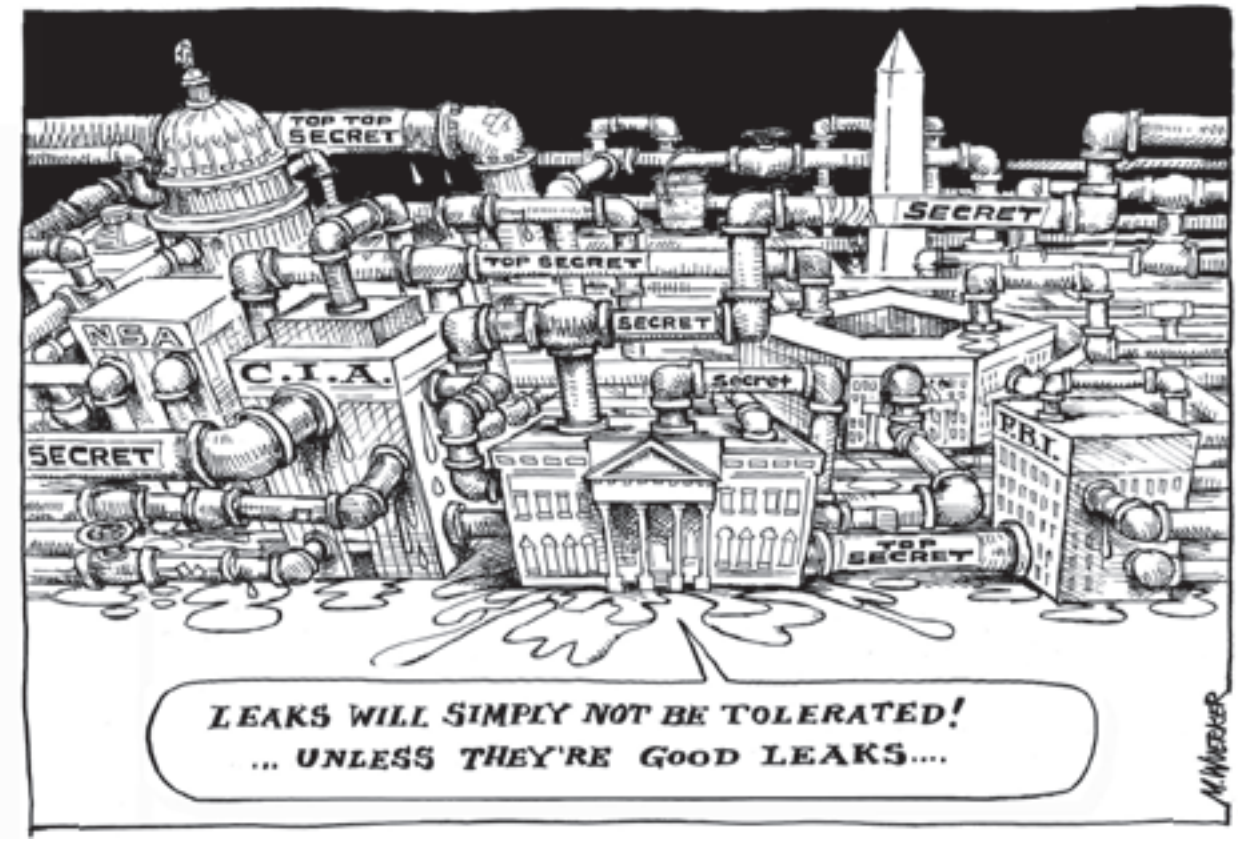
Executive Privilege

Underlying many of the Administration's claims for denying information is the belief that the Administration is not subject to most requests (even legal)

for information because its release would violate "executive privilege." The administration has from the beginning strongly worked to enhance its powers in relation to the other branches of government and the public. It has stated its belief that the Presidency should return to the (largely mythical) unchecked powers that it held before the Watergate era. As Bush told a press conference in 2002, "I'm not going to let Congress erode the power of the Executive Branch."[65]

Hiding from Congress

Starting in 2001, the Administration began using expansive claims of executive privilege to resist Congressional inquiries into a variety of areas, including the Boston FBI's misconduct in the 1960s that resulted in an innocent man being imprisoned for 30 years, Justice Department memorandums on campaign finance prosecutions, and copies of the President's Daily Brief relating to perceived terror threats prior to 9/11. Officials have claimed, under



The privilege comes from the constitutional separation of powers and is promoted to protect the advice given to presidents. Scholar Mark Rozell defines it as "the right of the president and high-level executive branch officers to withhold information from those who have compulsory power -- Congress and the courts (and therefore, ultimately, the public)."[66]

The claim was first made in the administration of George Washington, but it was not recognized by the courts until the 1950s. In cases such as the Watergate tapes and debates over the files of President Nixon, the Courts found that it is limited and diminishes over time.[67]

executive privilege, that they are immune from testifying before Congress and providing information. Instances include the activities of White House Counsel Alberto Gonzales when he was nominated for Attorney General, and Supreme Court nominee John Roberts' activities in the Justice Department.

The claim of executive privilege also has been used to stymie investigations by Congressional officers. The General Accounting Office (now the Government Accountability Office), the investigative arm of the Congress, was asked to review the activities of the 2001 task force on energy policy chaired by Vice-President Cheney, which had held a series of secret meetings. It was widely believed that these included meetings with controversial compa-

nies such as Enron. The GAO was asked to obtain information on the meetings, who participated and what was discussed. The Office of the Vice-President refused and in February 2002, for the first time ever, the GAO filed suit to enforce its powers. The case was dismissed in December 2002 after the court found that, as there was no personal injury to the GAO, it could not bring the case. It chose not to appeal the case.

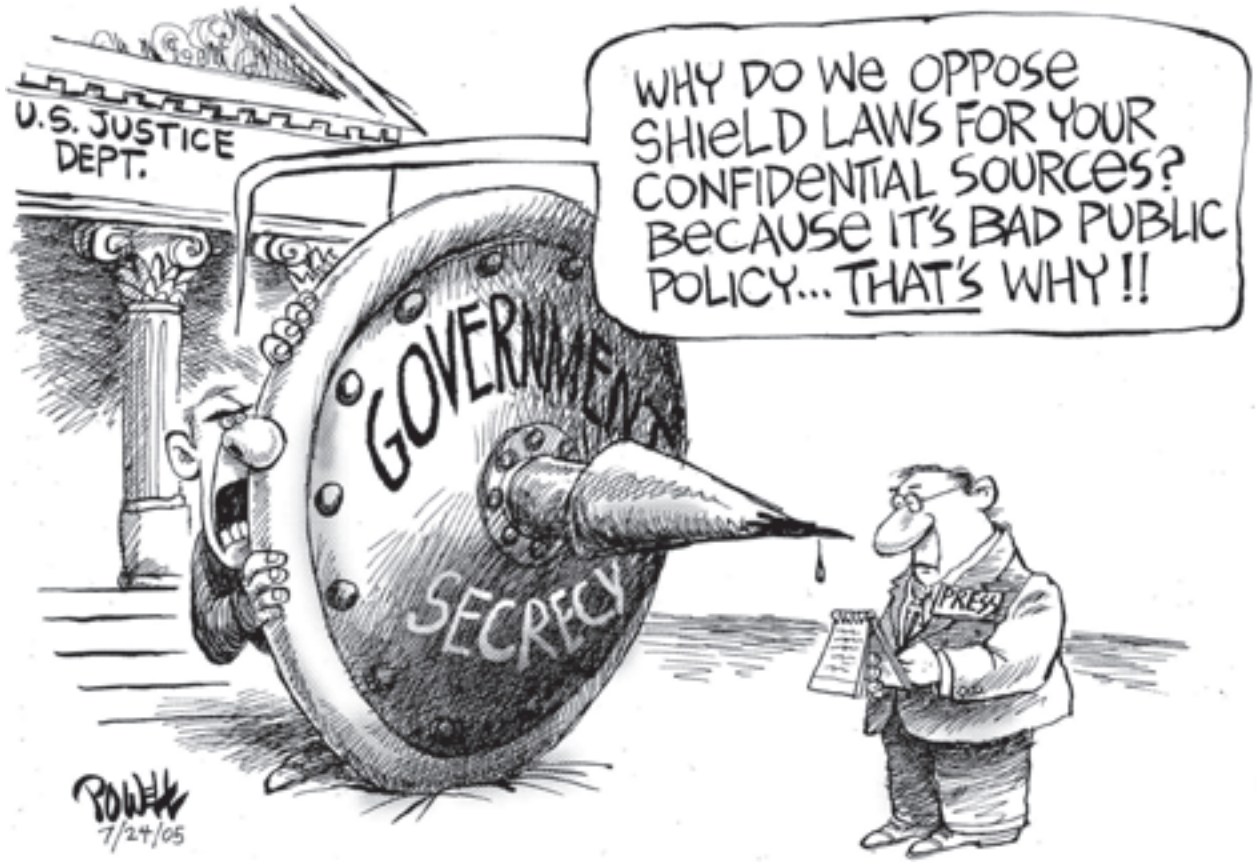
In June 2007, the House Oversight and Government Reform Committee released letters and other documentation showing the Vice-President asserting that his office was not bound by Executive Order 13292 on national security classification as it was not "an entity in the Executive Branch." This is an odd claim from an official asserting Executive Privilege.

The 110th Congress has sent numerous requests for documents to the White House, on such topics as the White House's involvement in the hiring and firing procedures of the Justice Department and the warrantless surveillance program first revealed in late 2006. The White House is responding with assertions of executive privilege, but the new Congress does not appear inclined to back down and accept these claims without a fight.

Accessing Presidential Records

Executive privilege is also being used to justify limiting access to the historical files of the past presidents. In 1978, following Watergate, the Congress enacted the Presidential Records Act.[68] The Act set the principle that presidential records are owned by the public rather than private property of the president and are to be maintained and made public by the National Archives. The law allows records to be kept sealed for 12 years and following that period to be made public subject to nearly all of the exemptions of the Freedom of Information Act. Under an Executive Order issued by President Reagan, the President and his predecessors were given 30 days notice when records were about to be released and the Archives was required to identify any records that would affect executive privilege.[69] The records would then be released unless the President or the previous president claimed privilege. Requestors could challenge the decision in court.

In November 2001, President Bush issued an Executive Order that restricted access to these records.[70] The new order revokes the Reagan order, and in the words of the House Committee on Government Reform, "converts the Act's presumption of disclosure into a presumption of non-disclosure." Under the new order:



- The release of information must be first approved by both the current and previous president even if privilege is not claimed.
- The current president can withhold documents even if the previous one disagrees.
- The current president must follow the wishes of the previous president to withhold "Absent compelling circumstances". The Archivist must follow the wishes of the former president and defend the withholding even if it is without merit.
- Persons who challenge the designation of executive privilege must show a "demonstrated, specific need" for the records.
- The former president can designate a friend or relative who can claim the privilege even after the former president is dead.
- Requests from the public must be responded to in 90 days but can be delayed indefinitely.
- The claim of executive privilege was extended to the Vice-President.

The American Historical Association and other groups filed a lawsuit in 2002 challenging the order as violating the law. The suit is still pending.[71] Several bills were introduced in the House and Senate in the 109th Congresses and gathered bi-partisan support, but were not adopted.

In March 2007, the Presidential Records Act Amendments of 2007 was introduced in both the House (H.R. 1255) and the Senate (S. 886). It passed the House on March 14th and was passed out of the Senate Homeland Security and Governmental Affairs Committee in June. It is awaiting a floor vote.

Closing the Courthouse Doors

Americans have a long-held presumption that trials are to be open. The Supreme Court has described open courtrooms as "recognized as an indispensable attribute of an Anglo-American trial" as far back in history as could be found.[72] However, the same cloud of secrecy that has enveloped the executive branch has been advancing on the judicial branch.

Since 9/11, information about cases has become increasingly difficult to obtain. Individuals have been detained secretly, often held for months on immigration-related charges without any notice to their families or being given a chance to obtain legal representation, hearings have been closed, and filings and briefs have been sealed.

In September 2001, Chief Immigration Judge Michael Creppy (an employee of the Justice Department, not an independent judge) issued a memorandum ordering that immigration hearings in "special interest cases" be closed and prohibiting disclosure of information about the cases to anyone but employees and the person's lawyers.[73] Over 700 people were designated as "special interest cases" and of these 500 were deported.[74]

The closed hearings were challenged in several cases. The U.S. Court of Appeals for the 6th Circuit found that the rules were unconstitutional, decreeing "Democracies die behind closed doors….When government begins closing doors, it selectively controls information rightfully belonging to the people. Selective information is misinformation."[75] In the 3rd Circuit, however, the court ruled for closure of the hearings, finding that immigration cases did not have a long history of openness; the court gave "great deference to Executive expertise".

The secrecy is not limited to immigration hearings, though. Court hearings relating to national security or terrorism are also being regularly closed, and gag orders are being placed on lawyers to prevent them from discussing what is happening to their clients. Briefs and decisions issued at the district and appeals level are classified or redacted without any limits. In a case involving a challenge to the PATRIOT Act, the Justice Department even blacked out a quote in an ACLU brief from a 1972 U.S. Supreme Court case that said, "The danger to political dissent is acute where the government attempts to act under so vague a concept as the power to protect domestic security. Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."[76]

Many cases are not even appearing on dockets. In 2005, People for the American Way filed a FOIA request with the Justice Department asking how many cases have been completely closed. The DOJ demanded that PFAW pay almost $400,000 and then rejected the request as too burdensome, saying that the practice was common and that it did not keep track of the records. A DC Federal Court ordered the DOJ to conduct the searches.

Nor is the secrecy limited to national security related cases. The Justice Department is currently attempting to close the hearings of the U.S. Court of Federal Claims on whether the drug Thimerosal causes autism. The HHS has requested that all the evidence be sealed and not be provided to the

families or the press.[77] In a recent prosecution of an employee of Coca-Cola, the prosecution recommending using the procedures developed to protect classified information against the defense.

GAGGING THE INSIDERS: PUBLIC EMPLOYEES

As secrecy in the administration has become more severe, the importance of whistleblowers has grown. These insiders, often government officials who are dismayed by the activities of their fellow

officials, can be invaluable in revealing to the public information essential to the public interest that otherwise never would have seen the light of day. Some of the recent important stories they have revealed include:

- The existence of the National Security Agency policy of warrantless wiretapping of telephone calls between the U.S. and foreign countries.
- Abuses at Abu Ghraib prison.
- The existence of CIA rendition and torture centers.
- The substantial no-bid contracts given to Halliburton and other defense contractors and price gouging by the companies.

The number of times the administration has started investigations into leaks has also substantially increased. A recent FOIA request by the New York Sun found that 94 investigations of leaks of classified information were started between 2001 and 2006.

Gag rules

In general, public employees have the same First Amendment rights of free speech as other citizens. However, these rights can be limited in some circumstances to "promote the efficiency of public services".[78] This is especially true relating to classified information obtained while employed by the government.[79] The CIA and other agencies have the power to review all materials that the employee or former employee wish to publish and censor them.

There has been an increase in efforts to prevent public employees, especially scientists, from presenting to the public information which challenges the views of the administration, especially relating to climate change.[80] At NASA, a junior political appointee with no scientific background[81] ordered the Director at the Goddard Institute for Space Studies to not speak to conferences or the media. At the U.S. Geological Survey, scientists must obtain preapproval of all presentations, reports or other public releases of any material that has "findings or data that may be especially newsworthy, have an impact on government policy, or contradict previous public understanding".[82] The Department of State Inspector General found, at the Bureau of International Informational Programs, a "virtual censorship" of speakers who were vetted.[83]

The designation of "sensitive" information (see above for discussion) is also being used to restrict employees' ability to disclose information of serious public interest. Employees of Wackenhut Corporation, which provides Transport Security Administration screeners, were required in April 2006 to sign non-disclosure agreements after several publicly revealed security problems at DHS headquarters.[84] A federal marshal was fired in 2003 for releasing TSA plans to limit marshals on long distance flights. The disclosure led to Congressional and public criticism and a reversal of the plan. In May 2004, the DHS proposed requiring all 180,000 employees and contractors to sign an agreement[85] to not disclose any information designated as sensitive, including even information that could be released under FOIA. The employees would also be subject to random searches as a condition of employment. This order

was partially repealed in January 2005 following protests from employee unions, Congress and civil liberties groups. The policy is still in force, however, for contractors.

Plugging the Whistle

At the same time as the government is clamping down on employees' speech, there has been a substantial increase in public recognition of the importance of whistleblowing. In 2002, Time Magazine made three whistleblowers, including an FBI agent, their "Persons of the Year". However, the protections that are given to whistleblowers are often inadequate. Some common practices used against whistleblowers, as noted by the Project on Government Oversight (POGO), include:

- Taking away job duties so that the employee is marginalized.
- Taking away an employee's national security clearance so that he or she is effectively fired.
- Blacklisting an employee so that he or she is unable to find gainful employment.
- Conducting retaliatory investigations in order to divert attention from the waste, fraud, or abuse the whistleblower is trying to expose.
- Questioning a whistleblower's mental health, professional competence, or honesty.
- Setting the whistleblower up by giving impossible assignments or seeking to entrap him or her.
- Reassigning an employee geographically so he or she is unable to do the job.[86]

Whistleblower Protection Act

Federal whistleblower protection was first adopted in 1978 in the Civil Service Reform Act and was extended in 1989 and 1994.[87] The revised Act, now known as the Whistleblower Protection Act, is intended to protect federal employees from being punished when they make a disclosure of information relating to violations of laws, rules or regulations, gross mismanagement, gross waste of funds, abuses of authority, or substantial dangers to public health. Agencies are prohibited from making "prohibited personnel practices," such as discriminating on appointments, transfers, promotions, pay or benefits, or changes of duties, because an employee has blown the whistle.

Under the Act, the Office of Special Counsel (OSC) was set up as an independent investigative agency that takes complaints of "prohibited personnel practices," recommends corrective or disciplinary action, and brings cases for employees before the Merit Systems Protection Board. The OSC can also receive reports from whistleblowers about illegal or unlawful activities. Employees who are punished for whistleblowing can appeal to the Merit Systems Protection Board and then to the U.S. Court of Appeals.

Most observers believe that the WPA has not worked well at protecting public employees. Congressional committees and the Government Accountability Office have conducted a number of investigations into the effectiveness of the Whistleblower Protection Act and have found serious problems with the protections and enforcement of the Act.[88]

The OSC has been a major impediment to whistleblowers. It was criticized by the GAO in 2004 for allowing a huge backlog of cases.[89] During the backlog, OSC only found for the whistleblower in four percent of the cases. Following the GAO report, the OSC controversially "dumped" 1,000 cases without review. When various staff members complained, they were sent to offices far away on short notice or were forced to resign.[90] Appeals have been less than effective as well. Since 1999, whistleblowers have won only two cases at the Board, and the Court of Appeals has been widely criticized for limiting rights even after successive changes in the legislation.[91]

In the 109th Congress, several bills to improve whistleblower protections were discussed and approved in committees. However, nothing was enacted before the end of the session. Early in the 110th Congress, the House passed the "Whistleblower Protection Enhancement Act of 2007 (H.R. 985); it was referred to the Senate (S. 274) and passed out of the Senate Homeland Security and Governmental Affairs Committee in June. It is awaiting a floor vote.

National security whistleblowers

Even more problematic are the cases of whistleblowers who wish to reveal classified information. The 1999 Intelligence Community Whistleblower Protection Act allows intelligence employees to report misconduct by officials to the House and Senate Intelligence Committees and the agency's Inspector General. It provides little protection, however, for the employees. Threats have increased against whistleblowers who are revealing information on mismanagement of agencies such as the NSA and FBI and abuses by military contractors.[92]

First Amendment Protections

The right of a public employee to reveal abuses has also been undermined in the courts. The U.S. Supreme Court ruled in May 2006 that public employees who make statements about abuses they discovered while working were not protected by the Constitution.[93]

Official Secrets? The Espionage Act and other criminal statutes

The threat of jail for public employees and journalists who reveal information in the public interest is the ultimate penalty. While repressive countries like China and Russia routinely imprison citizens and journalists for disclosing embarrassing information that the governments claim is classified, the United States, with its strong protections of free speech, does not have an Official Secrets Act.

The closest law is the Espionage Act adopted in 1917[94]. The Act prohibits the unauthorized disclosure of classified defense information to enemy powers with the intent to harm the United States. When the law was being considered in 1917, the Congress on several occasions rejected efforts to include a broader prohibition on disclosure, expressing concern over the restrictions on free speech and the possible misuse of the discretionary power given to the President to determine what was classified.[95] It is generally accepted that this law does not apply to the publication of state secrets by newspapers and there has never been a prosecution of a newspaper in the history of the law.

In the nearly 90 years that the Act has been in place, there have been only a few cases under the law for non-espionage-related incidents. In the Pentagon Papers case, the government attempted to prevent the publication of a classified history of the Vietnam War that was leaked to the Congress and newspapers.[96] The Supreme Court refused to censor the papers, finding that the government had not met the heavy burden of justification – of "direct, immediate and irreparable damage to our Nation or its people" in ordering the withholding. The case against Daniel Ellsberg, the source of the material, failed due to the illegal searches conducted against him. In 1988, Samuel Morison, a navy intelligence analyst, was convicted and sentenced to two years in jail for providing satellite photographs of Soviet installations to Jane's Defense Weekly, which he worked for part time. He was pardoned by President Clinton in January 2001.

In the past several years, the barriers to using this law have been broken down. In an unprecedented prosecution, Steven Rosen and Keith Weissman, staff members of the American Israel Public Affairs Committee (AIPAC) are being tried under the Espionage Act for receiving information from a Defense Department employee.[97] Following the publication of stories on the National Security Agency's warrantless wiretapping of telephone calls, Attorney General Gonzales, Members of Congress, and a few conservative commentators called for the prosecution of the New York Times under the Espionage Act.[98] In December 2006, federal prosecutors in New York City cited the Espionage Act in demanding that the ACLU return all copies of a leaked memo on media policy on photographing detainees designated as "Secret". The subpoena was dropped following a court hearing where the judge rejected the government's bid to seal the hearing and expressed skepticism that the case was strong enough to go forward. The government subsequently declassified the document in full.

Attempts have been made in recent years to adopt an Official Secrets Act. In 2000, the Senate Intelligence Committee included a provision in the Intelligence Authorization Act that would have criminalized any unauthorized disclosure (disclosure by any person with authorized access to classified information to any person not allowed to see it) of information that the discloser could have reason to believe might be classified. The penalty was three years in jail. The bill was widely criticized by the media and by Democratic Senators. In November 2000, President Bill Clinton vetoed the bill saying that the "provision is overbroad and may unnecessarily chill legitimate activities that are at the heart of a democracy."[99] In 2006, the bill was reintroduced in the Senate by Senator Kit Bond (R-Mo) but gained little support and was not voted on before the end of the 109th Congress.[100]

Not all officials support such a new law. In 2002, Attorney General Ashcroft issued a report recommending against adopting new statutes on criminalizing disclosures finding that "current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified" and called for strong procedures for the identification of government employees who reveal information.[101]

These current laws include laws on general theft. The theft statutes have been used controversially to

penalize employees who leak information. In 2003, a Drug Enforcement Agency employee was convicted and sentenced to one year in prison under the federal anti-theft statute for providing unclassified information to the UK's The Times newspaper on Lord Ashcroft, the UK Conservative Party treasurer, whose bank in Belize might have been involved in money laundering.[102]

Attacking the Messenger: the Media and Protection of Sources

The media is a crucial partner in ensuring that information from insiders is publicized. However, in order for many of these sources to come forward, reporters must promise that their identities will not be revealed, for fear of retaliation. As Justice Potter Stewart once wrote, "When neither the reporter nor his source can rely on the shield of confidentiality against unrestrained use of the grand jury's subpoena power, valuable information will not be published and the public dialogue will inevitably be impoverished."

The remedy for this situation is a legal recognition that journalists and those who work with them have a privilege similar to a doctor/patient or attorney/client, to not have to reveal the identities of their sources, or provide unpublished works and other information related the journalist's work when they promise their sources that they will not do so. This right was first adopted by the Maryland General Assembly in 1896. It is widely recognized on the state level with 31 states and DC adopting specific "shield laws" to protect these sources. In nearly all the other states, the courts have recognized a right based on common law or the state constitution.[103]

There is no recognition of this right, however, at the federal level. The Supreme Court ruled in 1973 that there is no constitutional right of journalists to not testify before a grand jury.[104] The court was sharply divided and, since then, many federal courts have found a limited privilege based on the different opinions in the decision.

Until recently, attacks on journalists to force them to reveal their sources or testify in court proceedings were relatively rare over the last 25 years. Under long-standing Attorney General's Guidelines, federal prosecutors required the permission of the Attorney General. It could be sought and given only in cases where the information sought must be essential to the investigation and not peripheral, nonessential or speculative. Reasonable attempts to obtain the information from alternative sources must also be attempted.

In the last six years, there has been a boom of cases where prosecutors have demanded that journalists disclose their sources for a variety of reasons. In many of the cases, there has been very little point for forcing the disclosure except as a punitive assault on the reporters who published it.[105]

In the 109th Congress, a number of bi-partisan bills were introduced in the House and the Senate to provide at least a qualified privilege. In May 2007, the "Free Flow of Information Act of 2007" was introduced in both the House (H.R. 2102) and the Senate (S. 1267). ❖

3

Opportunities for Public Access and Participation in a Digital Age

The past fifteen years have seen significant changes in how government agencies operate, due to the widespread adoption of information and communications technologies (ICTs) such as desktop computers and the Internet. They have improved the way government works and opened new opportunities for citizens to follow and participate in government activities. The technologies can also significantly improve citizen access to government information. Information that once was difficult and time-consuming to collect, analyze, and distribute can now be easily made available inexpensively to anyone who wants it.

However, electronic government also creates new challenges. These include ensuring that access is available to everyone equally, and that the increased volume of information being created electronically is going to be kept for future generations to be able to find and use.

ELECTRONIC GOVERNMENT

For over a decade, electronic government (E-government) has held the promise of providing more responsive and efficient government. There are three major components to E-government: E-information - the making of public information available electronically to the public; E-governance – the use of technologies to facilitate consultations, voting and other democratic activities; and E-services – the better providing of government services using technologies.

The use of E-government has been steadily increasing as more Americans go online. A 2004 study by the Pew Foundation found that 77 percent of Internet users (97 million Americans) had used the Internet to obtain information from or to contact government agencies. Internet users are much more likely to contact government offices than non-Internet users and report a higher level of success in their interaction with the government.[106] Still, the situation is not ideal; 46 percent of those who contact the government through the Web reported a problem.

The E-Government Act of 2002 sets a variety of standards on electronic rulemaking, records management, digital signatures, web sites standards and other E-government initiatives.[107] The lead government agency for electronic government is the Office of Management and Budget (OMB), which through the Office of Information and Regulatory Affairs, has long been involved in information policy. The E-Government Act created an Office of Electronic Government at OMB and also requires the OMB to issue policies to organize information to facilitate searching of information across the government.[108]

Access to government information online

Information technologies can be extremely powerful at providing access to government information online to facilitate the understanding of how government is working. Every Congressman, Senator and Congressional Committee and federal agency has a web site and many maintain multiple sites which provide extensive information about their activities.

Much more needs to be done, though. Government web sites are complex and often self-serving. Information appears and disappears. Many are formatted in such a way that access to raw information for analysis is limited. Public access advocates have asked for years for better management of the government's information, and now companies such as Google are asking agencies to design the databases to allow for better indexing by their search engines.[109]

The following are some examples of information that is available to the public which is used to promote oversight and accountability:

Legislation and regulations

For nearly 150 years, the Government Printing Office has published and made available to the public information such as the texts of laws, the Federal Register, the Congressional Record and important government documents such as the report of the 9/11 Commission. The Federal Depository Library Program places government documents in over 1200 libraries in all 50 states to ensure that citizens have access to the documents.

Electronic publication has steadily increased access to the information available. In 1993, Congress enacted the Government Printing Office Electronic Information Enhancement Act to put an index of documents, the Federal Register, Congressional Record and other records online and act as a depository online.[110] It now maintains thousands of databases and government documents online, available for free. Millions of records are accessed each month.

In 1995, the Library of Congress launched the THOMAS system to allow for citizens to easily and freely obtain legislative information. The system gives access to bills, committee and floor schedules, votes on specific bills, hearings, reports and other related information. It received over 150 million hits in FY 2004.[111]

It is often difficult for citizens to be able to effectively follow what is going on in the government and Congress, however, and many areas where information is still difficult to find. There has already been some consideration in the 110th Congress about making more information about lobbyists, campaign financing and travel available. The Open House Project is examining other areas such as Congressional Research Service reports, Congressional Committee transcripts and votes, archiving Congressional web sites, and making changes to

bills available publicly in an understandable format.[112] ReadtheBill.org is calling on the Congress to enact a "72 hours online rule" to ensure that all bills and conference reports are available before they are voted on to give time for members of Congress and the public to review legislation before it is approved.[113]

Electronic Budget Info

In FY 2006, the total budget of the U.S. was 2.7 trillion dollars. According to the CRS, over 1 trillion dollars per year is given in the form of contracts, grants or loans.[114] Public accountability can reduce money spent for frivolous or wasteful projects such as the infamous Alaskan "Bridge to Nowhere," or lost though mismanagement and poor contracting in Iraq and following Hurricane Katrina. The U.S. has historically had a reasonably open process but the complexity of procurement and spending, increased secrecy, and attempts to limit the powers of agency Inspectors General have lessened that. The International Budget Project ranked the U.S. as the sixth most open country in the world of 59 countries, below France, the United Kingdom, New Zealand, South Africa and Slovenia.[115]

One of the most innovative developments in the past five years in both access to information and electronic government was the adoption of the Federal Funding Accountability and Transparency Act in 2006. The law was enacted with overwhelming bi-partisan support in the House and the Senate and by over 150 groups from across the political spectrum.

The Act requires that the OMB create a new online database with a "searchable website" about organizations that receive contracts, grants or loans from the federal government by January 2008. This is to expand to include credit card transactions, subcontractors and subgrantees by January 2009. The information will include a description of purpose of the spending, the amount, and the Congressional district benefiting.[116] Any person or group will be able to search to see who received money from the federal government and for what purpose.

Concerns have already been expressed that the underlying information may be unreliable. The OMB database will use information from the Federal Procurement Data System (FPDS), Federal Assistance Award Data System (FAADS), and Grants.gov. The GAO in 2003 and 2005 expressed concern over the timeliness and accuracy of the FPDS[117] and found similar problems with FAADS. There was also concern over the General Services Administration (GSA) initially blocking access to federal contracting data. After years of managing a database on federal contracts, called the Federal Procurement Database System (FPDS), the GSA contracted out the responsibility. The GSA initially denied FOIA requests for the data, claiming that, as the contractor also took over collecting the data, GSA did not have the database anymore, and that, instead, the data would have to be purchased from the private contractor. Eventually, GSA backed off this controversial position and began having the contractor provide raw data to those requesting it, free of charge.[118]

Corporate Activities

The federal government also collects and disseminates information about activities of private corporations in many areas including the environment, financial records and consumer protection.

Environment

In 1986, following the releases of deadly methyl isocyanate gas in Bhopal, India killing thousands, and in Institute, West Virginia injuring hundreds, the U.S. Congress enacted the Emergency Planning and Community Right to Know Act.

The law requires that companies provide information to state agencies and the Environmental Protection Agency on toxic chemicals that they use or release into the environment. The EPA is required to maintain a Toxic Release Inventory (TRI) and make that information widely public using information technology. The information is available online and citizens can type in their zip code and obtain information about the releases in their areas.

The data has many users: civil society groups have combined this data with other records to create comprehensive search engines for use by citizens groups;[119] the EPA uses the data in developing regulations; and even companies use it to determine where they should focus their efforts on reducing pollution. The TRI is considered to have successfully reduced the amount of toxic materials released in the U.S. by nearly half.[120]

As mentioned in the previous chapter, the EPA decided in December 2006 to limit the usefulness of the TRI by raising the threshold of pollution that is to be allowed before the companies must notify the public.

Finances

One of the earliest efforts to use ICTs to disseminate information was the Security and Exchange Commission's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.[121] The system allows investors and others to examine filings made by public companies. It is also used by companies to create extended databases and tools to assist investors. Starting in the 1990's, the system was put online. The SEC reports that it was searched nearly 400 million times in FY 2005. In 2005, the SEC began releasing publicly its Staff Comment letters without requiring a FOIA request.[122]

Consumer Information

Other important information that is collected and is in some part made public includes the safety of toys and consumer products, autos and food. One of the first federal information laws was the 1958 Automotive Information Disclosure Act which required car companies to place price stickers on new cars.[123] On the other hand, the FCC in 2004 overturned a ten-year-old policy and refused to release information on how often land line and cell phone companies have outages, claiming that the release of the information would help terrorists and harm the companies.[124]

E-Rulemaking

One area where there has been significant progress is in the development of using ICTs to facilitate public participation in developing federal rules (e-rulemaking). Each year, 8,000 rules are created by federal agencies and departments. The standards for rules are set by the Administrative Procedures Act of 1946, which determines the process that the agency must follow in developing regulations based on the principles of information, participation, and accountability.[125] In a typical rulemaking, the agency will publish a Notice of Proposed Rulemaking in the Federal Register and solicit public comments for a set period. After the period, the agency will review the submissions and publish a final rule and response to the comments. The rule can be challenged in court, if it is believed that the agency created it without justification or that it failed to follow the requirements of the enabling legislation.

There has been a gradual move to holding rulemakings online. It is generally believed that Internet rulemakings allow people to more easily identify rulemakings that affect them and to participate. The development of the rules themselves benefit from receiving input from a wider ranger of participants. The E-Government Act of 2002 requires that agencies create "electronic dockets" and receive comments via their websites on proposed rules.[126] In 2003 the regulations.gov website which gives access to the rulemakings published in the Federal Register was launched.

It is not clear whether e-rulemaking substantially improves citizen participation. The new systems often duplicate the existing processes that do not allow for much input into the process. In some cases, the lobby groups are the main beneficiaries.[127] Electronic submissions may also be treated less seriously by officials. The EPA decided in December 2006 to reduce the amount of information on chemicals released to the environment even after over 120,000 individuals, groups and state and local governments wrote letters opposing the proposal while only 34 supported it.[128]

E-participation

A more significant step would be the further development of using electronic networks not just to provide information, solicit comments or provide services but to increase public participation in governance beyond rulemaking. These could include holding online forums, running discussion lists through electronic mail or blog-type forums. There have been limited efforts to use these tools by federal departments thus far.

The use of such tools should not, of course, be allowed to circumvent the Federal Records Act, the Presidential Records Act, the Federal Advisory Committee Act or other accountability legislation and regulations.

CHALLENGES OF DIGITAL GOVERNMENT INFORMATION

Digital Divide

One barrier to e-government is adequate access to computers and networks. While there is steadily increasing use of the Internet, a significant portion of the population still lacks access. The number of adults with access to the Internet reached over 70 percent in 2006, but only 42 percent had access to high speed broadband.[129] The level of access is sig-

nificantly lower for those on limited incomes. Only 53 percent of those with household incomes under $30,000 per year had access.

Education or even willingness of individuals to use electronic services, especially those from older generations, is also a serious problem. Only 32 percent of those over 65 and only 40 percent of adults with less than a high school education use the Internet.[130] Language may also be a problem. There are also privacy and security concerns that cut across demographics and may limit demand for some services.

Digital-only access may also limit understanding. There has been a growing move toward only providing access in electronic form. In 2006, the EPA closed five libraries including its main library at EPA headquarters, and reduced the times at four others. There is concern that many of the resources in these libraries will not be converted to digital form to maintain access and will disappear.[131] It addition, the expert help provided by professional librarians may also be limited. Also in 2006, the Library of Congress also stopped collecting certain documents such as dissertations in exchange for access to a more limited commercial database.[132]

Thus, for the foreseeable future, any government information or services should ensure that all persons have equal and equitable access. The role of libraries, particularly public libraries, is very important here. According to a 2006 survey, nearly 100 percent of all libraries in the U.S. provide some form of public Internet access, up from on 20 percent in ten years.[133] The libraries are now often taking on the role of assisting people with using e-government sites. However, these libraries are funded usually by state budgets and are under constant financial pressures.

Disappearing documents and web sites

While electronic dissemination of information can facilitate the release and access to information, it can also make the job of making it disappear easier. Following 9/11, many agencies removed information from their web sites or blocked public access to information that was designated as "sensitive".

These included:[134]

- The United States Geological Survey ordered librarians to destroy a CD-ROM on water supplies.
- The Federal Aviation Administrative removed information on enforcement actions.
- The Environmental Protection Agency removed Risk Management Plans, chemical hazards, emergency contingency plans, and access to the largest database of environmental information.

A review in 2004 by the Rand Corporation of information removed from federal web sites found that most of the information was of little use to terrorists and was widely available elsewhere. It also found that the possible dangers needed to be balanced against the interests in pubic access such as informing people of potential dangers.[135]

In other cases, the government has been using expanded excuses of commercial confidentiality to justify the removal of information. In 2006, the Small Business Administration began pulling data from the Central Contractor Registry on the size of revenue of small companies after investigations using the data showed that many of the businesses given government contracts under the program were not eligible.[136]

Managing "Born Digital" Information

Each year, billions of electronic documents are created in federal agencies. More data than ever before is created or collected in email, databases and other electronic systems. Websites are developed, updated and merged. Previously physical archives are being converted to digital form. Document formats are increasing in number and complexity; the National Archives has found over 4,500 different types of files.[137] Many different programs and different systems are used to operate and manage them.

Determining what should be preserved and ensuring that it is maintained and indexed in a form that will be useful both for agencies now and for future generations are crucial problems. The entire "life cycle" of the information, from its creation to its disposal or permanent archiving, must be ensured. This must be understood to include the ability to access and use the data in its original format, or in other ways, over time.

Previously, letters and files were routinely kept based on a long-standing understanding on how to handle paper documents. But electronic documents have changed that. Archival systems of paper-based documents are designed to ensure that the documents will last at least 100 years. In

comparison, it is estimated that the typical life cycle for the technologies – the formats and systems on which the record or our government exists -- is now only 18 months. Management of these systems is still evolving, with very little consistency government-wide and virtually no oversight within the executive branch or from Congress. The challenges are monumental and they do not decrease if and as we ignore them. Popular Mechanics magazine has described this as a potential future "Digital Ice Age".

WHAT THE PUBLIC CAN DO

Activism/ organizing

The role of the Internet as a tool to promote grassroots democracy can be extremely powerful. Its developments has come more from private efforts then from government bodies. The web has allowed new groups such as MoveOn to better organize citizens in ways that were not possible before.

Many websites have emerged to assist citizens in better tracking the activities of government and Congress. It is now possible to track new legislation through GovTrack[138] or congressional travel[139] or spending.[140] Sites such as DocuTicker, beSpacific and the Federation of American Scientists locate and publish government documents and related reports on major issues.

Websites, blogs and Wikis are used by millions every day to share, comment and advocate. The Federal Funding Accountability and Transparency Act in 2006 was enacted due to citizen and public interest groups from a wide spectrum using the Internet to coordinate lobbying efforts to identify which Senators had placed secret holds on the law and pressure them to remove them. The use of networks of plane spotters allowed journalists to be able to track the flights of CIA aircraft used for "rendition" of prisoners to secrets prisons.[141]

Video is now widely available outside of the mainstream media or official channels though services such as YouTube and MySpace. The availably of these video sites makes it easier for citizen journalists to show abuses. During the 2006 political campaign, the video of Senator George Allen commenting on the race of his opponent's campaign worker seriously changed the tenor of the campaign and led to his defeat. The widely disseminated video of an UCLA student being Tasered and other videos of the LAPD using pepper spray on suspects forced the police and FBI to address abuses.[142]

Beyond sharing information, though, the public can join organizations and coalitions that promote openness and accountability. A partial list of such organizations is provided at the end of this report.

The public needs to hold the government's feet to the fire – through letters and meetings, in public forums, and at the ballot box. ❖

Appendix – List of Relevant Legislation

Atomic Energy Act of 1946

Classified Information Protection Act

Critical Infrastructure Information Act of 2002

Data Quality Act

E-Government Act of 2002

Espionage Act

The Federal Advisory Committee Act (FACA)

Emergency Planning & Community Right to Know Act

The Federal Funding Accountability and Transparency Act

Freedom of Information Act

Government in the Sunshine Act

Intelligence Community Whistleblower Protection Act

Intelligence Identities Protection Act

Invention Secrecy Act of 1951

Military Whistleblower Protection Act

National Security Act of 1947

Nazi War Crimes Disclosure Act of 1998 (PL 105-246)

NoFEAR Act of 2002

The President John F. Kennedy Assassination Records Collection Act of 1992

Presidential Records Act of 1978

Public Interest Declassification Act of 2000

Whistleblower Protection Act

Appendix - Resources

Books and Reports

Report of the Commission on Protecting and Reducing Government Secrecy, 1997
http://www.fas.org/sgp/library/moynihan/index.html

Hammitt et al, Litigation under the Federal Open Government Laws 2004 (EPIC 2004)

Alasdair Roberts, Blacked Out: Government Secrecy in the Information Act (Cambridge University Press 2006)

Louis Fisher, In the Name of National Security: Unchecked Presidential Power and the Reynolds Case (Kansas University Press 2006)

Patrice McDermott, Who Needs to Know? The State of Public Access to Federal Government Information (Bernan Press 2007)

David Banisar, Freedom of Information Around the World 2006, Privacy International.
http://www.privacyinternational.org/foi/survey

Susan Maret, On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Federal Government, October 2006.
http://www.fas.org/sgp/library/maret.pdf

Secrecy Report Card 2006, OpenTheGovernment.org
http://www.openthegovernment.org/otg/SRC2006.pdf

U.S. House Committee on Government Reform. Citizen's Guide on Using the Freedom of Information Act (2005)
http://www.fas.org/sgp/foia/citizen.html

Newsletters

Access Reports. http://www.accessreports.com

Policy and News Updates. http://www.openthegovernment.org

Privacy Times. http://www.privacytimes.com

Secrecy News. http://www.fas.org/blog/secrecy

The FOI Advocate. http://nfoic.org/advocate

Websites of FOI related Organizations and blogs

beSpacific. http://www.bespacific.com

The Brechner Center for Freedom of Information. http://brechner.org

Coalition of Journalists for Open Government. http://www.cjog.net

Cryptome. http://www.cryptome.org

Electronic Frontier Foundation FLAG Project. http://www.eff.org/flag

Electronic Privacy Information Center Open Government Page. http://www.epic.org/open_gov

Federation of American Scientists Secrecy Project. http://www.fas.org

The Freedom of Information Center. http://foi.missouri.edu

Government Accountability Project. http://www.whistleblower.org

The Memory Hole. http://www.thememoryhole.org

National Freedom of Information Coalition. http://nfoic.org

National Security Archive. http://www.gwu.edu/~nsaarchiv

OMB Watch. http://ombwatch.org

OpenTheGovernment.org http://www.openthegovernment.org

Project on Government Oversight. http://pogo.org

Public Citizen FOI Clearinghouse. http://www.citizen.org/litigation/free_info

The Reporters Committee for Freedom of the Press. http://www.rcfp.org

The Right-to-Know Network (RTK NET). http://rtknet.org

Society of Professional Journalists. http://spj.org/foi.asp

Sunlight Foundation http://www.sunlightfoundation.com

Sunshine in Government Initiative. http://www.sunshineingovernment.org

Transactional Records Access Clearinghouse (TRAC). http://trac.syr.edu

Federal Government Sites

Department of Justice Office of Information and Privacy. http://www.usdoj.gov/oip/oip.html

The Information Security Oversight Office (ISOO). http://www.archives.gov/isoo

U.S. Government Portal. http://www.usa.gov

GPO Access. http://www.gpoaccess.gov

Thomas. http://thomas.loc.gov

PACER. http://pacer.psc.uscourts.gov

Endnotes

[1] John Adams, A Dissertation on the Canon and Feudal Law, 1765. http://teachingamericanhistory.org/library/index.asp?document=43

[2] Patrick Henry, The Debates in the Convention of the Commonwealth of Virginia, on the Adoption of the Federal Constitution, June 9, 1788.

[3] Letter from James Madison to W. T. Barry, Aug. 4, 1822, in The Complete James Madison (Harper and Brothers, 1953). Cited in Wiggens, Freedom or Secrecy (Oxford University Press, 1956).

[4] Executive Order 11652 - Classification and Declassification of National Security Information and Material, June 8, 1972.

[5] Woodrow Wilson, The New Freedom: A Call For the Emancipation of the Generous Energies of a People 1913

[6] Louis D. Brandeis, "What Publicity Can Do," Other People's Money, p. 92 (1932). Quoted in Respectfully Quoted: A Dictionary of Quotations. 1989.

[7] See Gary Bass and Sean Moulton, The Public's Right to Know: A Case Study from the United States, in Calland and Tilley, The Right to Know, the Right to Live (ODAC, South Africa, 2002); OECD PRTR pages: http://www.oecd.org/env/prtr

[8] Reporters Committee for Freedom of the Press, Open Government Guide: Wisconsin, 5th Edition. http://www.rcfp.org/ogg/index.php?op=browse&state=WI

[9] The Office of the Federal Register. "A Brief History Commemorating the 70th Anniversary of the Publication of the First Issue of the Federal Register, March 14, 1936." http://www.archives.gov/federal-register/the-federal-register/history.pdf

[10] Panama Refining Co. v. Ryan, 293 U.S. 388 (1935).

[11] For a detailed review, see Lotte E. Feinberg, Mr. Justice Brandeis and the Creation of the Federal Register, Public Administrative Review, Vol 61, No 3, May/June 2001.

[12] United States Senators Daniel Patrick Moynihan and Ron Wyden, Secrecy in International and Domestic Policy Making: The Case for More Sunshine, October 2000. http://www.fas.org/sgp/library/wyden.html

[13] Report of the Commission on Protecting and Reducing Government Secrecy, Sen Doc 105-2. 1997. http://www.fas.org/sgp/library/moynihan/index.html

[14] GAO, Managing Sensitive Information: DOJ Needs a More Complete Staffing Strategy for Managing Classified Information and a Set of Internal Controls for Other Sensitive Information. GAO-07-83, October 2006; GAO, Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors, GAO-06-706.

[15] Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing, Hearing before the Subcommittee on National Security, Emerging Threats and International Relations, August 24, 2004.

[16] Secrecy News, Volume 2003, Issue No. 45, May 27, 2003.

[17] Executive Order 13292.

[18] Secrecy News, FAS Project on Government Secrecy. Volume 2004, Issue No. 42, May 5, 2004.

[19] President John F. Kennedy Assassination Records Collection Act of 1992, PL 102-526.

[20] Japanese Imperial Government Disclosure Act of 2000 December 6, 2000; Nazi War Crimes Disclosure Act. PL 105-246.

[21] Final Report of the Kennedy Assassination Records Review Board, 1998.

[22] Bush Ordered Declassification, Official Says, NY Times, April 10, 2006.

[23] John Prados, "Declassifixation," The New Republic, April 21, 2004.

[24] S. 2660.

[25] U.S. House of Representatives, Permanent Select Committee on Intelligence, Oversight Plan for the 110th Congress, February 7, 2007.

[26] U.S. Reclassifies Many Documents in Secret Review, NY Times, February 21, 2006; National Security Archive, Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program, February 21, 2006, http://www.gwu.edu/~nsaarchiv/NSAEBB/NSAEBB179/index.htm

[27] Information Security Oversight Office, Audit of the Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes, April 26, 2006. http://www.archives.gov/isoo/reports/2006-audit-report.html

[28] Press Release National Archives Releases Second Declassified MOU, April 17, 2006.

[29] The National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261.

[30] William Burr, How Many and Where Were the Nukes?", National Security Archive Electronic Briefing Book No. 197, August 18, 2006. http://www.gwu.edu/~nsaarchiv/NSAEBB/NSAEBB197/index.htm

[31] Title VII, FY 2001 Intelligence Authorization Act. It was amended in 2004 to hear appeals from Congressional committees on classification.

[32] U.S. v Reynolds, 245 US 1 (1953).

[33] See Chesney, Robert, "State Secrets and the Limits of National Security Litigation". George Washington Law Review, 2007 Available at SSRN: http://ssrn.com/abstract=946676

[34] For a very detailed analysis, see Louis Fisher, In the Name of National Security: Unchecked Presidential Power and the Reynolds Case, University Press of Kansas 2006.

[35] William G. Weaver and Robert M. Pallitto, State Secrets and Executive Power: Political Science Quarterly, Vol 120 No 1, 2005. p86.

[36] Memo from WH Chief of Staff Andrew Card on Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security, March 19, 2002.

[37] CRS "sensitive but Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, November 4, 2006. p35.

[38] Ibid p58.

[39] Ibid p64.

[40] Jason Program Office, MITRE, Horizontal Integration: Broader Access Models for Realizing Information Dominance", December 2004. p5. http://www.fas.org/irp/agency/dod/jason/classpol.pdf

[41] Government Accountability Office, Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information, GAO-06-385, March 2006.

[42] GAO, Managing Sensitive Information: DOJ Needs a More Complete Staffing Strategy for Managing Classified Information and a Set of Internal Controls for Other Sensitive Information. GAO-07-83, October 2006.

[43] National Security Archive, Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information, March 2006. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/press.htm

[44] CRS "Sensitive but Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, November 4, 2006.

[45] NSA report ibid p. 21.

[46] Steve Aftergood, The Secrets of Flight, Slate, Nov. 18, 2004.

[47] "No-Fly" Doesn't Fly, GovExec.com, June 24, 2004.

[48] White House, Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment, December 16, 2005.

[49] CRS Ibid, p16.

[50] The Homeland Security Act of 2002, PL 107-296 s 892.

[51] Department of Homeland Security Appropriations Act, 2007, PL 109-295, s. 525

[52] EPA Office of Inspector General, EPA's Response to the World Trade Center Collapse: Challenges, Successes, and Areas for Improvement, Report No. 2003-P-00012. http://www.epa.gov/oig/reports/2003/wtc/toc.htm

[53] EPA, NYC Blamed for 9/11 Health Problems, AP, September 8, 2006.

[54] Death by Dust, The Village Voice, November 28, 2006.

[55] See Fisher p23.

[56] See GAO, Principles of Federal Appropriations Law: Third Edition: Volume I http://www.gao.gov/special.pubs/3rdEditionVol1.pdf

[57] U.S. Military Covertly Pays to Run Stories in Iraqi Press, Los Angeles Times, November 30, 2005.

[58] 5 U.S.C. 552

[59] Every state, the District of Columbia and most federal territories have their own FOIA laws. See The Reporters Committee for Freedom of the Press, Open Government Guide. http://www.rcfp.org/ogg/index.php

[60] Attorney General's October 12, 2001 Memorandum on the Freedom of Information Act. http://www.usdoj.gov/oip/011012.htm

[61] GAO, Information Management: Implementation of the Freedom of Information Act, May 11, 2005.

[62] S. 394, OPEN Government Act approved by the Senate Judiciary Committee Sept 21, 2006; S 589, Faster FOIA Act of 2005, Approved by the Senate Judiciary Committee March 17, 2005, S. 1181, Approved by Senate June 24, 2005.

[63] Executive Order 13,392, on improving Agency Disclosure of Information, December 15, 2005. http://www.whitehouse.gov/omb/memoranda/fy2006/m06-04.pdf

[64] Letter from National Security Archive to Attorney General Gonzales, October 19, 2006.

[65] Secrecy News, Volume 2002, Issue No. 21, March 14, 2002.

[66] Mark J. Rozell, Executive Privilege Revived?: Secrecy and Conflict During the Bush Presidency, 52 Duke L. J. 403 (2002).

[67] US v. Nixon, 418 U.S. 563 (1974); Nixon v GSA, 433 U.S. 425 (1977).

[68] Public Law 95-591, codified at 44 U.S.C. 2201-2207.

[69] Executive Order 126.

[70] Executive Order 13233 of November 1, 2001 Further Implementation of the Presidential Records Act. http://www.fas.org/irp/offdocs/eo/eo-13233.htm

[71] See National Security Archive Page. http://www.gwu.edu/~nsarchiv/news/20040430/index.htm

[72] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).

[73] Memorandum from Michael J. Creppy to Immigration Judges and Court Administrators on "Cases requiring special procedures", Sept. 21, 2001. http://news.findlaw.com/hdocs/docs/aclu/creppy092101memo.pdf

[74] Statement of Lily Fu Swenson Deputy Associate Attorney General Before the House Judiciary Subcommittee on Immigration, Border Security and Claims, Concerning Immigration Removal Procedures Implemented in the Aftermath of the September 11th Attacks, June 30, 2005.

[75] Detroit Free Press v. Ashcroft 303 F.3d 681 (August 26, 2002).

[76] See The Memory Hole. Justice Department Censors Supreme Court Quote http://www.thememoryhole.org/feds/justice_redaction.htm

[77] David Kirby, The Other Secret Bush Court?, The Huffington Post, Nov. 15, 2006.

[78] Pickering v. Board of Education of Township High School District, 391 U.S. 563 (1968).

[79] Snepp v United States, 444 U.S. 507 (1980).

[80] Union of Concerned Scientists and Government Accountability Project, Atmosphere of Pressure: Political Interference in Federal Climate Science, February 2007.

[81] The New Gag Rules, Science 17 February 2006: Vol. 311. no. 5763, p. 917.

[82] New Publishing Rules Restrict Scientists, AP, December 2006.

[83] United States Department of State and the Broadcasting Board of Governors Office of Inspector General

Report of Inspection U.S. Speaker and Specialist Program Review Bureau of International Information Programs, Report Number ISP-C-06-52, September 2006. http://oig.state.gov/documents/organization/75589.pdf

[84] Yost, Guards Say Non-Disclosure Agreements Were Used to Hide Security Flaws at DHS, CQ Homeland Security – Industry & Contracting, April 19, 2006.

[85] DHS Non-Disclosure Agreement. http://www.fas.org/sgp/othergov/dhs-nda.pdf

[86] ibid. 82.

[87] 5 USC 2302; PL 95-454, 101-12.

[88] Congressional Research Service, National Security Whistleblowers, December 30, 2005.

[89] General Accounting Office, U.S. Office of Special Council, Strategy for Reducing Persistent Backlog of Cases Should be Provided to Congress GAO-04-36.

[90] Joint POGO, PEER, GAP letter to members of Congress regarding U.S. Special Counsel, Scott Bloch's retaliation against employees, January 10, 2005. http://www.pogo.org/p/government/gl-050101-whistleblower.html. See also PEER, Special Counsel Tags Interns to Close Out Whistleblower Cases; Staff Resignations Leave Agency Short-Handed, March 9, 2005. http://www.commondreams.org/news2005/0309-07.htm

[91] See Project on Government Oversight, Homeland and National Security Whistleblower Protections: The Unfinished Agenda, April 28, 2005.

[92] ibid.88

[93] Garcetti v. Ceballos, No 04-473. May 30, 200689.

[94] 18 USC 793 et sec.

[95] Edgar and Schmidt, The Espionage Statutes and Publication of Defense Information, 73 Columbia L.R. 929 (1973).

[96] New York Times Co. v. United States, 403 U.S. 713, (1971).

[97] See FAS page on Selected Judicial Branch Documents on Secrecy, Security, Intelligence and Freedom of Information for briefs and decisions on the case. http://www.fas.org/sgp/jud/index.html

[98] See e.g. Gabriel Schoenfeld, Has the New York Times Violated the Espionage Act? Commentary, March 2006.

[99] Statement by the President, November 4, 2000.

[100] S. 3774. A bill to amend title 18, United States Code, to prohibit the unauthorized disclosure of classified information; to the Committee on the Judiciary.

[101] Attorney General's Task Force Report on Unauthorized Disclosures of Classified Information, October 15, 2002. Available at http://www.fas.org/sgp/othergov/dojleaks.html

[102] 18 USC 641. See R. Robin McDonald, DEA Employee Gets Prison Term for Leaking to Reporter, Fulton County Daily Report January 15, 2003; Dmitrieva, Stealing Information: Application of a Criminal Anti-Theft Statute to Leaks of Confidential Government Information, 55 Florida Law Review, 1043 (2003).

[103] (CRS, Journalists' Privilege to Withhold Information in Judicial and Other Proceedings: State Shield Statutes, March 8, 2005. Available at http://www.fas.org/sgp/crs/secrecy/RL32806.pdf , Reporters Committee for Freedom of the Press, The Reporter's Privilege. http://www.rcfp.org/privilege/index.htm. It should also be noted that the right of journalist's confidentiality has been adopted in over 80 countries and has been recognized by the European Court of Human Rights and the Organisation of American States.).

[104] Branzburg v. Hayes, 408 U.S. 665 (1972).

[105] RCFP, Special Report: Reporters and Federal Subpoenas As reporters facing contempt charges in a number of federal cases around the country, Congress is taking its first serious look at a reporter's shield law in decades. Current as of: 11/29/06 http://www.rcfp.org/shields_and_subpoenas.html

[106] Pew Internet and American Life, How Americans Get in Touch with Government, May 24, 2004.

[107] E-Government Act of 2002, PL 107-347.

[108] See OMB, Memorandum on Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model, December 16, 2005.

[109] Google seeks better access to government information, GovExec.com, October 25, 2006.

[110] Government Printing Office Electronic Information Enhancement Act of 1993, PL 103-40.

[111] Annual Report of the Librarian of Congress, 2004.

[112] http://www.theopenhouseproject.com

[113] http://www.readthebill.org

[114] See CRS, The Federal Funding Accountability and Transparency Act: Background, overview and Implementation Issues, October 6, 2006.108.

[115] The International Budget Project, Open Budget Initiative 2006.

[116] For a detailed review of the legislation, see CRS, Ibid.

[117] GAO letter to OMB Director Joshua Bolten on Reliability of Federal Procurement Data, December 30, 2003. http://www.gao.gov/new.items/d04295r.pdf. GAO letter to OMB Director Joshua Bolten on Improvements Needed to the Federal Procurement Data System-Next Generation, Sept. 27, 2005. http://www.gao.gov/new.items/d05960r.pdf

[118] Letter from 11 non-project groups to GSA, August 9, 2004. http://www.pogo.org/p/government/gl-040801-foia.html

[119] See the Right-to-Know-Network http://www.rtknet.org

[120] See Gary Bass and Sean Moulton, The Public's Right to Know: A Case Study from the United States, in Calland and Tilley, The Right to Know, the Right to Live (ODAC, South Africa, 2002).

[121] http://www.sec.gov/edgar.shtml

[122] US Securities and Exchange Commission, SEC Staff to Publicly Release Comment Letters and Responses, June 24, 2004.

[123] Richard L Smith, The 1958 Automotive Information Disclosure Act: A Study of the Impact of Regulation,

Jnl of Industrial Economics, June 1980.

[124] Christopher Stern, FCC Cuts Public Line To Phone Outage Data, The Washington Post, August 28, 2004.

[125] RFF paper. p3

[126] PL 107-116 (December 17, 2002).

[127] John M. De Figueiredo, E-Rulemaking: Bringing Data to Theory at the Federal Communications Commission, 55 Duke L. J. 969 (2006).

[128] See OMB Watch, Against the Public's Will, December 2006. http://www.ombwatch.org/info/TRICommentsReport.pdf

[129] Pew Internet and American Life Project, Internet penetration and impact, April 2006.

[130] Ibid, Pew report.

[131] CRS, Restructuring EPA's Libraries: Background and Issues for Congress, January 3, 2007.

[132] Thomas Mann, What is Going on at the Library of Congress?, June 19, 2006.

[133] Bertot et al, Public Libraries and the Internet 2006: Study Result and Findings, September 2006.

[134] See OMB Watch, Access to Government Information Post September 11th,http://www.ombwatch.org/article/articleview/213/1/1/; Reporters Committee for Freedom of the Press, Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know.

[135] Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information, Rand Corporation (2004). http:www.rand.org/pubs/monographs/2004/RAND_MG142.pdf

[136] Small Business, Miami Herald, Dec. 16, 2006.

[137] The Digital Ice Age, Popular Mechanics, November 21 2006.

[138] http://www.govtrack.us

[139] http://www.opensecrets.org/travel/index.asp

[140] http://www.fedspending.org

[141] How planespotters turned into the scourge of the CIA, The Guardian, December 10, 2005.

[142] LA Times, A third incident, a new video, November 16, 2006.

Credits

Page 8, 24, 32
Dwane Powell Editorial Cartoon ©2005 Dwane Powell. Printed originally in the Raleigh News-Observer. Reprinted with the permission of Dwane Powell and Creators Syndicate

Page 26
Frank and Ernest ©2005 Thaves. Used with the permission of the Thaves and the Cartoonist Group.

Page 23
Matt Wuerker Editorial Cartoon ©2006 Matt Wuerker. Used with the permission of Matt Wuerker and the Cartoonist Group.

Page 10
Nick Anderson Editorial Cartoon ©2005 Nick Anderson. Published originally in the Louisville Courier-Journal. Used with the permission of Nick Anderson and the Washington Post Writers Group in conjunction with the Cartoonist Group.

Page 17
Signe Wilkinson Editorial Cartoon ©2006 Signe Wilkinson. Published originally in the Philadelphia Daily News. Used with the permission of Signe Wilkinson and the Washington Post Writers Group in conjunction with the Cartoonist Group.

OpenTheGovernment.org

Americans for Less Secrecy, More Democracy