Karen Hogenboom

Government Information Librarian

University of Illinois at Urbana-Champaign

Room 200-D Main Library

1408 W. Gregory

Urbana, IL 61801

LESSONS LEARNED ABOUT ACCESS TO GOVERNMENT INFORMATION AFTER WORLD WAR II CAN BE APPLIED AFTER SEPTEMBER 11

The cost of unrestricted dissemination of government information to the U.S.'s safety and security has been a topic of heated debate since September 11, 2001. The risks of dissemination seem to have skyrocketed in this age of terrorist attacks. However, the U.S. faced similar risks after World War II, when the secret of the atom bomb required close protection. Congress can learn from the process that the U.S. government went through to pass the Atomic Energy Act of 1946 during a similar time of national stress and fear, and work to pass laws regulating the dissemination of information to the public. In the absence of legislative guidance, agencies have been left to restrict information as they think is best, with inconsistent and disastrous results.

> Rarely in the history of this nation have the American people been confronted with a problem which is as complex, as multi-faceted, as the present problem of security of information [1, p. 9].

In many ways, Americans and the U.S. government are facing a completely new threat since September 11, 2001: a threat that requires new responses from both individuals and the government. The George W. Bush administration has responded to this threat with military force, administrative reorganization and reprioritization, and with restriction on freedoms--including freedom of access to government information--for reasons of national security. The profoundly shocking image of commercial airliners crashing into the World Trade Center towers and the Pentagon created a sense that all bets are off, that terrible things can happen at any time to anyone, and that we need to give up some of the freedoms we have taken for granted in order to guarantee our safety.

However, how different is this sense of danger in a world out of control from the sense of danger Americans experienced early in the Cold War, when Soviet Communists were supposedly recruiting sympathetic Americans to pass information about U.S. secrets, schoolchildren were drilled in what to do if a nuclear bomb fell on their neighborhood and homeowners built bomb shelters stocked with bottled water and canned goods? Is the perceived hatred of Arab extremists for America any greater than the perceived hatred of Soviet

Communists was? Weart's description of the American public's reaction to the dropping of the atomic bomb on Hiroshima seems remarkably contemporary:

> The public simply felt that the ground had fallen away under them. One element in this was the realization, which struck many people right from the first news, that at some point in the foreseeable future no city on earth would be safe. A related element, harder to pin down in factual concerns, was best expressed in a famous editorial by Norman Cousins: "The fear of irrational death…has burst out of the subconscious and into the conscious, filling the mind with primordial apprehensions." The old sense of security was lost; something unimaginable had come into the everyday world to stay [2, p. 106].

Certainly it is harder in many ways to deal with amorphous terrorist organizations whose members are perfectly willing to die than to deal with a foreign government as the U.S. did during the Cold War. The Internet has also transformed access to all kinds of information. However, the risks of disclosing government information are the same in either case: some government information, in the hands of persons or governments hostile to the United States and its citizens, can be used for great harm. This risk has fueled government attempts to increase secrecy and to control access to information for decades, not just since September 11, 2001.

The quote at the beginning of this article, published at the beginning of the Cold War in 1949, captures the current dilemma as well as the problems faced after World War II. As a Washington Post reporter pointed out a few months after September 11, U.S. officials are concerned that terrorists are using publicly available government information to plan their attacks [3]. Likewise, Congress and the Atomic Energy Commission were very concerned that information about the U.S. nuclear weapons program be kept out of Soviet hands during the Cold War.

Because the risks and concerns about publicly available information are similar, examining how access to sensitive government information was handled at the beginning of the Cold War could provide policymakers with a model for handling access to information during the War on Terrorism. The 79th Congress approached its information policy crisis very differently than the 107th Congress did in 2001: it directly addressed the problem of security of information, and although it moved quickly to protect the U.S.'s nuclear secrets, it took the time to consider a variety of solutions and to talk to experts and affected parties before passing the Atomic Energy Act. This paper will compare the history and information provisions of the Atomic Energy Act of 1946 with the PATRIOT Act and the Homeland Security Act, both passed shortly after September 11, and then discuss the consequences of current information policy on the Nuclear Regulatory Commission and on access to its information.

A broad range of government information has been inaccessible since September 2001, but because information about atomic energy has been a focal

point of information policy several times during the last sixty years it is an instructive point of comparison over time. Since the Manhattan Project in the early 1940s, which culminated in the dropping of atomic bombs on Hiroshima and Nagasaki, Japan, Congress and the executive branch have struggled with how to keep scientific and technical information about U.S. nuclear capabilities out of the hands of hostile governments and terrorist organizations.

The physicists working on the atomic bomb during World War II were the first to realize that nuclear information needed to be kept secret for reasons of national security [4, p. 76]. The first that most Americans, including most government officials, heard about atomic weapons was on August 6, 1945, when President Truman announced that the Enola Gay had dropped an atomic bomb on Hiroshima, Japan.

Legislative Response to Hiroshima and Nagasaki

Immediately after atom bombs were dropped on Hiroshima and Nagasaki in August 1945, the 79th Congress took up the issue of how to control the production of atomic weapons, including the control of information about atomic energy. However, in spite of the urgency and complexity of the problem of access to nuclear information, Congress took the time to address the issue thoroughly and creatively. Although the Soviets had fought on the same side as the U.S. for most of World War II, it quickly became apparent that the USSR's priority was the spread of communism, by violence if necessary, at the expense of

capitalism and democracy. Therefore, the fact that the USSR had not built a nuclear bomb at the end of World War II made secrecy of the U.S.'s scientific and technical discoveries imperative. After months of congressional hearings, the Senate Special Committee on Atomic Energy summarized the situation in the spring of 1946 as follows:

> Other countries of the world will be able to make atomic bombs. The monopoly which we hold at present is precarious and certain to be short-lived…it is clear that any nation which is relatively industrialized has a good chance of producing bombs within the next 5 to 15 years….
>
> No real military defense against the atomic bomb has been devised, and none is in sight. The destructiveness of atomic bombs is so engulfing that any defense which is not almost literally airtight will not protect our country against devastation.
>
> The secrets which we hold are matters of science and engineering that other nations can and will discover. In large part they are secrets of nature, and the book of nature is open to careful, painstaking readers the world over. We can give ourselves a certain temporary protection by retaining the secrets we now have. But that protection grows weaker day by day, and our research must be vigorously encouraged, supported, and

> pursued if we are to maintain or place among other nations, to say nothing of retaining our advantage [5].

Suddenly the world was a much more dangerous place, and from this summary it is clear that the Senate Committee thought that control of information was one of the few possible safeguards against mass destruction. The tension between secrecy and the encouragement of scientific development is also clear, however, and both were considered vital to U.S. interests and security.

The first bill about atomic energy, introduced exactly one month after Hiroshima, provided for a board that would develop atomic energy and control its use [6]. This and later bills provided for a commission to monitor atomic energy issues [7]. Other bills asked for studies or for international prohibitions on the use of atomic weapons [8]. Also, on October 3, 1945, President Truman called on Congress to establish a commission regulating the production and use of atomic energy in the U.S., whose mandate would include regulating information about atomic energy [9].

These bills addressed the issue of controlling nuclear information in varying levels of detail. 79 H.R. 3912's sole provision was to make it a capital offense to disclose information or impart knowledge that would assist in learning the secret of the atomic bomb; 79 H.R. 3997 was similar. 79 S. 1359 and 79 H.R. 4014 provided for up to five years' imprisonment and/or a $10,000 fine for revealing confidential atomic energy information, as defined by a board of military and executive branch officials (Section 5). These bills did not distinguish

intent of disclosing information: innocent or inadvertent disclosures could have been punished as severely as willful espionage activities if these bills had passed.

S. 1463 authorized the Atomic Energy Commission (AEC) to promulgate regulations about information security (Section 17) and provided stiff penalties for willful violations: up to ten years in prison and/or a $100,000 fine (section 18). Non-willful violations would have been grounds for dismissal from employment with the AEC, as well as a $500 fine and thirty days' imprisonment. Intent to jeopardize the interests of the U.S. would have brought a $300,000 fine and thirty years in prison (Section 19).

H.R. 5230 contained a section titled "Guarantees of Scientific Freedom," restricting the AEC from interfering with scientific activity, communication, or the travel of scientists outside the U.S.. However, activities concerning the development or use of atomic energy were required to be disclosed to the AEC.

None of these bills passed, however. 79 S. 1717, introduced on December 20, 1945 by Senator Brien McMahon, became the Atomic Energy Act of 1946. The Act was the first legislative attempt to regulate research and development into atomic energy in the U.S., and its stated purpose was to "direct the development of atomic energy in such a way as to improve the public welfare, increase the standard of living, strengthen free competition in private enterprise, and promote world peace," all subject to the primary objective of assuring national security [5, p. 9]. Discussing freedom of research in his original report about S. 1717, Senator McMahon stated that "…this bill is not a good bill because of the precautions it takes, because of the controls it establishes, because of the limitations it places on

free development of atomic energy. This bill is a good bill because of the freedom it allows and because of the encouragements it gives to this development" [10].

The bill contained a section titled "Dissemination of Information" that defined "basic scientific information" as theoretical knowledge and all results capable of accomplishment (distinguished from the processes used to reach those results). This section also provided for unfettered dissemination of basic scientific information and established a Board of Atomic Information to administer libraries and other means of dissemination, and to designate information as basic scientific information [11].

By the time S. 1717 was approved by the Special Senate Committee on Atomic Energy after an extensive series of hearings, this section had been retitled "Control of Information" and had a completely different focus:

> (a) Policy. It shall be the policy of the Commission to control the dissemination of restricted data in such a manner as to assure the common defense and security.

Principles to guide the AEC in disseminating information stressed sharing information with other nations once international safeguards were established and encouraging dissemination of information to encourage scientific progress. The commission was authorized to publish, as well as establish libraries and information services. However, this section also defined "restricted data:" a

concept that took atomic information out of the general classification system applicable to other sensitive information. Any information in the following areas was automatically classified:

1. The manufacture or utilization of atomic weapons
2. The production of fissionable material
3. The use of fissionable material in the production of power

However, if the AEC determined that data could be published without adversely affecting national defense and security, it could be released.

This was a drastic departure from how other national security information was treated. The current system of setting criteria and procedures for classification in an executive order began in the Eisenhower administration, so classification at the end of World War II was handled by individual agencies [12, p. 217]. For example, in 1946 Army regulations provided that:

> Official matter requiring classification shall be examined, graded, and marked top secret, secret, confidential, or restricted. Top secret is a special grading given to certain secret matter…the security aspect of which is paramount and whose unauthorized disclosure would cause exceptionally grave damage to the nation…

> Documents, information, or matériel, the unauthorized disclosure of which would endanger national security, cause serious injury to the interests or prestige of the nation, or any governmental activity thereof, or would be of great advantage to a foreign nation shall be classified secret…
>
> Documents, information , or matériel, the unauthorized disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, any governmental activity, an individual, or would cause administrative embarrassment, or difficulty, or be of advantage to a foreign nation shall be classified confidential…
>
> Documents, information, or matériel (other than top secret, secret, or confidential) which should not be published or communicated to anyone except for official purposes shall be classified restricted…[13].

Setting aside the appropriateness of the criteria described above, each piece of information needed to be affirmatively reviewed and classified under these and other similar rules; no information other than nuclear information was "born classified." Furthermore, non-nuclear information would automatically be declassified after the passage of a certain period of time unless affirmative action was taken after determining that release of the information could still be detrimental to national security. There was no provision in the 1946 Act for restricted data to be released except by affirmative review of the AEC. Penalties

for disclosing or conspiring to disclose restricted data with intent to secure an advantage to a foreign nation or reason to believe an advantage to a foreign nation will result carried stiff penalties, including imprisonment for up to 20 years and fines up to $20,000.

The Atomic Energy Act of 1946 and its information provisions have not remained static. By the early 1950s, the non-military uses of atomic energy were obvious, and the restrictions set up by the 1946 Act were impeding industrial use of nuclear power. The Atomic Energy Act of 1954 was Congress's response to the changing information needs of government agencies, U.S. industry, and the international community. The definition of restricted data was not changed, but a new category of information, formerly restricted data (FRD), was created so that the Department of Defense could have access to information about the military use of atomic weapons under the normal classification rules [14]. Public Law 97-90, passed early in the Reagan administration, also modified the information provision of the Atomic Energy Act. It added a category of Unclassified Controlled Nuclear Information (UCNI) that restricted access to information about nuclear production and utilization facility design, information about security measures at nuclear facilities, and previously restricted data about design, use or manufacture of atomic weapons if there was a "reasonable expectation" that the information could be used to steal, sabotage, or illegally manufacture nuclear weapons [15].

The Atomic Energy Act of 1946 was far from perfect and has not completely stood the test of time, but by the time it passed it had been thoroughly

discussed, with significant input from all affected parties inside and outside the government. It attempted to balance the needs of scientists for freedom to disseminate their research results and the needs of the military for secrecy about U.S. weapons development and capabilities. Its information dissemination provisions were specific and concrete. It required reports to Congress on how the Act's information restrictions were being applied and provided for judicial review of agency decisions.

The category of UCNI added to the Atomic Energy Act during the Reagan administration is just one example of information that is not classified, but is inaccessible to most citizens, federal employees, and government contractors. This information has many names, including "sensitive national security information," critical infrastructure information," and the most common, "sensitive but unclassified information." Many of these terms have a history that long predates September 11, but the use of these terms to justify withholding information after the World Trade Center and Pentagon attacks has placed them under increased scrutiny. UCNI is one of the few examples in this category that was established by legislation: often information is withheld on the basis of agency rules, memos from the Office of Management and Budget, or even memos within agencies [16].

Legislative Response to September 11, 2001

Just eight days after September 11, Attorney General John Ashcroft delivered proposed legislation to a group of senators that eventually became the PATRIOT Act [17]. The House Judiciary Committee held the first hearings on the proposal on September 24, and several more hearings were held during the following two weeks, before a bill had even been introduced.

On October 23, 2001, Rep. Sensenbrenner introduced H.R. 3162, which became the PATRIOT Act [18]. Briefly, most of its provisions related to increased surveillance authority for law enforcement agencies, immigration control, and to attempts to cut off funding streams to terrorist organizations. Criminal penalties were increased for terrorism offenses and information sharing and cooperation between law enforcement agencies was increased. There is no provision in H.R. 3162, or in the final PATRIOT Act, that directly addresses public access to information, as the original Atomic Energy Act did. The PATRIOT Act became law within two months of September 11 and three days after it was introduced, on October 26, 2001 [19].

Although the PATRIOT Act had no provisions directly affecting public access to government information, the Homeland Security Act addresses this issue in a section titled "Homeland Security Information Sharing Act" [20]. There were three bills with this title in the 107th Congress, but the provisions of the Homeland Security Act are most similar to 107 S. 2887, introduced by Sen. Dianne Feinstein on August 1, 2002 but never considered by a Senate committee or the full Senate. Like the PATRIOT Act's information provisions, the Homeland Security Information Sharing Act's main focus is on information

sharing among state, local and federal law enforcement agencies. However, Section 892 directs the President to establish procedures and standards for sharing sensitive unclassified information that apply to all federal agencies [20, §892]. The other two bills titled "Homeland Security Information Sharing Act," H.R. 3825 (introduced February 28, 2002) and H.R. 4598 (introduced April 25, 2002) do not address the issue of establishing and standardizing definitions of sensitive unclassified information and procedures for its dissemination [21]. The Homeland Security Act was signed by the President on November 25, 2002.

At this point, the issue of defining sensitive but unclassified information left the legislature's hands. In an executive order signed on July 29, 2003, President Bush delegated the functions assigned to him in section 892 of the Homeland Security Act to the Secretary of Homeland Security, except for the responsibility to ensure that the rules regarding information sharing apply to all federal agencies [22]. Currently the only sign that this directive is a priority for the Homeland Security Agency is an item in the Homeland Security Agency's agenda for the second half of 2005 stating that identifying, safeguarding and sharing sensitive homeland security information is in the proposed rule stage [23]. Therefore, if the rulemaking process goes smoothly and if these Homeland Security Agency regulations apply to the entire government, there will be procedures and criteria in place shortly before the fifth anniversary of September 11.

Meanwhile, a December 2005 memorandum from President Bush citing Section 892 of the Homeland Security Act as his authority directed that a program

manager in the office of the Director of National Intelligence collect information about existing information sharing procedures used by executive departments, and to create common standards for an "information sharing environment" across government. The Director of National Intelligence is also directed by this memorandum to inventory agencies' definitions and procedures for dealing with sensitive but unclassified information and to develop a definition and procedures that will apply across government, in coordination with other cabinet-level officials. All of this work is directed to be finished within 90 days of the memorandum, in mid-March, 2006 [24].

Executive Branch Actions Restricting Public Access to Information After September 11

In this vacuum of legislative leadership about public access to information, chaos has reigned. Six months after the attacks on the World Trade Center and the Pentagon, Feinberg wrote that "the traditional concerns for balancing access, privacy and secrecy are not in play. Many key decisions are being made by members of the law enforcement and military communities, either with little experience in information policy issues or with institutional predilections toward secrecy, and by a small group of executive branch officials who have a history of favoring restrictions on government information" [25].

Because Congress did not address public access to information in its legislative response to September 11, executive branch agencies were left to make

decisions based on existing laws like the Freedom of Information Act, U.S. Code Title 44 (which describes the types of government information that should be distributed to depository libraries), and the current executive order establishing rules for classified information. Government agencies almost immediately started taking down documents from their web sites, and in some cases removed whole sections of the sites to keep information out of terrorists' hands. For example, in February of 2002 over 6,600 technical reports were withdrawn from circulation by the National Technical Information Service as part of an ongoing security review [26]. The U.S. Geological Survey required depository libraries to destroy a CD-ROM containing water data in October 2001 [27].

The first general and official information policy guidance that agencies received after the attacks was on October 12, 2001, when Attorney General John Ashcroft issued a memorandum describing the policy executive branch agencies should follow when processing requests under the Freedom of Information Act (FOIA) [28]. The most striking change from previous FOIA policy was a default policy of non-disclosure: while the memorandum asserted the importance of FOIA, agency officials were assured that the Justice Department would back them up in their decisions not to release documents as long as the denial was based on a statutory exemption to release described in FOIA.

The second piece of guidance agencies received came in March 2002 from White House Chief of Staff Andrew Card in the form of a memo [29]. Card stressed agencies' responsibility to "safeguard" information about weapons of mass destruction and "other information that could be misused to harm the

security of our nation and the safety of our people." A second memorandum from the Information Security Oversight Office and the Office of Information and Privacy of the Justice Department included sensitive but unclassified information specifically in the category of information that must be safeguarded, but did not define this term other than to say that it does not meet the criteria for classification [30].

The Nuclear Regulator Commission's (NRC) actions to protect its information from terrorists who may be planning attacks on power plants are a good indicator of the ambiguity of this advice, especially in contrast with the handling of atomic energy information by its predecessor agency, the Atomic Energy Commission (AEC), after World War II. The NRC inherited a strong tradition of public access to its unclassified information from the AEC. Before the advent of internet access to government information, this access was provided through its public document rooms, located near power plants, as well as through the National Technical Information Service and the Federal Depository Library Program. Once the NRC established a web presence, it included an online public reading room on its website and closed most of its physical reading rooms.

Despite this tradition of openness and despite the fact that much of its information is "born classified" as provided in the Atomic Energy Act and therefore would seem unlikely to be overlooked in the classification process, the NRC took down its entire web site on October 11, 2001 for security review. The site was reposted later in the month, minus information the public uses to participate in NRC proceedings [31]. In early 2002, information that was

previously available on the NRC web site was still being reviewed and returned to the site only if it did not contain sensitive information [32]. In March of 2002, the Superintendent of Documents, who administers the Federal Depository Library Program (FDLP), informed depository library directors that the NRC was reviewing the microfiche that had been distributed to depository libraries and might be requesting that some reports be withdrawn from libraries [33].

On April 4, 2002, after Ashcroft's and Card's memos had been issued, an internal NRC Action Memorandum finally provided guidance on releasing potentially sensitive information. The memorandum provided that information generated by NRC or its contractors will be withheld if it could provide a clear and significant benefit to an adversary in a potential attack. General information will not be withheld, and information that was widely available on the date of the memorandum will not be reviewed [34].

An incident during August 2003, described in a letter from Rep. Henry Waxman (D-CA) to Christopher Shays, the Chairman of the Committee on Government Reform's Subcommittee on National Security, Emerging Threats, and International Relations, shows the result of NRC's tendency toward secrecy combined with confusion about procedures and criteria for restricting access to information. The NRC staged a mock attack on a nuclear power plant during the summer of 2003 and reported to Congress that the attack was repelled successfully. The Project on Government Oversight (POGO) wrote a letter to the NRC Chairman detailing problems with the mock attack and posted the letter on their website. The NRC demanded that the entire letter be removed from public

access, although it was based on publicly available information, but after several months of correspondence and the threat of litigation the NRC identified specific information in the POGO letter that it considered sensitive (although none of it was classified) and the report was revised [35].

In spite of this cautious approach to releasing information, the NRC's electronic reading room was taken down again on October 25, 2004 because a private citizen and a watchdog group found information they felt could help terrorists. About 700,000 documents were removed from public access [36]. The NRC planned to review 5,000 documents per day, completing the review process by June of 2005 and reposting any documents the agency did not consider sensitive [37]. In February of 2005, the NRC issued a proposed rule codifying the many internal orders about access to information that had been issued since the first one in April 2002, and creating an additional category of sensitive unclassified information [38]. Critics are concerned that the new rules would conceal information that enables the public to participate in discussions about safety at nuclear power plants and participate in holding the NRC accountable for its management of the nuclear power program [39]. For example, in March of 2005, Rep. Edward Markey (D-MA) asked the NRC's inspector general to study whether the NRC's actions prevent the public from accessing documents that do not pose a security risk [40].

Discussion

No one can deny that the information landscape has changed since September 2001, or that the Internet created new challenges related to sensitive information. But much of the chaos over the last five years has been due to lack of authoritative guidance on these issues. The laws that govern information dissemination were crafted in an era of tangible formats, where even the most widely distributed government information was still only available in libraries. The Andrew Card and Attorney General memorandums issued within six months of September 11 are examples of this, relying on the Freedom of Information Act, which is a product of the 1960s and 1970s, to guide agencies in releasing information on their Internet sites.

Without strong guidance from Congress, agencies like the Nuclear Regulatory Commission are left to decide on their own what should be available to the public, and the realities of government almost guarantee that they will err on the side of caution. Furthermore, the fact that many officials untrained in information management are setting information policy leads to vague guidance that can be difficult to apply to individual situations. Policies are also likely to contain large areas where discretion can or must be used, making the policies flexible but also leaving decision makers open to criticism, scapegoating, or even legal liability. Halchin describes information dissemination policies developed by the Department of Defense, Federal Bureau of Investigation, and National Archives and Records Administration jointly with the Department of Justice [41]. While none of them are the same, all give officials wide discretion in withholding information based on their own judgment of the risk of disclosure. Herman

describes a possible model policy, issued by the United States Geological Survey in December 2002, that provides for multiple levels of review before withholding information and acknowledges the complexity of security concerns by providing for a range of security restrictions [42].

What if NRC information about nuclear power plant vulnerabilities or USGS water table data could be tied to a terrorist attack? The agency that released the data would be blamed, certainly in the media and most likely in Congress and by the President, because it was the decision of someone at the agency that the information should be released. This threat is much more immediate to an agency official than the risks that arise from withholding information. This balance of risks is a recipe for conservative information dissemination, because agency officials will understandably do whatever is necessary to protect the public and limit their agencies' political vulnerability. However, Halchin also points out the irony that the same medium that makes information available to terrorists also enables the government to share information about preventing and responding to terrorist attacks [41]. Further illustrating this irony, Dahl discusses the risk management plans that companies submit to the Environmental Protection Agency, their removal from the Internet, and the likelihood that denying terrorists access to this information about chemical releases and their consequences will deny citizens information about how to respond to a public health emergency [43].

But imagine an alternate scenario, where the NRC, USGS, and all other agencies are following generally applicable information dissemination policies

established by law and enforceable by the federal courts, as the information provisions of the Atomic Energy Act are. Not only would agencies all be following the same rules, the public and the librarians who serve the public would know what should be available to them. Agency officials could release information with some confidence that if they are following the law they are not harming public safety or risking their careers and the careers of everyone working under them. If confusion arose about how to apply the law or situations developed that were not considered when the law originally passed, the courts could interpret the law or Congress could amend it. And if agencies do not follow the law, the courts could enforce it.

This scenario is based on junior high social studies rather than nuclear physics, but it has not come to pass. Congress declined an opportunity to legislate this issue by directing the President to define "sensitive but unclassified" information, and the President then passed the ball to the Department of Homeland Security and the Director of National Intelligence. DHS is only one agency and a new one at that, and cannot make rules that have the same authority and enforceability as laws even if it does pick up the ball. The Director of National Intelligence is also a newly created position, in an area of government that is famous for its unwillingness to share information. Both DHS and the Director of National Intelligence are also as vulnerable as any other agency or official to becoming a scapegoat if information winds up in the wrong hands. The ball needs to be passed back to Congress, whose job is to develop and enforce policy decisions.

However, we are not living in a social studies class and the political realities of the fight against terrorism complicate these issues endlessly. Two years after her initial assessment that key decisions about access to information were being made in an uncoordinated way by officials with no background in information policy, Feinberg wrote that repeated that policy about access to government information is still in a state of flux, and with no bipartisan agreement in Congress about directions for information policy. Furthermore, access to government information is not at the top of any member's legislative agenda [44]. President Bush may be able to shape the discussion of this issue in Congress if the Director of National Intelligence determines that legislation is necessary to implement whatever information sharing policies and procedures are established pursuant to the president's December 2005 memorandum. Given the well-documented viewpoint of this administration that presidential power needs to be restored to what it was before FOIA passed, it is unlikely that any proposed legislation would contain provisions regarding judicial or congressional oversight. Congress needs to take back the initiative and pass a bill about access to government information that provides specific guidance for reasonable withholding of sensitive information and oversight of agency decisions by the legislative and judicial branches of government. If the Department of Homeland Security compiles and evaluates executive branch departments' definitions and policies concerning sensitive but unclassified information, this evaluation could be a starting point for Congressional staff to draft legislation and schedule hearings that include affected non-governmental groups and individuals rather

than relying entirely on agency input, as President Bush's most recent memorandums do.

Conclusion

Although the Atomic Energy Act of 1946 was not a perfect piece of legislation and no one could say that the Cold War was the golden age of access to information, Congress's reasoned and thoughtful response to the problem of access to nuclear information was effective and a similar process could be effective now. Much information has already been lost to agency web site purges and other recent government information has never been released, but it is better to have principles, rules, and reporting structures for agency decisions late than not at all. Librarians, scientists, community activists, and other interested parties could shape the legislation via congressional hearings and communications with the members of Congress who are accountable to them.

Congress could set up the mechanisms for all agencies to report and be held accountable for their decisions to withhold information. Agencies could make decisions based on the legislation that Congress passes, with some level of confidence that they were not releasing information inappropriately. Ultimately, while information may not be as accessible as it was before September 11, it would be possible for citizens, scientists, and the librarians who serve them to know what should be available and what should be inaccessible.

While agency officials' fears of releasing sensitive information are justified in the current policy environment, they need to be balanced with citizens' need to know what their government is doing and their right to have access to information produced with tax dollars. The best place for that balance to be struck is in Congress, where accountability to citizens is most direct and where the expertise and authority lie to make decisions that apply to all of government and to hold agencies accountable for how they apply these decisions. This is not to say that there is an easy or simple way to protect sensitive information while maintaining the openness of government that is necessary for democracy to thrive, but it is certainly no less possible to strike this balance now that it was in 1946.

References

1. Summers, Robert, comp. Federal Information Controls in Peacetime. New York: H.W. Wilson, 1949.
2. Weart, Spencer R. Nuclear Fear. Cambridge, MA: Harvard University Press, 1988.
3. Cha, Ariana Eunjung. "Risks Prompt U.S. to Limit Access to Data: Security, Rights Advocates Clash Over Need to Know." Washington Post, Sunday, 24 February 2002, sec. A, p. 1.
4. Relyea, Harold C. Silencing Science: National Security Controls and Scientific Communication. Norwood, N.J.: Ablex Publishing Corp, 1994.
5. U.S. Congress. Senate Special Committee on Atomic Energy. Atomic Energy Act of 1946. S.Rep. No. 1211, 79th Cong., 2nd Sess. (1946).
6. S. 1359, 79th Cong., 1st Sess. (1945).
7. S. 1463, 79th Cong., 1st Sess. (1945); S. 1557, 79th Cong., 1st Sess. (1945).
8. i.e. S. Con. Res. 38, 79th Cong., 1st Sess. (1945); S. Res. 186, 79th Cong., 1st Sess. (1945); S. Con. Res. 28, 79th Cong., 1st Sess., (1945); S. J. Res. 93, 79th Cong., 1st Sess. (1945).
9. Belair, Jr., Felix. "Truman Suggests Atomic Bomb Ban, U.S. Control Body." New York Times, 4 October 1945, p. 1.
10. Congressional Record, 79th Cong., 2nd sess., 1946, 92, pt. 5: 6,096.
11. S. 1717, 79th Cong., 1st Sess. §9 (1945).

12. Moyihan, Daniel Patrick. Secrecy: The American Experience. New Haven, CT: Yale University Press, 1998.

13. War Department. Army Regulations No. 380-5, § 1 (August 15, 1946), quoted in Summers, supra: 128-129.

14. Atomic Energy Act of 1954, § 141(c). Statutes at Large 68 (1954): 941.

15. Department of Energy National Security and Military Applications of Nuclear Energy Authorizations Act of 1982, § 148. Statutes at Large 95 (1982): 1169.

16. Knezo, Genevieve. "Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy. Washington, D.C.: Congressional Research Service, 2003.

17. Washington, Wayne and Leonard, Mary. "America Prepares Shaping Strategy: Proposed Legislation: U.S. Seeks New Power to Track, Detain, Deport." Boston Globe, 20 September 2001, 3rd ed., sec. A, p. 31.

18. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107th Cong., 1st sess., H.R. 3162.

19. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Statutes at Large 115 (2001): 272.

20. Homeland Security Act of 2002, § 891 et seq. Statutes at Large 116 (2002): 2252.

21. H.R. 4598 passed in the House but was not actively considered in the Senate, and H.R. 3825 never reached the House floor.

22. President. Executive Order 13311. "Homeland Security Information Sharing." Federal Register 68, no. 147 (31 July 2003): 45149.

23. Department of Homeland Security. "Unified Agenda of Federal Regulatory and Deregulatory Actions," Federal Register 70: 26,891 (2005).

24. Bush, George W. "Memorandum for the Heads of Executive Departments and Agencies." Available at http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html (last accessed February 11, 2006).

25. Feinberg, Lotte E. "Homeland security: implications for information policy and practice—first appraisal." Government Information Quarterly 19, no. 3 (2002): 265-266.

26. Broad, William J. "A Nation Challenged: Domestic Security: U.S. is Tightening Rules on Keeping Scientific Secrets." New York Times, Sunday, 17 February 2002, late edition final, sec. 1, p. 1.

27. Buckley Jr., Francis J. "SuDocs Letter: Destroy USGS CD-ROM," Administrative Notes 22 (October 15, 2001): 7.

28. Ashcroft, John. "Memorandum for Heads of All Federal Departments and Agencies," Available at http://www.usdoj.gov/04foia/011012.htm (last accessed October 14, 2005).

29. Card, Jr., Andrew H. "Memorandum for the Heads of Executive Branch Departments and Agencies," Available at http://www.fas.org/sgp/bush/wh031902.html (last accessed October 14, 2005).
30. Kimberley, Laura L.S., Huff, Richard L., and Metcalfe, Daniel J. "Memorandum for Departments and Agencies," available at http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm (last accessed October 14, 2005).
31. Jaffe, Susan. "Cautious Agencies Restrict Internet Information," (Cleveland) Plain Dealer, 23 October 2001, final, sec. B, p. 5.
32. Smith, Tom. "Access to Documents of the U.S. Nuclear Regulatory Commission After September 11, 2001." Presentation at the midwinter meeting of the American Library Association, New Orleans, LA, January 19, 2002.
33. Buckley Jr., Francis J. to Depository Library Directors, 14 March 2002. Administrative Notes 23 (15 April 2002): 10-12.
34. Travers, William D. "Withholding Sensitive Security Information from the Public," Available at http://www.nrc.gov/reading-rm/doc-collections/commission/comm-secy/2002/2002-0015comscy.pdf (last accessed October 14, 2005).
35. Waxman, Henry, to Christopher Shays, 1 March 2005. Available at http://www.democrats.reform.house.gov/Documents/20050301112122-90349.pdf (last accessed October 14, 2005).

36. OMB Watch. "NRC Removes All Nuclear Information from its Public Website," Available at http://www.ombwatch.org/article/articleview/2498/1/229 (last accessed October 14, 2005).
37. Nuclear Regulatory Commission. "NRC Restoring 70,000 Additional Documents to its On-Line Library After Security Review." Available at http://www.nrc.gov/reading-rm/doc-collections/news/2005/05-090.html (last accessed October 14, 2005).
38. Nuclear Regulatory Commission. "Protection of Safeguards Information." 70 Fed. Reg. 7,196 (2005) (to be codified at 10 C.F.R., (proposed February 11, 2005).
39. OMB Watch. "OMB Watch Criticizes Nuclear Commission's Secrecy Rule," Available at http://www.ombwatch.org/article/articleview/2766/1/229?TopicID=1 (last accessed October 14, 2005).
40. Savage, Charlie. "In War's Name, Public Loses Information." Boston Globe, 24 April 2005, 3rd ed., sec. A, p. 1.
41. Halchin, L. Elaine. "Electronic Government: Government Capability and Terrorist Resource." Government Information Quarterly 21, no. 4 (2004): 406-419.
42. Herman, E. "A Post-September 11th Balancing Act: Public Access to Information Versus Protection of Sensitive Data." Journal of Government Information 30 (2004): 42-65.

43. Dahl, Richard. “Does Secrecy Equal Security? Limiting Access to Environmental Information.” Environmental Health Perspectives 112, no. 2 (2004): A104(4).

44. Feinberg, Lotte E. “FOIA, Federal Information Policy, and Information Availability in a Post-9/11 World.” Government Information Quarterly 21, no. 4 (2004), 439-460.