Biosecurity and Secrecy Policy: Problems, Theory, and a Call for Executive Action

BRIAN J. GORMAN*

ABSTRACT

The national security and academic communities are facing unprecedented issues that portend the greatest paradigm shift between the federal government and the global community of science. For the first time since the formalization of information policy at the federal level, there is an opportunity to fashion a well reasoned solution to the growing dual use dilemma in life science research. This paper examines the biosecurity threat in the context of federal secrecy policy and dynamics of the information society. In the absence of a rich literature on secrecy theory, an attempt to examine the theoretical issues underlying aspects of federal secrecy policy is undertaken with particular emphasis on classic problems in secrecy policy. The duty to consider developing countries when assuming public health risks related to the public release of dual use biological research is introduced. It is also suggested that the Executive amend Export Administration Regulations in order to create a notice mechanism to enable national security vetting of U.S. research on select agents, toxins and microorganisms integrally related to pandemics and bioweapons.

PART 1: POLICY

I. INTRODUCTION

The nation is facing unprecedented challenges on a number of fronts. Specifically, science, terrorism, federal secrecy and the information society seemed to have, all at once, challenged the laws and policies that have governed to date. Advancements in the life sciences are greater than ever, but so too are the destructive capabilities they bring. Meanwhile, terrorism has crossed boundaries with unrivaled depravity, and federal secrecy appears to be rising to unprecedented levels, raising questions over governmental transparency and whether the nation's intelligence apparatus is blinded

* Assistant Professor, Department of Law, Police Science & Criminal Justice Administration, John Jay College of Criminal Justice, City University of New York. The author would like to thank the reviewer and John B. Belmonte for helpful comments, in addition to Steven A. Figueiredo for technical assistance.

by its own secrets. Raising the stakes and reducing margins for error in all of the above is the inexorable and transformative force of the information society. Thus, analysis of each new challenge is warranted, but caution dictates a comprehensive review of the possible interactions new policies and laws will have for and amongst all of the above. This paper addresses the intersection of science, secrets, and national security in the context of the information society.

II. THE UNIQUE THREAT OF BIOTERRORISM

The threat from bioterrorism is old in the sense that it is a historic tool of war and new in the sense that it is viewed as a clear and present danger in the post 9-11 era. The unsolved anthrax attacks of 2001 and the more recent use of terrorism on civilian targets in Madrid and London reinforces the need to address all potential terrorist threats. Thus, counterterrorism efforts need to focus on conventional warfare techniques as well as weapons of mass destruction (WMD) incorporating chemical, biological, radiological and nuclear (CBRN) materials that would cause incalculable damage in urban settings.

While all of these threats deserve careful attention, the threat from bioterrorism is particularly ominous at this juncture due to several factors.[1] First, the financial, intellectual, and material barriers to bioterrorism are falling at a faster rate than other WMD threats. It is already estimated that the cost of killing one person with a biological weapon is $1 while chemical and nuclear weapons would cost $1000 and $1 million, respectively.[2] Second, although there is hope for developments in 2006, global efforts such as the Bioweapons Convention and UN Security Council Resolution 1540 lag behind comparable nuclear and chemical treaties. Third, while CBRN threats as a whole are seen as high impact, low frequency threats, infectious diseases are already high frequency, high impact events. Unlike unintentional CBRN events such as those at Bhopal and Chernobyl, microbiological pathogens regularly cause an estimated 1,500 deaths

---

[1] *See* Marc L. Ostfield, Senior Advisor on Bioterrorism, Biodefense, and Health Security, Off. of Int'l Aff., Remarks at NATO Conference on Elements of Combating WMD Terrorism: Intersectoral and International Cooperation on Combating Bioterrorism (Sept. 14, 2005), http://www.state.gov/g/oes/rls/rm/56614.htm (Dr. Ostfield discusses the uniqueness of bioterrorism and its impact upon international policy.).

[2] P. Scott Layne & Tony J. Beugelsdijk, *High-Throughput Laboratories for Homeland and National Security*, 1 BIOSECURITY AND BIOTERRORISM 123 n.2 (2003).

per hour around the world.[3] Thus the lethality of infectious diseases provides a uniquely tempting and accessible force of destruction for terrorists.[4]

III. GLOBALIZATION AND BIOSECURITY

The global nature of bioscience also leads to a greater strain on biosecurity. Despite widespread use of CBRN materials in industry and academia around the world, they tend to be more compatible with tight controls due to their limited and costly uses. In contrast, biological equipment capable of advancing bioterrorism is nearly ubiquitous since some of the most basic laboratory techniques can be used in developing or enhancing virulent pathogens.[5] Thus, apparently benign school, industry, and clinical laboratories in community settings can be of use to a terrorist with the right knowledge. The seemingly distant connection between the governance of basic laboratory facilities needed for health care and the global reach of bioterrorism was recently recognized in the Kampala Compact of 2005. The Compact recognized that the patchwork of national and global public health networks is uniquely tied to the threat and response to bioterrorism. The Compact stated that it is in fact illegitimate to address the threat of bioweapons without addressing the enormous health crises facing developing countries.[6] The threat of biosecurity will no doubt bring to the fore the notion that the best community health money can buy is actually a function of the health of the poorest communities in the world so long as people and goods intersect in a global market community.

---

[3] World Health Organization, *Report on Infectious Diseases: Removing Obstacles to Healthy Development*, http://www.who.org/infectious-disease-report/pages/textonly.html#Anchor1 (last visited Oct. 24, 2005).

[4] Intentional misuse at lower levels is also of concern. *See* Anna Arutunyan & Oleg Liakhovich, *Bioterror Suspected in Hepatitis Outbreak*, MOSCOW NEWS, June 15-21, 2005, http://english.mn.ru/english/issue.php?2005-22-8 ("With some 574 people hospitalized with hepatitis A in the Tver region and an initial influx of some 45 new patients each day, regional investigators are looking into a possibility that the outbreak… may be linked to a biological attack.").

[5] Tara O'Toole, Address at the Preventing Bioterrorism, 1st Interpol Global Conference at Lyon, France: Bio-Terrorism: The Threat of the 21st Century (Mar. 1, 2005).

[6] *Kampala Compact: The Global Bargain for Biosecurity and Bioscience* (Oct. 1, 2005), http://www.icsu-africa.org/Resource_centre/KampalaCompactoct05.pdf.

The growing awareness of the transmissibility of self-replicating pathogens will likely lead to far reaching cooperation as stakeholders with greater wealth realize the value of investing in public health networks in developing countries. Unfortunately, however, the lack of incentives for wealthy stakeholders to include developing countries in decisions on information policy matters related to biosecurity may result in balkanized scientific communities. Thus, insular national approaches to the dual use dilemma may help calcify the divide between the countries leading in scientific research and the rest of the world.[7] At present, no global organizations are addressing the dual use issue, with efforts commensurate to the United States.[8] The U.S., through the National Institutes of Health, is currently leading a unique effort to address the dual use dilemma through the creation of a federal advisory board known as the National Science Advisory Board for Biosecurity (NSABB).[9]

The NSABB is an original public and private effort designed to advise the government on ways to draw lines between protected and public access information. NSABB's pioneering mission presents many new challenges, not the least of which is its duty to design a program that assures a biosecurity policy for the United States that is compatible with the global community. Thus, NSABB must create policies that support the advancement of the premiere league of science while being sensitive to the needs of developing nations as well. For instance, some level of risk is inherent in the study and publication of research on pathogens. Thus, the government must be mindful of the risk inherent in conducting cutting-edge research in U.S. labs and protect the country from intentional or accidental

---

[7] David A. King, *The Scientific Impact of Nations: What Different Countries get for their Research Spending*, 430 NATURE 311 (2004) (identifying a divide between the premiere league of 31 countries which account for 98% of the world's highly cited scientific articles and the remaining 162 countries which only produced 2%).

[8] Shana Dale, Esq., Chief of Staff and General Counsel, Off. of Sci. and Tech. Policy in the Exec. Off. of the Pres., Address at the Inaugural Meeting of the National Science Advisory Board for Biosecurity ("Although not overtly articulated at some of the international meetings I've been to, there appears to be a feeling at least with some of the countries that this is a U.S. problem and not necessarily for them.").

[9] "The NSABB has been established to provide advice to federal departments and agencies on ways to minimize the possibility that knowledge and technologies emanating from vitally important biological research will be misused to threaten public health or national security. The NSABB is a critical component of a set of federal initiatives to promote biosecurity in life science research." National Science Advisory Board for Biosecurity, http://www.biosecurityboard.gov (last visited Oct. 24, 2005).

exposure from infectious diseases. But, consistent with the spirit of the Kampala Compact, the U.S. must also make risk assessments with respect to developing countries with less advanced public health infrastructures. A troubling case in point is the apparent acceptance of the risk associated with the recent revival[10] and publication of the genomic sequence[11] of the Spanish Flu of 1918, based largely on U.S. resistance capabilities to the flu. The factors leading to a finding of acceptable risk included, in part, partial immunity against the 1918 flu, a comprehensive public health system, and U.S. stockpiles of vaccines that appear to combat the revived virus.[12] Clearly, this analysis fails to take into consideration communities that have less immunity, have faltering public health programs, and lack vaccine stockpiles. The Health and Human Services Secretary acknowledged the globalization of public health when he said, "if [an avian flu outbreak] happens anywhere, there is risk everywhere."[13] Thus, it is no longer acceptable in the age of globalization for any country to measure public health risks from infectious diseases according to the strengths within its own borders. If the U.S. seeks the cooperation of foreign governments as a key strategy in the fight against avian flu, then, at a minimum, a sense of fair play dictates that, in policy decisions, the U.S. take into account the risk of nations without commensurate public health resources.[14]

---

[10] Terrence M. Tumpey et al., *Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus*, 310 SCIENCE 7 (2005).

[11] Jeffrey K. Taubenberger, *Characterization of the 1918 Influenza Virus Polymerase Genes*, 437 NATURE 889 (2005).

[12] Special Report, *The 1918 Flu Virus is Resurrected*, NATURE, Oct. 6, 2005, at 794-95 ("[Tumpey] adds that even if the virus did escape, it wouldn't have the same consequences as the 1918 pandemic. Most people now have immunity to the 1918 virus because subsequent human flu viruses are in part derived from it. And, in mice, regular flu vaccines and drugs are at least partly effective against an infection with reconstructed viruses that contain some of the genes from 1918 flu.").

[13] *U.S. Builds Response Plans for Bird Flu, Bioterror Attack*, WALL ST. J., Aug. 3, 2005, at D4.

[14] Lauran Neergaard, *Containing Bird Flu Abroad Critical to new U.S. Flu Pandemic Plans*, THE ASSOCIATED PRESS (BC Cycle), Oct. 6, 2005 ("[I]n an interview with The Associated Press, Leavitt said U.S. health officials would rush overseas to wherever a bird flu outbreak occurred and work with local officials to try to contain it."); *Researchers Model Avian Flu Outbreak, Impact of Intervention*, NIH NEWS, Aug. 3, 2005, *available at* http://nih.gov/news/pr/aug2005/nigms-03.htm ("[T]hey offered this good news: The models show that containing an avian flu pandemic at its source is feasible.").

The members of NSABB decided to make an effort to reach out to the global community of science at its first meeting in July 2005 so the results of their efforts are not known at this writing. The structure of a federal advisory committee does not lend itself to a global forum, but the inclusion of representative countries beyond the premiere league of science may be warranted for a U.S. policy that will have repercussions for biosecurity the world over.

IV. U.S. INFORMATION POLICY AND SCIENCE

It is widely recognized that science advances at its greatest pace in an open environment where findings are accessible, transparent and replicable by any interested party. The problem, however, is that the open science model is not universally appropriate if it provides terrorists with a free ride from open research in pursuit of malevolent goals. Although the prevailing model of science is open, it is important to note that much science is conducted under cover of secrecy in the interests of national security[15] or financial gain.[16] The most notorious classified area is atomic science where research is born classified, regardless of source. The current challenge posed through the dual use dilemma in life science research forces policymakers to shed light on the gray areas between classified and open source boundaries on sensitive information generated by public and private labs.[17] Thus, members of the NSABB and the policy makers ultimately responsible for making these decisions should have an understanding of the troubled state of U.S. information policy before applying the tenets of extant information policies to the scientific community.

The prospect of applying a classification regime to life science research that would otherwise be published openly in academic

---

[15] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON SECRECY (1970), *available at* http://www.fas.org/sgp/othergov/dsbrep.html (last visited Oct. 24, 2005).

[16] *See* JOHN P. WALSH, ASHISH ARORA & WESLEY M. COHEN, *Research Tool Patenting and Licensing and Biomedical Innovation*, in PATENTS IN THE KNOWLEDGE-BASED ECONOMY 285 (National Academy of Sciences, 2003).

[17] Elizabeth R. Parker, *Bioterrorism Threats Must Unite Academe and the U.S. Intelligence Community*, 70 THE EDUC. DIG. 9, 13 (2004) ("In fact, it is the private sector, not the government that owns and controls many of the structures and facilities that are central to our conflict with terrorists.").

journals causes great concern for many.[18] The prospect of applying government restrictions raises concern at the outset because there are already concerns that the government is over-classifying information to the detriment of much needed transparency.[19] Moreover, the publication process is an integral part of the professional life of scientists and the best known way to advance the field with deliberate speed.[20] Thus, scientific journals and reports are filled with emotional polemics decrying the prospect of tearing asunder a system that advances a fair, open, and global practice that serves the interests of humanity so well.[21] Working from an overly idyllic premise, however, invites unnecessary emotion into the debate and fails to recognize the

---

[18] Erika Check, *Biologists Apprehensive Over U.S. Moves to Censor Information Flow*, 415 NATURE 821 (2002).

[19] Scott Shane, *Since 2001, Sharp Increase in the Number of Documents Classified by the Government*, N.Y. TIMES, July 3, 2005, at A14.

[20] Dr. Harold Varmus, Nobel Prize Winner in Medicine and President Memorial Sloan-Kettering Cancer Center, Address at Trinity College: The Global Development Challenge, *available at* http://www.tcd.ie/iiis/pages/events/conferences_past/conf10July.php (last visited Oct. 14, 2005) (In a talk regarding scientific publishing, Dr. Varmus succinctly said with good humor, "All we want is fame.").

[21] Statement, National Institutes of Health, Unmasking the 1918 Influenza Virus: An Important Step Toward Pandemic Influenza Preparedness (Oct. 5, 2005), http://www3.niaid.nih.gov/news/newsreleases/2005/0510state.htm ("It would be impossible and counterproductive to attempt to enforce a worldwide ban on conducting research on the 1918 influenza virus or similar viruses because of fear of the misuse of such knowledge."); COMMITTEE ON RESEARCH STANDARDS AND PRACTICES TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, NATIONAL RESEARCH COUNSEL OF THE NATIONAL ACADEMIES, BIOTECHNOLOGY RESEARCh in an Age of Terrorism 110 (2004); Committee on Genomics Databases for Bioterrorism Threat Agents, National Research Council of the National Academies, Seeking Security: Pathogens, Open Access, and Genome Databases 36 (2004); see Brian Vastag, *Openness in Biomedical Research Collides with Heightened Security Concerns*, 289 J. OF THE AM. MED. ASS'N 686 (2003) (Donald Kennedy, went so far as to say, "[i]t is impossible to gauge if a research finding could ever be used for nefarious purposes."). *See* Deborah Byrd and Joel Block, *Bioterrorism vs. Science, A Radio Interview with Ronald Atlas*, Program #4,124 of the Earth Sky Radio Series, aired April 19, 2004, http://www.earthsky.com/shows/edgeofdiscovery.php?date=20040419 (last visited Oct. 13, 2005) (Atlas said, "Science today is collaborative, …the United States cannot act alone. We can't look to the U.S. government…What we need to do is look to the scientific community worldwide. This is not a US scientist issue. It is a global scientist issue aimed at protecting science."). Ronald Atlas, Address at Assisting States to Effectively Fulfill UNSCR 1540's Legal Requirements, International Consortium for Law and Strategic Security Workshop at New York, NY (Nov. 15, 2005) (Atlas compared government regulation of sensitive scientific information with "a license to think.").

realities of the competitive side of U.S. science.[22] Moreover, the idyllic view overlooks the realities of the relationship between modern science and national security. A number of classification regimes already do co-exist harmoniously with the scientific community.

Moreover, the proposed control of sensitive information is a logical extension of the widely accepted physical restrictions of select agents that few, if any, criticized, [23] beyond the headache of paperwork and fears of prosecution for the mishandling of same.[24] The tighter one holds the view that science is a pure and global epistemological endeavor, the more it lends itself to myth. Rather, it is merely international[25] and arguably the most unregulated clinical discipline despite being subject to many of the same ethical challenges facing lawyers, physicians and other licensed professionals. Thus, awareness of export control regimes, the capture of patents, and the vast array of federally funded classified research at private and federal facilities adds much needed balance to this debate on how to capture similarly sensitive research in the largely unregulated field of life sciences. Figure 1 details a number of existing and proposed restrictions on life science research.

---

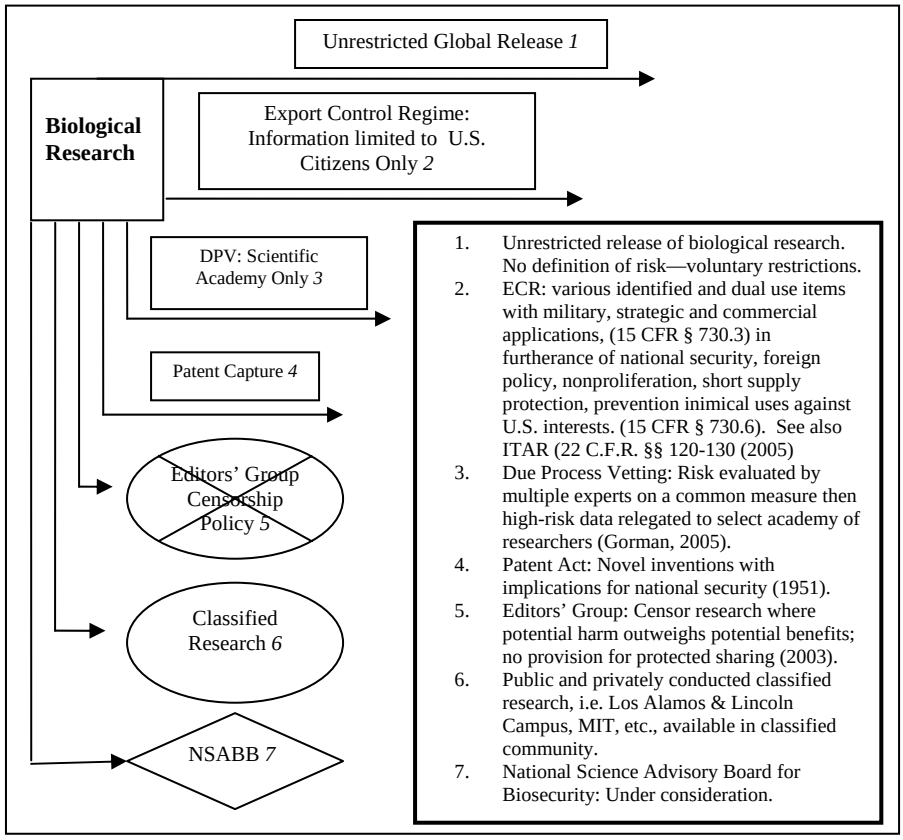
[22] William J. Broad, *Top Advisory Panel Warns of an Erosion of the U.S. Competitive Edge in Science*, N.Y. TIMES, Oct. 13, 2005, at A21 (Regarding a report convened by the National Academies of Science).

[23] Helen Pearson, *Biologists Seek to Revamp Biowarfare Register*, news@nature.com, http://www.nature.com/news/2004/040719/pf/430388a_pf.html (last visited October 14, 2005).

[24] Use and Transfer of Select Agents and Toxins, 42 C.F.R. 72-73 (Mar. 18, 2005) (The CDC received 110 written comments for the public comment period ending February 11, 2003, and no comments for the comment period for the interim final rule ending January 2, 2004.).

[25] *Id.*; King, *supra* note 7 (King notes that the divide between the premiere league of 31 scientific nations is expanding and leaving the remaining 162 nations behind.).

Table 1: Existing and Proposed Restrictions on Dissemination of Life Science Research



One of the few areas of consensus in secrecy policy is the acknowledgment over the need for a new paradigm. A new paradigm has been called for by many, including Tom Blanton[26] and the National Academy of Sciences,[27] while others have started drafting

[26] Tom Blanton, Remarks at the National Security and Open Government: Striking the Right Balance Symposium (May 2003), http://www.justiceinitiative.org/activities/foifoe/foi/opengov ("We need a new paradigm beyond the balancing test.").

[27] *See* COMMITTEE ON RESEARCH STANDARDS AND PRACTICES TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, NATIONAL RESEARCH COUNSEL OF THE NATIONAL ACADEMIES, *supra* note 21; COMMITTEE ON GENOMICS DATABASES FOR BIOTERRORISM THREAT AGENTS, NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, SEEKING SECURITY, *supra* note 21.

plans.[28] The need for a new paradigm that assures that information is shared and protected grows more urgent each day as the stakes in life science research[29] and public health grow higher.[30]

V. U.S. SECRECY POLICY

Despite years of reliance on secrets, it took over 150 years for significant controversies to develop over access to government information.[31] The government, however, only started to formulate information (or secrecy) policy in earnest through Executive Orders (E.O.), legislation, and case law in the twentieth century. The technical, scientific, and tactical advancements made during World War II combined with advancements in communication increased the need to secure information upon which national security relied. Thus, ever since the 1940's, the federal government has made adjustments to secrecy policy in search of the appropriate balance of secrecy and openness. The balance of secrecy and openness in a democracy, however, is an abstraction; thus, it can never settle on a fixed point. The perpetual tension between those seeking access to government information and those in government who need to protect information assures perpetual dissatisfaction with the balance of federal secrecy and openness. But, ironically this tension can actually serve as an asset. The ebb and flow of policy decisions responding to these pressures may actually help find this elusive target of "balance" in the murky waters of federal secrecy. Thus, NSABB has a unique

---

[28] *See* Brian J. Gorman, *Balancing National Security and Open Science: A Proposal for Due Process Vetting*, 7 YALE J.L. & Tech. 59 (2005); Robert H. Sprinkle, *The Biosecurity Trust*, 53 BIOSCIENCE 270 (2003); Michael Barletta, Amy Sands & Jonathan B. Tucker, *Keeping Track of Anthrax: The Case for a Biosecurity Convention*, 58 BULL. ATOM. SCI. 57 (2002); George M. Church, *A Synthetic Biohazard Non-Proliferation Proposal* (Aug. 6, 2004), http://arep.med.harvard.edu/SBP/Church_Biohazard04c.doc; Elisa D. Harris & John D. Steinbruner, *Scientific Openness and National Security After 9-11*, 67 THE CBW CONVENTIONS BULL. 1 (Mar. 2005).

[29] Taubenberger et al., *supra* note 11; Tumpey et al., *supra* note 10.

[30] Gardiner Harris, *Fear of Flu Outbreak Rattles Washington*, N.Y. TIMES, Oct. 5, 2005, at A23 ("An outbreak could cause 100,000 to 2 million deaths and as many as 10 million hospitalizations in the United States.").

[31] Harold C. Relyea, *Access to Government Information in the United States*, CONG. RES. SERVICE, Jan. 7, 2005, at 1 ("Throughout the first 150 years of the federal government, access to government information does not appear to have been a major issue among the three branches or for the citizenry.").

opportunity to create or endorse a new and lasting paradigm that meets a variety of compelling goals for the advancement of life sciences, national security and the global community.

Federal secrets have traditionally served at least two functions. One has been to protect information from adversaries and the other to shield policy deliberations from the electorate and others so that discussions and analysis can be candid.[32] Areas typically requiring secrecy include foreign relations,[33] military affairs, and more recently, counterterrorism. Since modern secrecy policy on science started out in reaction to a need, i.e. the preservation of atomic secrets from the Manhattan Project, its development reflects reactive rather than proactive planning. Thus, due to its relative youth, reactive nature and need for flexibility in federal secrecy policy, secrecy policy development has not been entirely orderly. The most stable developments were made by Congress.

VI. THE LEGISLATURE: SECRECY POLICY AND SCIENCE

Shortly after World War II, Congress passed the Atomic Energy Act (AEA) of 1946[34] to maintain control over the scientific secrets from the Manhattan Project. The AEA led to the establishment of the Atomic Energy Commission (AEC) which ultimately formalized strict rules governing the restriction of information related to atomic energy. The policies created by the AEC in turn promulgated the most stringent restraints on scientific information in the U.S. via the "born classified" doctrine. The result is a standing prior restraint on all scientific data concerning the proscribed areas of atomic science, which are considered classified from inception regardless of origin.

The Cold War period followed with additional secrecy legislation. The Invention Secrecy Act (hereinafter ISA) of 1951[35] compliments the "born classified" doctrine in atomic sciences by capturing scientific techniques critical to national security from any scientific

---

[32] *See* Mark J. Rozell, *Executive Privilege in the Carter Administration: The "Open" Presidency and Secrecy Policy*, 27 PRESIDENTIAL STUD. Q. 272, 278 n.2 (1997).

[33] *See* Owen T. Smith, *Book Reviews-Victory: The Reagan Administration's Secret Strategy that Hastened the Collapse of the Soviet Union by Peter Schweizer*, 24 PRESIDENTIAL STUD. Q. 883 n.4 ("Frequently, White House staffers were dismissed from Presidential meetings because of the 'sensitive' nature of the intelligence materials to be discussed.").

[34] The Atomic Energy Act of 1946, 42 U.S.C. §§ 1801-1819 (2003).

[35] The Invention Secrecy Act, 35 U.S.C. § 181 (2004).

discipline that comes to the attention of the U.S. Patent Office through the application process. The Patent Office screens patent applications for novel discoveries with implications for national security. Once potentially sensitive discoveries are identified, a referral is made to the federal agency with expertise in the discipline covered in the application, and then a Secrecy Order (hereinafter S.O.) may be issued which captures the science by classifying it.[36]

The ISA, however, was the last capture measure created for "free-range" science in the U.S., i.e. science conducted by and for private parties and entities. Thus, there remains a gap in the identification and capture of contentious[37] science and technology that are classifiable but evade the limited catchments of the AEA or ISA. The ISA does offer compensation when it issues a S.O., much like a reimbursement for land taken by eminent domain. Thus, when it comes to national security, intellectual property, like real property, is subject to seizure by the sovereign. There are no other legislative schemes to capture and reward strategic science beyond that which is commissioned by the government. This gap was recently noted by a voting member of NSABB, Michael Osterholm.[38] Thus, the next step in the evolution of information policy would logically lead to a capture mechanism with incentives for the science and technology not addressed by the AEA and PSA.

Much like a sword, secrecy policy cuts both ways, the other side in this case being access rights to government information. The Administrative Procedure Act of 1964 was intended to assure disclosure of governmental information.[39] But unfortunately, it "was generally recognized as falling far short of its disclosure goals and

---

[36] See *infra*; Secrecy News, *Pentagon Pursues "Strategic Influence"* (Feb. 20, 2002), http://www.fas.org/sgp/news/secrecy/2002/02/022002.html.

[37] Gerald Epstein, Public comments at the National Science Advisory Board for Biosecurity Meeting in Bethesda, Md. (June 20, 2005), *available at* http://webconferences.com/nihnsabb/380405.html (offering the following operational definition of contentious research: "Fundamental biological or biomedical investigations that produce organisms or knowledge that could have immediate weapons implications and that therefore raise questions concerning whether and how that research should be conducted and disseminated.").

[38] Eugene Russo, *1918 Flu Papers test HHS' Ability to Efficiently Monitor Pre-Publication Dual-Use Research*, RESEARCH POLICY ALERT (Oct. 6, 2005) ("[Osterholm] acknowledged that the board does not yet have a process in place to monitor pre-publication research by non-government researchers who do not feel obligated to have HHS vet their findings.").

[39] The Administrative Procedure Act of 1964, 5 U.S.C. §§ 1002-1003 (1964).

came to be looked upon more as a withholding statute than a disclosure statute."[40] Two years later, however, Congress mended the errors of the Administrative Procedure Act by making the single greatest effort to advance the rights of the access community through the Freedom of Information Act (FOIA) of 1966. FOIA can be seen as a formalization of the tradition of transparency in government and also a radical change in the relationship between the public and government agencies.[41] FOIA assured the public access to government information subject to limits for a number of exemptions for personal privacy, law enforcement, and the protection of classified information among others.

The bounds of FOIA were tested in the 1970's when members of Congress tried to compel production of classified documents prepared for the President concerning underground nuclear tests. The U.S. Supreme Court, in *EPA v. Mink*, clarified the limitations of FOIA and affirmed deference to the Executive in matters of national security.[42]

> What has been said thus far makes wholly untenable any claim that the Act intended to subject the soundness of executive security classifications to judicial review at the insistence of any objecting citizen. It also negates the proposition that Exemption 1 authorizes or permits *in camera* inspection of a contested document bearing a single classification so that the court may separate the secret from the supposedly nonsecret and order disclosure of the latter.[43]

The Court, however, did not close the door on conflicts with the Executive branch. The Court noted that Congress was free to establish its own classification procedures subject to the limitations of executive privilege or have the Executive adopt new procedures.[44] Congress also weighed in on secrecy matters in the 1970's after reviewing the recommendations of the Church Committee. In an effort to curb activities such as domestic spying, Congress brought about a "major

---

[40] EPA v. Mink, 410 U.S. 73, 79 (1973).

[41] Lotte E. Feinberg, *FOIA, Federal Information Policy, and Information Availability in a Post-9/11 World*, 21 GOV'T INFO. Q. 439 (2004).

[42] *Mink*, 410 U.S. at 83.

[43] *Id.* at 84.

[44] *See id.* at 83.

power shift" by enhancing supervision and accountability for covert activities.[45]

VII. THE EXECUTIVE: SECRECY POLICY AND SCIENCE

Given the concurrent authority of the Executive and Legislative branches over information policy, the question is begged over the resolution of potential conflicts. The Judicial branch is the likely arbiter of such disputes, but the Supreme Court is likely to defer to the Executive when it comes to national security matters. For instance, in *U.S. v. Reynolds*, the government successfully barred discovery of classified materials including an accident report in a wrongful death case brought by the estates of civilian defense contractors who died on a military plane testing secret electronic equipment.[46] The government offered discovery of non-classified information, and the Court thought that was sufficient. The Court was not going to second guess the Executive in matters of national security. This privilege created great deference for the Executive in national security matters and has made challenges to classification decisions through judicial avenues problematic. As noted by Professor Kellman, the privilege creates a circular dilemma "because the inquiry itself violates the privilege."[47]

A recent development in the Reynold's case underscores the perpetual fears of government secrecy via abuse of the privilege. Despite having settled the case with the government decades ago, relatives of the deceased in the Reynold's case sought to re-open the Supreme Court case by claiming that the government committed fraud in the original case. This assertion was made after a review of de-classified documents concerning the 1948 plane crash. This development is subject to interpretation. But assuming *arguendo* that the allegations are true, one can either find solace in the fact that the secrecy policies work by eventually providing a check, albeit late, on itself through declassification mechanisms or find support for suspicions over the disturbing misuse of the privilege.[48]

---

[45] *See* Loch K. Johnson, *Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee*, PUB. ADMIN. REV., Jan./Feb. 2004, at 3, 11 ("[T]he Church Committee had been able to bring about a major power shift. Responsibility for supervision of the intelligence agencies would be largely removed from the jurisdiction of Armed Services Committee and given the closer attention it warranted.").

[46] U.S. v. Reynolds, 345 U.S. 1 (1953).

[47] Marcia Coyle, BROWARD DAILY BUS. REV., Mar. 11, 2003, at A7.

[48] *Id.*

There were two important cases in the 1970's concerning access and protection of information which loom behind the current debate on open science and society. In a case over media access to areas in a jail with adverse conditions, the Supreme Court held that there are limits to accessing government information. The opinion spoke to the delicate balance of secrecy and access rights in dicta by stating, "[t]he Constitution itself is neither a Freedom of Information Act nor an Official Secrets Act."[49] Lower federal courts weighed in again on information policy through *U.S. v. Progressive*.[50] *Progressive* concerned a prior restraint standoff between a publisher seeking to publish H-bomb secrets and the government, which foreshadows recent government requests of scientific publishers. The *Progressive* standoff abated after the government withdrew the case. The publisher eventually published the article in its entirety,[51] but the government did establish a precedent for prior restraint in the courts by successfully restraining the article until the government was satisfied with its vetting of the article.

VIII. EXECUTIVE POWERS

The Executive plays a prominent role in the formation of secrecy policy due to its authority in national security and foreign policy matters. The primary tool exercised by the Executive is the Executive Order (E.O.) which led to the current classification regime. E.O.s in tandem with temporary legislation provide authority for the current Export Administration Regulations which restrict export of dual use technology and information.[52]

---

[49] Houchins v. KQED, Inc., 438 U.S. 1, 11 (1978).

[50] U.S. v. Progressive, Inc., 467 F. Supp. 990, 994 (W.D. Wis. 1979), *reh'g denied*, 486 F. Supp. 5 (W.D. Wis. 1979) ("There are times in the course of human history when time itself may be very important. This time factor becomes critical when considering mass annihilation weaponry…").

[51] Murray Kempton, "*The Secret" Revealed*, THE PROGRESSIVE, Nov. 1979, at 6-8.

[52] Export Admin. Reg. Database, Part 730 General Information § 730.2, Apr. 29, 2005, *available at* http://www.access.gpo.gov/bis/ear/pdf/730.pdf ("The EAR have been designed primarily to implement the Export Administration Act of 1979, as amended, 50 U.S.C. app. 2401-2420 (EAA). … The EAA is not permanent legislation, and when it has lapsed, Presidential executive orders under IEEPA [International Emergency Economic Powers Act] have directed and authorized the continuation in force of the EAR.").

The Executive Order is a powerful tool of the Executive that has been criticized for the growth in power over the years.[53] Regardless of the controversy, a review of information policy from the 1940's reveals an inter-administration learning curve on fundamental secrecy issues in the Executive branch. For instance, some of the recurring issues identified through the years concern the scope of classifiable information, declassification, reclassification, time limits, rationale labeling and the misuse of classification authority. While the recognition of common issues appears to have developed, a common approach toward them has not.

A number of classic issues have been addressed through E.O.s from the advent of World War II to today. For instance, the first presidential E.O. on classification policy issued by President Roosevelt cast a net over strategic materials and delineated a tiered system with graduated classifying labels, i.e., secret, confidential, and restricted. [54] Two years later, Roosevelt issued another Executive Order[55] which sought to influence rather than control public information via propaganda through the Office of War Information.[56] Thus, modern export controls through Export Administration Regulations (EAR),[57] International Traffic in Arms Regulations (ITAR),[58] the creation of NSABB and the increased use of public affairs officials to handle the

---

[53] Tara, L. Branum, President or King? The Use and Abuse of Executive Orders in Modern-Day America, 28 J. of Legis. 1, 2 (2002) ("[P]residential directives have been increasingly used-both by Republicans and Democrats-to promulgate laws and to support public policy initiatives in a manner that circumvents the proper lawmaking body, the United States Congress."); William J. Olson & Alan Woll, Executive Orders and National Emergencies: How Presidents Have Come to "Run the Country" by Usurping Legislative Power, http://www.cato.org/pubs/pas/pa-358es.html (last visited Oct. 9, 2005).

[54] Exec. Order No. 8381, 5 Fed. Reg. 1147 (Mar. 26, 1940).

[55] Exec. Order No. 9182, 7 Fed. Reg. 4468 (June 16, 1942).

[56] Allan M. Winkler, Information Control and Propaganda: Records of the Office of War Information, Research Collections in the Social History of Communications, http://www.lexisnexis.com/academic/2upa/Sc/InformationControlPropaganda.asp (last visited Oct. 24, 2005).

[57] Export Administration Regulations, 15 C.F.R. §§ 730-774 (2005).

[58] International Traffic in Arms Regulations, 22 C.F.R. §§ 120-130 (2005).

release of government information reflects classic war footing responses to information control.[59]

Another classic issue that has been addressed through E.O.s over the years concerns the mosaic theory[60] which was originally addressed in 1951.[61] In an effort to curb over-classification, President Truman ordered that decisions to classify rest solely on the contents of the document in question. President Reagan addressed the phenomenon in the 1980's by allowing the classification of information in the context of other pieces of information. Los Alamos National Lab currently deals with a mosaic problem from the accumulation of non-classified information that becomes classified when juxtaposed with other information in forwarded e-mails.[62] Truman's secrecy policy also foreshadowed the current stovepipe dilemma as well when he allowed department heads to establish higher standards than that found in the E.O. This action led to obstacles in inter-agency sharing of information, which continue to plague the intelligence community to this day.[63]

Beyond the classic secrecy problems, modern secrecy policy first went adrift with the volley of inter-administration policy decisions beginning with President Carter. Carter introduced a balancing test through an order in 1978 which framed decisions in terms of public interest in access and the government's need to protect information from disclosure.[64] This order also tightened classification standards by raising the standard for "Confidential," the lowest classification

---

[59] Tom Brune, *Cadre Grows to Rein in Message*, NEWSDAY, Feb. 24, 2005, at A22 (The argument has been made that Bush Admin. has hired public affairs officials to help manage public relations while tightening up the release of information.).

[60] Michael Liebman, Line Attorney, Criminal Division, Department of Justice, Prepared Testimony Before the Senate Judiciary Committee, Subcommittee on Administrative Oversight and the Courts (Apr. 12, 2000), *available at* http://fas.org/irp/congress/2000_hr/liebman.html (last visited July 29, 2005) ("By mosaic theory, I mean that items of information considered separately are unclassified, but when grouped together they become classified.").

[61] Exec. Order No. 10,290, 16 Fed. Reg. 9795 (Sept. 27, 1951).

[62] Thomas J. Bowles, Chief Sciences Officer, Los Alamos National Laboratory, Address Before the National Science Advisory Board Meeting: Past as Prologue: Are there Lessons to be Learned from the Nuclear Physics and Cryptography Communities? (June 30, 2005), *available at* http://biosecurityboard.gov/meetings/200506/NSABB_Bowles.pdf (last visited Oct. 24, 2005).

[63] See *infra*; Exec. Order No. 10,290, 16 Fed. Reg. 9795 (Sept. 27, 1951).

[64] Exec. Order No. 12,065, 43 Fed. Reg. 28,949 (June 28, 1978).

designation. The new standard established by Carter attempted to shrink the universe of classified information by making the minimum requirement for classification "identifiable damage" as opposed to mere "damage."[65] Carter's E.O. is also unique because it set a limiting clause in the classification of science. The Order stated that basic science could not be classified unless it was "clearly related to the national security."[66] This order also identified the reclassification issue by stating that information cannot be reclassified if it was previously "declassified and released to the public."[67]

The longest lasting legacy from Carter's secrecy policy may be the creation of the Information Security Oversight Office (ISOO). The ISOO became a fixture that exists to this day under the leadership of its second director, William Leonard. Thus, Carter assured that federal secrecy had continued attention. The creation of this office provided a counterbalance to overclassification by directing complaints and suggestions regarding classification issues to a central office. Carter also created an appeal mechanism for contested classification decisions.

As expected, President Reagan's secrecy policy reflected a departure from Carter's approach. President Reagan's order in 1982 reversed Carter's E.O. provisions by expanding the classifiable universe of information.[68] Reagan removed Carter's "identifiable damage" standard and restored the broader "damage" standard. In addition, Reagan removed the prohibition against the reclassification of information. Reagan allowed reclassification in cases where the information may reasonably be recovered.

Reagan's orders were silent on science, but he did release National Security Directive Decision No. 189 on the issue (hereinafter NSDD-189).[69] Reagan turned to the National Academy of Sciences for direction on the treatment of sensitive scientific data. In the 1980's, the security of science focused primarily on the transfer of physical sciences research from open sources to the Soviet Union. The Academy convened a panel to address the issue and produced the

---

[65] *Id.*

[66] *Id.*

[67] *Id*.

[68] Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (Apr. 2, 1982).

[69] National Security Directive Decision, Directive 189, Association of American Universities, Sept. 21, 1985, http://www.aau.edu/research/ITAR-NSDD189.html.

Corson Report which acknowledged that the need to the classify science in certain areas is "clearly indicated."[70] Otherwise the report recommended "limited restrictions" for a small gray area of science and openness for the remainder.[71] Reagan's NSDD-189 reflected the Corson Report's recommendations for a least restrictive approach toward classification by stating, "It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted."[72]

In addition to the worries over the transfer of open science to the Soviet Union, there was great concern over the integrity of the nation's classified information. Thus, in 1985, the Department of Defense commissioned a Security Review Commission to investigate the matter.[73] The Stilwell Report expressed concern that unauthorized disclosure of classified information could upset the military balance. Thus, the report made various recommendations to improve the security of classified information. In addition, the report opined the lack of criminal statutes relating to unauthorized disclosure of classified information. At about the same time as the release of the Stilwell Report, a criminal case was unfolding over the release of three classified photos to the press by a Navy intelligence analyst, Samuel Loring Morison.[74] The government argued in the rare espionage case that, "the courts should interpret the espionage laws as applying to the transmission of classified information to the press."[75] Morison was convicted and sent to jail, but President Clinton pardoned him at the end of his term in office.[76] Prosecutions for leaking classified information to the press are still rare, but as testament to the classic

---

[70] COMM. ON SCI., ENGINEERING, AND PUB. POL'Y, NAT'L ACAD. OF SCI., SCI. COMM. AND NAT'L SECURITY 4 (1982).

[71] *Id*.

[72] National Security Directive Decision, *supra* note 69.

[73] Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policy and Practices (1985), http://www.fas.org/sgp/library/stilwell.html.

[74] U.S. v. Morison, 604 F. Supp. 655 (D. Md. 1985).

[75] Thomas I. Emerson, *Comment on "Access to Classified Information: Constitutional and Statutory Dimensions*, 26 WM & MARY L. REV. 845 (1985).

[76] Valerie Strauss, *Navy Analyst Morison Receives a Pardon, 2 Sentenced in Drug Cases Win Their Freedom*, WASH. POST, Jan. 21, 2001, at A17.

nature of secrecy issues, a similar controversy is underway at this writing.[77] The government is making a similar argument in the current spy case.[78]

Much like the Presidents before him, President Clinton was responsible for revisions in information policy through the Executive Order.[79] The changes in classification procedures made by Clinton included the requirement to leave the name and title of the person making the classification decision, along with the rationale for doing so, with the document. This forward looking requirement was designed to help in the declassification of documents. In addition, Clinton's administration undertook an unprecedented bulk declassification effort in the sanguine glow of post-Cold War victory. Secretary of Energy, Hazel O'Leary referred to the effort as a way, "to lift the veil of Cold War secrecy," at the U.S. Department of Energy (DOE).[80] Bulk declassification resulted in the release of millions of declassified pages, but the method resulted in the inadvertent release of information that should have remained classified. Norta Trulock, a former director of intelligence at the DOE, claimed that openness had "run amok" due to the fact that after three years, the DOE released more than 300 declassified documents that contain nuclear-weapons secrets.[81]

To address this problem, Clinton signed the National Defense Authorization Act in 1998. The Act had a provision designed to protect against the inadvertent release of Restricted Data (RD) and Formally Restricted Data (FRD). The law required the development and implementation of a plan to prevent the unintended release of RD and FRD from inadvertent disclosure during the automatic declassification of 25 year old records.[82]

---

[77] *Rove 'Leak' Sparks US Spy Hearings*, THE INDEPENDENT (London), July 26, 2005, at 25.

[78] Jerry Markon, *U.S. Boosts Charges Against Defense Analyst*, WASH. POST, June 14, 2005, at B3.

[79] Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995).

[80] Richard A. Meserve, *Preface to* THE NAT'L ACAD. OF SCI., A REVIEW OF THE DEP'T OF ENERGY CLASSIFICATION: POLICY AND PRACTICE ix (1995).

[81] Notra Trulock, *Clinton Policy Declassified Nuclear Secrets*, INSIGHT ON THE NEWS, May 27, 2002, at 45.

[82] Memorandum from Steven Garfinkel, Dir., Info. Sec. Oversight Office, to Senior Agency Officials of Entities Granted Original Classification Authority by the President (Oct. 28, 1998), *available at* http://www.fas.org/sgp/isoo/suspdecl.html.

IX. SECRECY POLICY AND 9-11

In the short period of time between 9-11 and this writing, secrecy policy has undergone more changes than any other period in U.S. history. In order to meet the information policy challenges of the post 9-11 era, President George W. Bush's administration relied on a variety of tools, including: Executive Orders, legislation,[83] administrative action at the agency level,[84] persuasion,[85] solicited advice from private sector pundits,[86] and federal advisory committees.[87] Bush, like other presidents, has made repeated use of the E.O., in an ad hoc fashion. Bush used his first E.O. on classification to make significant revisions in secrecy policy.[88] This order increased the tendency to classify by removing Clinton's "significant doubt" standard, which required that a document should not be classified if there is significant doubt about the need to classify information.[89] Moreover, Bush encouraged more secrecy by ordering that information should not be disclosed "if the information reasonably could be expected to result in damage to national security."[90] Bush

---

[83] Public Health Security and Bioterrorism Preparedness Act of 2002, Pub. L. No. 107-188, 116 Stat. 594 (2003); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2002).

[84] Press Release, OMB Watch, Right-to-Know Advocates Win Battle for Access to Chemical Security Data (July 11, 2005*), available at* http://ombwatch.org/article/articleprint/2909/1/192 (The EPA removed the Risk Management Plan database which contained information on chemical facilities in October of 2001. The EPA refused FOIA requests from OMB Watch for the information until a law suit was filed, then the information was immediately released.); *see also* Coalition of Journalists for Open Government, *The Card Memo* (Mar. 19, 2002), http://www.cjog.net/background_the_card_memo.html.

[85] Letter from Stewart Simonson, Assistant Sec'y, Dep't of Health and Human Services, to Dr. Bruce Alberts, Nat'l Acad. of Sci. (May 27, 2005), *available at* http://www.fas.org/sgp/bush/hhs052705.pdf (requesting that the Academy refrain from publishing an article which discusses vulnerabilities in the nation's milk supply to terrorism).

[86] *See* COMMITTEE ON RESEARCH STANDARDS AND PRACTICES TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, NATIONAL RESEARCH COUNSEL OF THE NATIONAL ACADEMIES, *supra* note 18.

[87] National Science Advisory Board for Biosecurity, *supra* note 9.

[88] Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[89] Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (April 17, 1995).

[90] *Id.*

also expanded classification opportunities by granting original classification to the Vice President, the White House Science Advisor,[91] Health and Human Services,[92] the Environmental Protection Agency,[93] and the Department of Agriculture.[94] Bush also eased the ability to reclassify information and delayed the automatic declassification of documents more than 25 years old from April 17, 2003 to December 31, 2006. In addition, Bush gave veto authority to the Director of the CIA on declassification actions taken by the Interagency Security Classification Appeals Panel.

Criticisms abound from the tightening of information that has taken place due to Bush's information policies.[95] These criticisms also address Bush's adoption of stove-piping practices in the tradition of Truman and Reagan by allowing department heads to establish "Special Access Programs" (SAPs).[96] President Bush allowed SAPs, although he ordered that the number of these be kept "at an absolute minimum."[97] This practice raises concern that pockets of information are being secreted beyond the reach of other intelligence agencies, public access, and declassification protocols, in addition to adding to the tendencies to over-classify. Academics,[98] the 9-11 Commission,[99]

---

[91] Exec. Order No. 12,958, 68 Fed. Reg. 55,257 (Sept. 17, 2003).

[92] Exec. Order No. 12,958, 88 Fed. Reg. 64,347 (Dec. 12, 2001).

[93] Exec. Order No. 12,958, 67 Fed. Reg. 31,109 (May 6, 2002).

[94] Exec. Order No. 12, 958, 67 Fed. Reg. 61,465 (Sept. 26, 2002).

[95] TANIA SIMONCELLI, & JAY STANLEY, AMERICAN CIVIL LIBERTIES UNION, SCIENCE UNDER SIEGE: THE BUSH ADMINISTRATION'S ASSAULT ON ACADEMIC FREEDOM AND SCIENTIFIC INQUIRY 1 (2005), http://www.aura-astronomy.org/nv/sciundersiege.pdf ("The Bush Administration has sought to impose growing restrictions on the free flow of scientific information, unreasonable barriers on the use of scientific materials, and increased monitoring of and restrictions on foreign university students."); *see* Anne N. Barker, *Executive Order No. 13,233: A Threat to Government Accountability*, 22 GOV'T INFO. Q. 4 (2005).

[96] Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (Apr. 2, 1982).

[97] Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[98] Feinberg, *supra* note 41.

[99] Eileen Sullivan, *Too Much Secrecy: Overclassification Hampers Cooperation*, FED. TIMES (Sept. 13, 2004), *available at* http://www.federaltimes.com/index.php?S=347512 (The 9/11 Commission Report found: "Current security requirements nurture overclassification and excessive compartmentation of information among agencies.").

Congressmen,[100] and even the Secretary of Defense have voiced complaints about the practice of compartmentalization of information.[101] Ordinarily, some critics would be assuaged by the fact that each agency is supposed to have accounting procedures to track its compartmentalized secrets,[102] but it appears that the requirement is not consistently followed.[103] Although quick fixes are tempting and usual Executive practice, reformers need to be mindful of the tendency of government agencies to retain secrecy in new ways in response to efforts to take their secrecy away.[104] Thus, compartmentalization is a problem in need of a considered systemic solution.

Bush attempted to remedy the problems stemming from compartmentalized information through an E.O. in June of 2005.[105] This order focused on some of the same problems as the congressional hearings in 1997[106] by trying to bring uniformity to the classification system. Bush's order was unique, however, in that it is a temporary year-long order that allows the Director of the Office of Management and Budget (OMB) to implement the Executive's policy to standardize

---

[100] Press Release, Congressman Christopher Shays, Shays Holds Hearing on Overclassification (Mar. 2, 2005), http://www.house.gov/shays/news/2005/march/marchhear.htm ("Shays … held an oversight hearing about the proliferation of categories of information that are not classified but are withheld from public disclosure.").

[101] U.S. Dep't of Defense News Transcript, Donald H. Rumsfeld, Sec'y of Defense, Sec'y Rumsfeld Press Conference in Phoenix, Ariz. (Aug. 26, 2004), http://www.defenselink.mil/transcripts/ 2004/tr20040826-secdef1261.html ("But the real tension that exists is we have these stovepipes where only certain people know this and certain people know that.").

[102] Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[103] Editorial, *Too Much Secrecy*, WASH. POST, Aug. 28, 2004, at A24 (Quoting William Leonard, "What I find most troubling … is that some individual agencies have no idea how much information they generate is classified, whether the overall quantity is increasing or decreasing…").

[104] Karen K. Lewis, *Why Doesn't Society Minimize Central Bank Secrecy?*, 29 ECON. INQUIRY 403 (1991) (observing in her study of central bank secrecy, "if society tries to constrain secrecy in one way, central bankers will try to regain lost effectiveness by building up secrecy in other ways").

[105] Exec. Order No. 13,381, 70 Fed. Reg. 37,953 (June 27, 2005); Press Release, President George W. Bush, Executive Order: Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information (June 28, 2005), www.whitehouse.gov/news/releases/2005/06/print/20050628-4.html.

[106] COMM'N ON PROTECTING AND REDUCING GOV'T SECRECY, S. DOC. NO. 105-2, at 11 (1st Sess. 1997).

and improve the sharing of classified information between departments in the Executive Branch. The Order states, "agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal."[107] This order also attempts to address the loophole found in SAPs that leads to stovepipes of classified information. Both Sensitive Compartmentalized Information (SCI) and SAPs, with the exception of operational, strategic, and tactical military SAPs, were addressed by this order. Since this order did not change the general access restrictions, i.e. need-to-know, signed non-disclosure agreements and agency head approval prongs,[108] OMB will likely focus on the subjective areas in the agency approval and need-to-know prongs.

Bush's repeated orders to share information may indicate that it may take more than merely stating the goal to obtain a successful outcome. An order from August 27, 2004 addressed sharing of information between agencies in the intelligence community.[109] Also, another order on August 27, 2004 ordered cooperation between the heads of agencies holding terrorism information and the new Counterterrorism Center.[110] Agencies are specifically instructed to give prompt terrorism information to the director of the Center. This builds upon an order from May 14, 2003 which addresses the sharing of "terrorism information" between agencies and with appropriate designees in state and local governments.[111] Although sharing orders between agencies have a high failure rate, similar orders directing action within an agency tend to be more effective due to the identifiable accountability placed in the agency director and his ability to authorize compliance with the order through a chain of command. In contrast, inter-agency orders on sharing lack accountability and authority for execution among co-equal agency heads. Therefore, temporary management E.O.s like E.O. 13,381 may prove to be the effective model in these circumstances.

The ripple effect of the failed orders can be seen in local and state remedies to the problem. In response to the failure to receive adequate

---

[107] Exec. Order No. 13,381, 70 Fed. Reg. 37,953 (June 27, 2005).

[108] Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[109] Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Aug. 27, 2004).

[110] Exec. Order No. 13,354, 69 Fed. Reg. 53,589 (Aug. 27, 2004).

[111] Exec. Order No. 13,301, 68 Fed. Reg. 26,981 (May 14, 2003).

and timely classified information from the federal government, Chief William J. Bratton of the Los Angeles Police Department recently initiated a grassroots network of information sharing between major police departments to fill the gap.[112] But, such grassroots efforts need to be coordinated since they run the risk of duplicating the work of state based "fusion centers" where homeland security information is also collected and analyzed.[113]

One of the more controversial[114] efforts in Bush's information policy concerned an attempt to tackle the gray areas of science and secrecy via the "sensitive but unclassified" approach (SBU) via the Card memo.[115] The Card memo reminded agency heads of their obligation to safeguard sensitive documents related to weapons of mass destruction, regardless of its age, and is credited for being the impetus for the removal of over 6,000 pages of government web pages from the Internet.[116] The Card memo caused such uproar in the scientific community that it is easy to understand why many, such as the ACLU, fell under the misapprehension that the Bush administration actually created this label.[117] But, the SBU label has

---

[112] John M. Broder, *Police Chiefs Moving to Share Terror Data, Los Angeles Official Spearheads Effort to Create a Network*, N.Y. TIMES, July 29, 2005, at A15.

[113] *A Progress Report on Information Sharing for Homeland Security, Testimony Before the H. Comm. on Homeland Sec., Subcomm. on Intelligence, Info. Sharing and Terrorism Risk Assessment*, 109th Cong. 4 (July 20, 2005) (statement of John D. Cohen, Senior Homeland Security Policy Advisor for the Commonwealth of Mass.) ("[A]lmost every state is establishing an 'information fusion center' – a location where homeland security-related information can be collected and analyzed.").

[114] *See* William J. Broad, *Threats and Responses: Security Measures; Researchers Say Science is Hurt by Secrecy Policy Set Up by the White House*, N.Y. TIMES, Oct. 19, 2002, at A8; Megan Twohey, *Security Restrictions from Government Put Researchers in a Bind*, SAN DIEGO UNION-TRIB., Dec. 10, 2003, at F1 ("More than 50 troublesome [federal research] contracts [with universities] have been identified so far."); William Matthews, *'Sensitive' Label Strikes a Nerve*, FED. COMPUTER WEEK, Oct. 31, 2002, http://www.fcw.com/article78010-10-30-02-Web.

[115] Memorandum from Andrew H. Card, Jr., Asst. to the President and Chief of Staff, to the Heads of Executive Departments and Agencies (Mar. 19, 2002), http://www.fas.org/sgp/bush/wh031902.html.

[116] *See* Coalition of Journalists for Open Government, *supra* note 84.

[117] TANIA SIMONCELLI, ET AL., SCIENCE UNDER SIEGE, *supra* note 95, at 6.

actually been used by a number of government agencies since at least 1977.[118]

The SBU designation is also controversial due to the fact that it has inconsistent definitions throughout the government. Definitions vary from broad uses at the DOE[119] to an entirely different and narrower use at the Department of State.[120] Even if a uniform definition on SBU is reached, the question remains how SBU fits into an accountable and transparent classification system. OMB has been charged with the difficult task of providing clarification on this issue,[121] but no direction has been made public as of this writing from OMB.

X. THE INFORMATION SOCIETY AND BIOSECURITY

One of the arguments used against government classification of scientific knowledge relies on the fact that sophisticated articles, on the most lethal of pathogens, have natural barriers due to the tacit knowledge, lacking in the "typical" terrorist, needed to make use of the information.[122] This argument, however, is losing credibility with each passing day. First, it is undisputed that "biotechnical know-how is spreading quickly."[123] Furthermore, it is unwise to underestimate and stereotype terrorists. The fact that one of the suspects in the recent London subway bombings was a graduate student in biochemistry at a

---

[118] Genevieve J. Knezo, *"Sensitive but Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, CONG. RES. SERVICE, Apr. 2, 2003, at 10.

[119] *Id*. at 20 (The DOE definition concerns, in part, "Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests.").

[120] *Id*. at 47 (The Department of State definition of SBU includes: "[m]edical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, … could have a negative impact upon foreign policy or relations.").

[121] *Before the H. Comm. on Sci*., 106th Cong. (Oct. 10, 2002) (statement of The Honorable John H. Marburger, Director, Office of Science and Technology Policy), *available at* http://www.house.gov/science/hearings/full02/oct10/marburger.htm ("On the subject of sensitive information, OHS has asked OMB to develop guidance for Federal agencies to ensure consistency of treatment of 'sensitive homeland security information' across the Federal government and by recipients of such information.").

[122] Judith Reppy, *Dual Use Information: Issues for NSABB*, CORNELL UNIV., June 30, 2005, *available at* http://www.biosecurityboard.gov/meetings/200506/Reppy.pdf ("The tacit component of cutting-edge research offers some protection against bioterrorists.").

[123] Christopher F. Chyba, *Toward Biological Security*, 81 FOREIGN AFF. 122, 127 n.3 (2002).

major research university should help disabuse the allure of the tacit knowledge argument.[124]

The bounty of the information society may also make philosophers and policymakers question the wisdom of unlimited access to advanced scientific information. Thus, the question is whether the nation is back to where it was in the 1980's with concerns over the transfer of science and technology to the opposition. Needless to say, a great commotion would have likely ensued in the Reagan era if a Soviet spy had been caught walking out of a U.S. university library with copies of entire volumes of scientific journals. Now, however, recent advances in communication technologies can aid in the acquisition and instantaneous delivery of entire volumes of the world's most sophisticated science and technology journals to any interested party the world over. Today that scenario would in fact pose a greater threat since an adversary would be walking off with more dual use articles having WMD potential than ten years ago.[125]

Unfortunately, this situation may not be hypothetical. A number of universities have recently experienced bulk downloading of scientific journals. It has been disclosed that unsanctioned downloading has occurred at Simon Fraser University,[126] Northwestern University[127]

---

[124] *Egypt will not Hand over London Suspect*, UNITED PRESS INT'L, July 16, 2005, *available at* http://www.news24.com/News24/World/Londonattacks/0,,2-10-1854_1738691,00.html (A suspect of the July 7, 2005 subway bombings is a graduate student in biochemistry in Leeds, UK.).

[125] Jeronimo Cello, Aniko V. Paul & Eckard Wimmer, Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template, 297 Science 1016 (2002); Ronald J. Jackson et al., Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox, 75 J. of Virology 1205 n.3 (2001); Lawrence M. Wein & Yifan Liu, Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk, 102 Proceedings of the Nat'l Acad. of Sci. of the U.S. 9984 n.28 (2005); Taubenberger et al., supra note 11; Tumpey et al., supra note 10.

[126] Simon Fraser Univ. Library Collections Management Activity Report (Oct. 2004), http://www.lib.sfu.ca/about/collections/monthly_reports/CollMgmt0410.htm (In October of 2004, an e-journal publisher detected bulk downloading by a user and cutoff services for 4 days at Simon Fraser University. The University reports that it identified the user and resolved the situation.).

[127] Lloyd A. Davidson, *The End of Print: Digitization and Its Consequence—Revolutionary Changes in Scholarly and Social Communication and in Scientific Research*, 24 INT'L J. OF TOXICOLOGY 25 (2005) ("In one case we had somebody come into a library at Northwestern and proceed to download a significant fraction of the online contents of a physics journal database…").

and the University of Nevada, Reno.[128] It is not clear whether the downloading at Nevada involved scientific journals, but the Simon Fraser and Northwestern incidents, respectively, concerned optical engineering and physics. It appears, however, that this problem concerns far more university libraries than indicated by the aforementioned examples.

Thus, in order to informally investigate this matter further, a general inquiry[129] was made about this issue on a List Serve for research libraries,[130] and a number of public postings and private responses ensued indicating that this is not an isolated problem. Due to a number of issues, many respondents did not want public attribution of the bulk downloading experiences to their institutions. It does appear, however, that sophisticated scientific journals may be well represented in bulk downloading incidents. In one instance a university was notified of the apparent download of two entire journal volumes from the Society for Industrial and Applied Mathematics.[131] The downloaded journals were from the *Journal on Matrix Analysis and Applications*, which is described as providing papers of interest to the numerical linear algebra community with applications for a number of areas including mathematical biology.[132] The other

---

[128] Posting of Rick Anderson, rickand@unr.edu, to Liblicense-1@lists.yale.edu (July 1, 2005) (on file with author), *available at* http://www.library.yale.edu/~llicense/ListArchives/ 0507/msg00006.html ("In answer to Dr. Gorman's question, yes, we have had occasional problems with users massively and systematically downloading entire runs of online journals -- in at least one case, the student was burning the journal content to CD's so that he could take it home to a country known for its lax copyright law enforcement.").

[129] Posting of Lloyd Davidson, Ldavids@northwestern.edu, to Liblicense-1@lists.yale.edu (June 29, 2005) (on file with author), *available at* http://library.yale.edu/~llicense/ ListArchives/ 0506/msg00180.html ("Q: Have any of your libraries discovered cases of suspicious downloading patterns from scientific journals or other technical resources by walk-in or other users (e.g. massive downloading to capture a journal's archive)?").

[130] Liblicense: Licensing Digital Info., http://www.library.yale.edu/~llicense/index.shtml (last visited Oct. 24, 2005).

[131] SIAM Journals Online: The Accelerated Electronic Journals of the Society for Industrial and Applied Mathematics, http://epubs.siam.org (last visited Oct. 24, 2005).

[132] SIAM J. on Matrix Analysis and Applications, http://epubs.siam.org/sam-bin/dbq/ toclist/SIMAX (last visited Oct. 24, 2005) ("The SIAM Journal on Matrix Analysis and Applications publishes research articles in matrix analysis and its applications and papers of interest to the numerical linear algebra community. Applications include such areas as signal process, systems and control theory, statistics, Markov chains, and mathematical biology. Also contains papers that are of a theoretical nature but have a possible impact on applications.").

downloaded journal was *Theory of Probability and Its Applications*, which is described as a journal containing papers on the theory and application of probability, statistics, and stochastic processes.[133]

Clearly these downloading incidents may have had many motivations from nefarious to benign and naive. In fact, a number of respondents suggested explanations for such downloading as research projects on information sciences and neural processing. Moreover, bulk downloading may simply be a convenient tool in certain circumstances. For instance, the National Institutes of Health has an open access webpage with a guide to a number of websites offering bulk downloading of chemical structural databases.[134] It does appear, however, that the bulk downloading of scientific information is an issue worthy of further debate and investigation. This inquiry must also address the ethical and legal issues in light of past controversies[135] and current legislation concerning the investigation of library usage.[136] As previously discussed, academic issues are more global now than ever. Thus, actions taken in the U.S. need to be compatible with the academic community beyond the borders of the country because the U.S. is not the sole producer of scientific knowledge.[137]

XI. THE BIOHACKER THREAT

Another threat from exposure to advanced scientific information comes from what is known as the biohacker. Unfortunately, similar

---

[133] Theory of Probability and Its Applications, http://epubs.siam.org/sam-bin/dbq/toclist/TVP (last visited Oct. 24, 2005) ("Theory of Probability and Its Applications is a translation of the Russian journal Teoriya Veroyatnostei i ee Primeneniya, which contains papers on the theory and applications of probability, statistics, and stochastic processes.").

[134] Chemistry Databases, http://cactvs.cit.nih.gov/ncidb2/chem_www.html (last visited Oct. 24, 2005).

[135] *See* American Library Ass'n Documents Round Table, GODORT Resolution, http://sunsite.berkeley.edu/GODORT/resolutions/880713774.html (last visited Oct. 24, 2005).

[136] Eric Lichtblau, *Senate Makes Permanent Nearly All Provisions of Patriot Act, With Few Restrictions*, N.Y. TIMES, July 30, 2005, at A11 (The provision allowing the demand of records from libraries is renewed and set to expire in four years unless Congress reauthorizes the provision at that time.).

[137] Bernd Wegner, *EMIS 2000: The European Mathematical Information Service and Its Developments*, 25 ONLINE INFO. REV. 165 n.3 (2001) ("The main purpose of EMIS is to provide freely available information on mathematics in the Web. … freely available digital content of classical mathematical publications and access to grey literature.").

dynamics that led to computer hackers are rapidly developing in the life sciences as well. Life and computer sciences are similar in that they both originally had high barriers to entry to sophisticated applications, but they both saw reductions in barriers as technology improved and proliferated throughout private industry. The spread of computer usage into personal use led to the widespread use and anonymity of usage which also enabled hackers to make and spread computer viruses from the privacy of their own homes. Precocious youths with access to sophisticated equipment appear to fall victim to the temptations of computer hacking more than most. The recent conviction of a German teenager for causing billions of dollars in damage with the "Sasser" virus is a prime example. A 17 year old from Germany named Sven Jaschan created a computer virus that affected millions of computers around the world and caused more than $6.25 billion in damages.[138] Unfortunately, however, domestic saboteurs and malicious thrill seekers from the adult population are problems as well.[139]

It is unlikely that personal biolabs will be as common as the ubiquitous personal computer any time soon, if at all, but it is likely that precocious youths around the world in wealthier countries will have access to advanced dual use equipment that is the center of today's controversy in biosecurity. The most gifted high school students are already conducting research related to poxviruses.[140] Thus, it is a matter of time before more and more students acquire similarly advanced skills and access to equipment at their schools and homes.[141] In this connection, the falling costs and unrestricted access

---

[138] Daniel Thomas, *Businesses 'Let Down' by Virus Writer Ruling*, COMPUTING, July 13, 2005, at 6.

[139] Jeffrey Gold, *Man Who Admitted Shining Laser at Aircraft Indicted on Patriot Act Charge*, THE ASSOCIATED PRESS (BC Cycle), Mar. 23, 2005, *available at* http://phillyburbs.com/pb-dyn/articlePrint.cfm?id=467145 ("A cluster of reports of lasers striking airplanes received wide attention between Christmas and New Year's Day.").

[140] 64th Annual STS (2004-2005) Finalists Kelley Harris, http://www.sciserv.org/sts/64sts/Harris.asp (last visited Oct. 24, 2005) (A recent teenage finalist in the Intel Talent Search conducted a study related to a poxvirus.).

[141] Meeting of the National Security Advisory Board for Biosecurity, July 30, 2005, http://www.webconferences.com/nihnsabb/380405.html (last visited Oct. 24, 2005) ("My colleague said that not only are these things already the tools to do life science research already in colleges, but I wouldn't be surprised if it's not too many years before we see this sophisticated ability in high school laboratories. Given that, the question then becomes is it only the intentional adversary that we have to think about. As my friend said a moment ago, no, it's probably not. We have to worry about the mischievousness. We have to worry about

to biochemical technology raises many concerns. Professor George Church and Interpol have proposed licensing of certain biological equipment.[142] This effort would be consistent with increased and forthcoming federal control of chemical[143] and biological agents.[144] Professor Church warns that, "the future biodesigner will not need a detailed knowledge of biochemistry to effectively create complex biochemical machines."[145] Complex and expensive procedures are becoming easier and cheaper to accomplish. For instance, synthetic biology equipment capable of producing strings of nucleotides can be purchased over the Internet for discount prices.[146] Knowledge about the discipline is proliferating and the circle of accomplished scientists is growing wider over time. In light of the growing access teenagers are getting to dual use laboratories, greater emphasis must also be placed on the ethics of bioscience at the earliest ages as well. Thus, the goal of devising ethical codes and training for professionals must be widened to include younger students as well.

Potential economic liability for the misuse of synthetic biology may help foster the development of ethical codes and licensing efforts. Germany recently introduced a law that holds an individual liable for damages from the accidental spread of genetically modified crops.[147] Beside the ever present biosecurity threat to the food supply,[148]

---

those who are simply curious and those who are not old enough who have quite developed the super functioning ego.").

[142] Church, *supra* note 28; Ted Agres, *Interpol Pushes Research Controls*, THE SCIENTIST, July 21, 2003, http://www.the-scientist.com/news/20030721/03.

[143] *Bush Administration Endorses Chemical Security Requirements*, OMB WATCH, June 15, 2005, http://www.ombwatch.org/homeland/OMBWChemSecurityState.pdf.

[144] *See* Public Health Security and Bioterrorism Preparedness Response Act of 2002, Pub. L. No. 107-188, 116 Stat. 594 (2003); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2002).

[145] Chappell Brown, *Experts Worry that Synthetic Biology may Spawn Biohackers*, EE TIMES, June 29, 2004, http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=22102744.

[146] *See* Grizzly Analytical Biotech Lab Equipment, http://www.grizzlyanalytical.com (last visited Aug. 2, 2005) (Grizzly Analytical sells used, reconditioned and rebuilt biotech lab equipment.).

[147] Ned Stafford, *GM Law 'A Blow for Science'*, THE SCIENTIST, Dec. 1, 2004, http://www.the-scientist.com/news/20041201/01.

[148] Michael Doyle, New Alert Bares Risk to State's Ag Industry, Despite Increased Security Nationwide, Our Food Supply Still Isn't Safe Officials Say, The Sacramento Bee, Mar. 19,

accidental genetic modification of crops could likewise lead to devastation of certain crops. The accidental spread of genetically modified crops, such as the recently created ball of corn, which is a mutation away from the traditional stalk of corn, could have a disastrous impact on the agricultural industry.[149] Liability in the lab is another issue that will grow as more researchers work with self-replicating organisms. Courts have been reluctant to hold academics responsible for the harm resulting from the application of controversial techniques in the past,[150] but the question remains how the courts will deal with life science cases.

PART 2: THEORY

XII. TOWARD THEORETICAL ANALYSIS

U.S. secrecy policy may be the most criticized and under analyzed area of federal policy. Congress holds hearings on secrecy from time to time,[151] the ISOO keeps track of statistics, and others provide plenty of criticism, but there is little substantive analysis on the theoretical underpinnings of secrecy policy. More analysis is needed on the function of secrecy and acquisition of information by the government. The concept of capturing and classifying science can, at times, be a very emotional issue that strikes at the heart of one's pride, livelihood, and philosophy. The juxtaposition of two disparate comments on scientific knowledge and secrecy in the aftermath of two notoriously destructive events demonstrates the sharp differences.

> There has been a lot of talk about the evil of secrecy, of concealment, of control, of security.…the almost unanimous

---

2003, at D2 (" 'Experts … generally agree that terrorists could use food products as a vehicle for introducing harmful agents into the food supply,' the GAO warns.").

[149] Jamie Talan, *Gene Makes Tidy Earful*, NEWSDAY, July 25, 2005, at A29 (Scientists created a large ball of corn in lieu of a stalk by modifying its genetic make up.).

[150] *See* Storch v. Syracuse University, 629 N.Y.S.2d 958 (N.Y. Sup. Ct. 1995). *See also* Brian J. Gorman, *Facilitated Communication in America: Eight Years and Counting*, SKEPTIC, July-Sept. 1998, at 64 (Liability is discussed relative to the distinction between academic theory and academic action.).

[151] REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, APPENDIX G: MAJOR REVIEWS OF THE U.S. SECRECY SYSTEM (1997), *available at* http://www.access.gpo.gov/congress/commissions/secrecy/ (last visited Oct. 19, 2005).

> resistance of scientists to the imposition of control and secrecy is a justified position…it is the highest value to share your knowledge, to share it with anyone who is interested….and are willing to take the consequences. -Phycisist, J. Robert Openheimer, November 1945.[152]

~

> We have to get away from the ethos that knowledge is good, knowledge should be publicly available, that information will liberate us… Information will kill us in the techno-terrorist age, and I think it's nuts to put that stuff on Web sites. -Bioethicist, Arthur Caplan, November 2001.[153]

Secrecy policies have historically relied upon the simple bifurcation of military and civilian science. The bright line that separated military science from civilian science, however, has been blurred due to the dual uses of science. The problem is compounded by the fact that the growing sophistication of science, especially the life sciences, has increased in lethality.[154] Additionally, the means of communicating this lethal dual use information has become so facile in the information society that the temporal advantages and tacit barriers relied upon with science have all but vanished with regard to biosecurity.

All national security secrets appear to consist of two core elements: time and risk. If there is no risk derived from disclosure of the information, then there is no reason to have it classified. Moreover, if it is impossible to secure the information for any length of time, no matter how great the risk, logic dictates that it can not be secret. The apparent simplicity of these elements should not deter analysis into how these elements function. Rather, a better understanding of these elements should help in addressing challenges in formulating federal secrecy policy for both scientific and nonscientific information.

---

[152] J. Robert Oppenheimer, Speech to the Association of Los Alamos Scientists, (Nov. 2, 1945), *available at* http://www.honors.umd.edu/HONR269J/archive/OppenheimerSpeech.html.

[153] Eric Lichtblau, *Rising Fears that What We do Know can Hurt Us*, L.A. TIMES, Nov. 18, 2001, at A1.

[154] Tumpey et al., *supra* note 10.

XIII. RISK

The critical concept of risk is mentioned here in passing but it requires far more attention than this paper can provide. For purposes of this article, however, risk will be defined with Skinnerian simplicity as the increased probability of danger as result of exposure.[155] Unlike atomic weapons research, the scientific community cannot agree on a bright-line demarcation for sensitive bioweapons research because these findings may also benefit society through medical advancements.[156] In this connection, it is important to note the "intent fallacy" which repeatedly thwarts further analysis of risk on life science research. The claim of good intent has served as the shield and justification for the publication of several controversial life science articles of late. But this rationale, which overrides dangers as grave as pandemics, is unforeseen and without precedent in society. When searching for precedents on this matter, one is left with few choices. Thus, to find precedents for a commensurate disregard of a risk to human life for the benefit of society, one may have to go as far as Truman's decision to use the atomic bomb in World War II. Outside of the parameters of war, however, criminal law limits the shield of good intent when balancing against a knowing disregard for a risk to others. Of course, one may have to disregard a known risk when there is justification, but it is unforeseeable in our jurisprudence that pandemics or mass casualties could be justified for the vague promise of unspecified benefits for society. Cleary, in a criminal or tort context, the duty of care would oblige the scientific community to put up some sort of minimal guards for the attractive nuisance of research with bioweapons potential. Unfortunately, there are no set standards by which to measure the potential risk a scientific paper poses to national security.[157] Even the Patent Office filter remains largely

---

[155] *See also* S.N. Jonkman et al., *An Overview of Quantitative Risk Measures for Loss of Life and Economic Damage*, A99 J. OF HAZARDOUS MATERIALS 1, 2 (2003) (A review of risk literature resulted in the following definition of a risk measure: "a mathematical function of the probability of an event and the consequences of that event.").

[156] Charles M. Vest, President, Mass. Inst. of Tech., Report of the President for the Academic Year 2001-2002: Response and Responsibility: Balancing Security and Openness in Research and Education (Sept. 2002) ("[N]uclear weaponry seems to be an almost singular case. …The knowledge of what makes a virus virulent is also the key to medical therapies and disease prevention.").

[157] Arturo Casadevall and Liise-anne Pirofski, *The Weapon Potential of a Microbe*, TRENDS IN MICROBIOLOGY 6 (2004) (The authors present a formula for evaluating the weapons potential of microbes. This formula was designed for the evaluation of select agents, but

undefined despite having been in use for years. E.O.s are not much better since they address risk in an imprecise manner and lack quantifiable standards and operational definitions. The concepts of risk are vaguely addressed through the tiered classification system, but more precise guidance would certainly prove helpful in addressing chronic over-classification issues. Thus, it is no surprise that the scientific community is having difficulties evaluating the potential risk of publishing scientific information.

The absence of objective standards apparently steers classifiers to determinations offering the least discomfort. As a result, government workers will tend to over-classify to avoid mistakes that harm their careers, and publishers will likewise protect their livelihoods by leaning against classification. Risk assessment is often recognized as a challenging gray area, but little more has been done or said about it. Thus the challenge is to understand risk and then accurately measure, identify, and group sensitive information with like kind and in the best interests of society.

There has, however, been some recent progress on the identification and assessment of risk in life science research. The National Academy of Sciences Report on Terrorism identified seven "experiments of concern" to help identify articles of concern in 2004.[158] In addition, these findings were operationalized and combined with other factors to create an eighteen item Likert-type Risk Assessment Scale in the spring of 2005.[159] Unfortunately, members of the scientific community have fallen prey to the "vividness heuristic" [160] of an "I know it when I see it" approach when identifying risky science and an untenable ad hoc standard for the disposition of contentious science.[161]

---

further analysis needs to address whether it can be applied to a risk analysis of academic papers.).

[158] *See* COMMITTEE ON RESEARCH STANDARDS AND PRACTICES TO PREVENT THE DESTRUCTIVE APPLICATION OF BIOTECHNOLOGY, *supra* note 21.

[159] *See* Gorman, *supra* note 28.

[160] *See generally* MICHAEL PERLIN, THE JURISPRUDENCE OF THE INSANITY DEFENSE, 269-75 (1994) (Professor Perlin explains the phenomenon of the oversimplification of complex issues via the vividness heuristic.).

[161] *See* Paula Park, *New Standards for Publication of Sensitive Research*, THE SCIENTIST, Feb. 17, 2003, http://www.the-scientist.com/news/20030217/08 ("Atlas compared the process to defining pornography. 'I know it when I see it,' he said.").

Although the prevailing Editor's Group standard for the disposition of high risk science was arguably a pretext for continued self-governance of scientific matters, [162] despite denials,[163] the prevailing standard must be addressed. The Editor's Group standard, i.e. the "preponderance of harm standard," holds that censorship or modification of an article is warranted when the potential harm of a paper outweighs its potential benefits for society.[164] Unfortunately, it appears that the Editor's Group preponderance of harm standard was bootstrapped into rushed deliberations by the NSABB over the Spanish flu articles.[165]

This preponderance of harm standard must be abandoned because it oversimplifies the issues, fails to operationalize or define risk, and invites redundant consideration of the presumption that all knowledge could benefit mankind. Moreover, the benefit prong merely invites wide-eyed speculation on how beneficial the potential article can be for mankind. No extant classification criteria include such a standard. Moreover, the benefit prong is specious because the potential benefits to society an article holds are not relevant to the initial stage of analysis. The paper can still serve society with miraculous benefits without being published and widely distributed to friend and foe alike. For instance, a delay or classification of the methodologies in the Spanish flu articles would not have preempted the creation of vaccines and all the benefits purported by its authors and supporters. Rather, the questions to ask include whether or not: (1) public awareness of the article presents a risk; (2) public dissemination of methodologies presents a risk; and (3) dissemination of methodologies should be limited to professionals with a need to know.

XIV. THE FUNCTION OF TIME

The temporal factor is another essential element of secrecy theory. It is a critical element similar to risk because its absence negates the

---

[162] Deborah Byrd and Joel Block, *Interview with Ronald Atlas*, *supra* note 21 (Atlas said, "…nor should we look to the US government to impose a regulatory scheme…").

[163] Paula Park, *supra* note 161.

[164] *Statement on the Consideration of Biodefense and Biosecurity*, 421 NATURE 771 (2003) ("FOURTH: We recognize that on occasions an editor may conclude that the potential harm of publication outweighs the potential social benefits. Under such circumstances, the paper should be modified, or not be published.").

[165] Russo, *supra* note 38.

ability to protect information.[166] The time factor was likewise noted in the *Progressive* opinion.[167] The goal of a national security secret is to preserve the strategic advantage of time over adversaries and competitors. Secrets are not permanent, but they are worthless if they do not run long enough to maintain a favorable strategic edge.[168] Assessments of scientific secrets in 1970 acknowledged that secrets were likely to remain secure for about a year.[169] Thus, the information society presents especially unique challenges to modern secrecy policy. Designers of secrecy policy had greater margins for error back when the portability of information was cumbersome and slow. Now, however, the information society reduces margins for error since flaws in secrecy policy can have immediate and irreparable effects on national security. For instance, if a journal accidentally published a classified formula back in the 1950's, a considerable amount of time would pass before the publications reached their destinations in the limited community of mostly academic and government researchers. Thus, the concept of recall was feasible. Now, however, with the global reach of instant on-line dissemination, the physical retraction and ability to recover is limited. Moreover, this problem is compounded by the falling costs and rising competencies of individuals capable of using potentially lethal scientific applications.

There are at least two factors to consider in connection with the temporal element. The duration of the secret is the first factor, and the means of controlling the secret is second. Considerations in the duration factor include the length of time it takes for an adversary or competitor to develop the same targeted technology. If the technology raises concerns over weapons or accidents of mass destruction

---

[166] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON SECRECY, *supra* note 15 ("Secrecy will usually be most valuable in maintaining a technological lead during the period of development.").

[167] *Progressive*, 467 F. Supp. at 994 ("There are times in the course of human history when time itself may be very important. This time factor becomes critical when considering mass annihilation weaponry…").

[168] LEWIS M. BRANSCOMB, U.S. SCIENCE AND TECHNOLOGY POLICY: ISSUES FOR THE 1990'S 30 (1995), *available at* http://www.schwartzman.org.br/simon/scipol/branscomb.pdf ("[The Defense Science Board's Bucy Report] proposed that controls should be focused on retarding transfers of technology which could significantly enhance the military capability of potential adversaries.").

[169] REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON SECRECY, *supra* note 166.

(WAMD),[170] such as in the case of synthetic biology, then the duration element may be measured by the length of time it would otherwise take for the technology or information to become commonly attainable knowledge.

XV. THE FUNCTION OF LEAKS

Secrecy theory cuts two ways in like manner to secrecy policy. Just as risk and time are constant elements of federal secrets, so too is the leak. In addition to the aforementioned sources, sources within the government have provided another steady stream of information by way of the leak.[171] It is important to understand the function of the leak lest it undermine new secrecy paradigms. The leak has grown to institutional proportions.[172] Thus, it is necessary to review the function of the leak when evaluating secrecy policy. There appears to be at least six well established causes for leaks: (1) mistake,[173] (2) political gain,[174] (3) financial gain, (4) foreign loyalty, (5) morality,[175] and (6) personal legacy.

---

[170] Ian Sample, *From Frozen Alaska to the Lab: A Virus 39,000 Times more Virulent than Flu*, GUARDIAN UNLIMITED, Oct. 6, 2005, http://www.guardian.co.uk/science/story/0,3605,1585976,00.html ("'Assuming this is a replicant of the 1918 strain, if it got out, it could initiate disease in humans…' said Prof. Atlas… Viruses have escaped from high-security labs before. During the recent Sars [sic] outbreak the virus escaped at least twice, …when researchers became contaminated.").

[171] 139 CONG. REC. 18,764 (1993) (statement of Rep. Glickman) ("Virtually all the leaks that take place in this country occur someplace at the executive branch level.").

[172] Eric Lichtblau & David Johnston, *Administration Takes Broad Reading of Espionage Law*, N.Y. TIMES, Aug. 6, 2005, at A10 ("In the circular, echo-chamber world of official Washington, where government policy makers, members of Congress, analysts, lobbyists and journalists are forever seeking to cull information from one another to gain an edge, such conversations are a routine part of doing business and influencing public policy." Reporters' comments regarding a conversation where classified information was allegedly passed from a government employee and an influential lobbyist.).

[173] Tom Brune, *Homeland Secretary: Release of Terror Report was a Mistake*, THE SEATTLE TIMES, Mar. 17, 2005, at A7 ("[A] once-secret report that Homeland Security officials say came to light accidentally after it was posted Monday on the web by the state of Hawaii and reported in the New York Times yesterday."); (Los Alamos reports a 1/10 to the 7th failure rate in the release of classified information). Thomas Bowles, *supra* note 62.

[174] Lichtblau & Johnston, *supra* note 172.

[175] *See* Michel Foucalt, Discourse and Truth: The Problemization of Parrhesia, Berkeley Lectures 5 (Oct.-Nov. 1983), *available at* http://foucault.info/documents/parrhesia/foucault.discourseAndTruth.pdf ("[*P*]*arrhesia* is a verbal activity in which a speaker expresses

Leaks for financial gain, foreign loyalty and mistake need little explanation. Leaks for political gain are more complex because they are often sanctioned by government officials to assist with the political goal of an administration or political party. Furthermore, leaks may be intended to help political careers. Moral leaks, whether anonymous or of the whistle-blowing variety, are also well known.[176] The leak intended to preserve personal legacy is not as common but is emerging. This leak or revelation is likely to come from the aging figure, once bound by loyalty, who may be treated unkindly by history unless classified information in his favor is released to "correct the record." The leak by an elderly French admiral over his alleged role in the sinking of a Green Peace ship in the 1980's[177] and the self-unveiling by Michael Felt as "Deep Throat"[178] support this notion. In addition to the aforementioned, a new type of antecedent leak has emerged as a result of the conflict between the scientific establishment and the government identified here as the "publisher's veto."

XVI. PUBLISHER'S VETO

The publisher's veto is defined here as the premature publication of sensitive information despite non-binding requests or a public trust expectation to refrain from releasing said information before a security vetting takes place. The publisher's veto has two immediate benefits for the publisher. First, if the release is wide enough, i.e. via a widely available public access e-journal, then it immediately ends the dispute with the government. The government's request to vet the article becomes moot after the article is widely disseminated. Thus, the publisher's veto also enables the dumping of sensitive scientific information resulting in depreciated national security value of the information. Second, the publisher's veto nullifies export restrictions by triggering an exception for published information by enabling the

---

his personal relationship to truth, and risks his life because he recognizes truth-telling as a duty to improve or help other people…").

[176] Blanche Wiesen Cook, *Presidential Papers in Crisis: Some Thoughts on Lies, Secrets, and Silence*, 26 PRESIDENTIAL STUD. Q. 285, 287 (1996) ("In 1986, for example, an anonymous Veterans Administration worker contacted the National Association of Radiation Survivors to scream that all documents relating to atomic veterans were about to be shredded.").

[177] Marlise Simons, *Report Says Mitterand Approved Sinking of Greenpeace Ship*, N.Y. TIMES, July 10, 2005, at A3.

[178] Michael Janofsky, *New Book on Watergate Fleshes out Deep Throat*, N.Y. TIMES, July 2, 2005, at A9.

claim that such information is "ordinarily published."[179] The publisher's veto was exercised recently by the journal PNAS with the Toxic Milk article by Professor Wein.[180] The article detailed ways to poison the milk supply with botulimum toxin. The government became aware of the article before widespread distribution and asked the journal to refrain from publishing the article arguing that it provides a roadmap for terrorists.[181] The journal held the article briefly and then vetoed the government's involvement by publishing it in a fast track open access manner.[182]

More information is needed in order to determine whether Tumpey's recent Spanish flu article in *Science*[183] qualifies as a publisher's veto. It is possible that the editors at *Science* operated in good faith by relying on the apparent authority to proceed given by NIAID Director, Anthony Fauci and CDC Director, Julie Gerberding.[184] Fauci's and Gerberding's prior knowledge of the Spanish flu research and bias in favor of publishing this information begs the question as to what their role should be in providing prepublication notice of potentially contentious research to the national security community.[185] The question also applies to the authors, editors and other federal officials who have prepublication knowledge of potentially contentious research. Clearly, somebody must have a duty to provide adequate prepublication notice of such research to a designated authority from the national security community. If, however, federal authorities such as Fauci and Gerberding provided authority from the federal government for *Science* to proceed until the late hour, then their actions arguably amounted to a de facto national security vetting waiver.

---

[179] Export Administration Regulations (EAR), 15 C.F.R. § 734.8 (2005).

[180] Wein & Liu, *supra* note 125.

[181] Letter from Stewart Simonson, *supra* note 85.

[182] Bruce Alberts, *From the Academy Editorial, Modeling Attacks on the Food Supply*, 102 PROCEEDINGS OF THE NAT'L ACAD. OF SCI. OF THE U.S. OF AM. 9737 (2005).

[183] Tumpey et al., *supra* note 10.

[184] Russo, *supra* note 38.

[185] Anthony S. Fauci & Julie L. Gerberding, *Unmasking the 1918 Influenza Virus: An Important Step Toward Pandemic Influenza Preparedness* (Oct. 5, 2005), http://www3.niaid.nih.gov/news/newsreleases/2005/0510state.htm.

Stewart Simonson, the authority who previously asked for suppression of Wein's toxic milk article a few months prior, eventually received notice of the Spanish flu article and immediately asked for advice from NSABB.[186] With or without knowledge that the article was inexorably en route to the presses, NSABB convened for the second time in its history via emergency deliberations through cross country communications.[187] The result of these deliberations was an approval of the article citing a standard the Board had yet to debate and recommend for government use, i.e. the preponderance of harm standard.[188] Clearly, the Spanish flu scenario highlights flaws in the system that need immediate attention.

The publisher's veto is a consequence, in part, of the prevailing view in secrecy theory which holds that publicly available information is beyond capture because it is futile to classify that which is already public. The same principle is applied in the protection of trade secrets in private industry. But, the difference is that the business holding the trade secret must negligently disclose its own secret to terminate trade secret agreements.[189] The "pure" secret view was likewise found in Carter's E.O. 12,065 which mandated that once information was declassified and released to the public, it could not be reclassified. The problem with this view is that it fails to consider the gradients of exposure of the information. The assumption in Carter's order is that classified information must be contained like air in a balloon. As soon as there is the smallest compromise of the information, like the prick of a balloon, the classification is rendered useless. This view is clearly flawed because previously exposed information can exist in many situations in public pockets, such as a few research labs, without undermining the effectiveness of the protection of information from certain targets. The modern trend rejects this rigid approach in the analogous arena of export control where President Clinton rejected

---

[186] Russo, *supra* note 38.

[187] *Id.* ("Kennedy noted in an Oct. 6 interview that even if the board had voted to stop the paper, the journal was too late in the printing process to do anything about it.").

[188] *Id.*

[189] William M. Fitzpatrick, Samuel A. Dilullo & Donald R. Burke, *Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law*, 12 ADVANCES IN COMPETITIVENESS RES. 57 (2004).

license decisions based upon foreign availability of encryption products.[190]

XVII. CAPTURING AND COUNTING CLASSIFIED INFORMATION

At present there are mechanisms in place to capture sensitive articles in the interests of national security, but there is a gap in the paradigm. Capture mechanisms were conceived and created in the 1940's and 1950's through the AEA and Patent Act, but have not changed since then. The next opportunity to amend capture mechanisms after the AEA and Patent Acts came with the advent of research on recombinant DNA, but decisive and responsible actions taken by the scientific community contained the issue. In lieu of a capture mechanism, a voluntary moratorium on research was instituted, which helped to instill public confidence in scientists' intentions and efforts. Thus, an agreement in the 1970's involving government oversight through the National Institutes of Health was well received.[191] Although a voluntary moratorium on contentious publications may help improve public confidence in the scientific community in the instant matter, it is doubtful the present situation would resolve in like manner to Asilomar. The current situation is different in that the problem stems in large part from the potential misuse by an adversary. In contrast, the risk with R-DNA was perceived as coming from the accidental misuse by well intentioned scientists. Thus, the instant dual use dilemma is less amenable to the Asilomar approach used in the 1970's.[192] Likewise, the need to capture some contentious articles is a reality for the time being in the post 9-11 era.

The decades old capture program at the Patent Office shows that inventions or techniques previously exposed to any number of professionals can successfully be classified by the government. This program has proven effective and has actually escaped charges of over-classification. Statistics from the Patent Office also indicate that the number of S.O.s have not increased dramatically since 9-11. The established record on the classification of science from the private

---

[190] *See* President Clinton, *Letter to Congressional Leaders on Encryption Export Policy*, (Nov. 15, 1996), http://www.cdt.org/crypto/admin/961115letter.html.

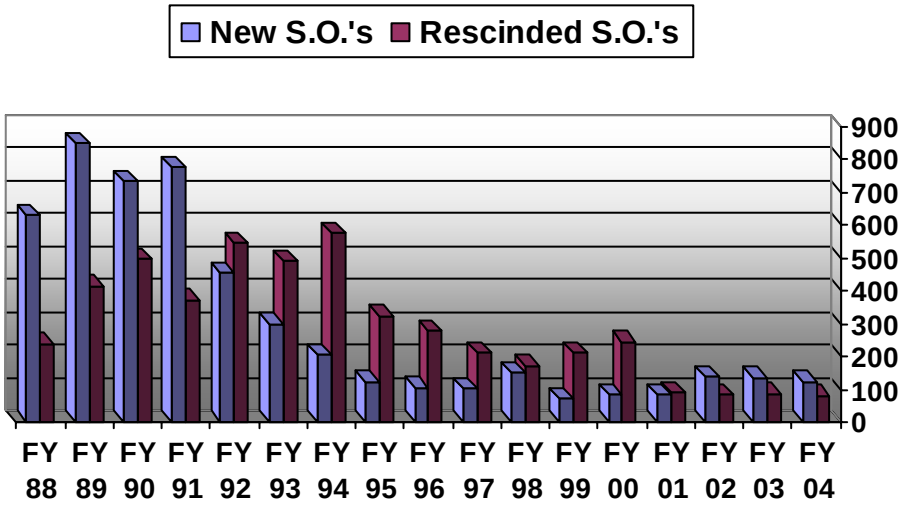
[191] Paul Berg, *Asilomar and Recombinant DNA*, http://nobelprize.org/chemistry/articles/berg (last visited Oct. 18, 2005).

[192] *See id.*

sector is most relevant to this debate and bodes well for those with concerns that the government may over-classify in the development of the next capture mechanism.

There were 4,885 S.O.s in effect at the end of fiscal year 2004.[193] But, only 61 S.O.s applied to private parties for the same period. Moreover, when looking at the trends in new and rescinded S.O.s, it appears that 9-11 did not have a major impact on the capture of scientific techniques through the Patent Office. (See Table 2). It is also interesting, if not surprising, to note the relatively low number of S.O.s issued during President George W. Bush's tenure.

Table 2: New S.O's Compared to Rescinded S.O's from 1988 to 2004



There is little opposition to the claim that the government is over-classifying information since 9-11.[194] Congressional testimony from William Leonard, director of the ISOO, and Carol Haave, Undersecretary of Defense for Counterintelligence and Security, "both

---

[193] Steven Aftergood, *Invention Secrecy*, http://fas.org/sgp/othergov/invention (last visited Oct. 18, 2005).

[194] Trent Lott & Ron Wyden, *Hiding the Truth in a Cloud of Black Ink*, N.Y. TIMES, Aug. 26, 2004, at A27; Shane, *supra* note 19.

estimated that an astounding percentage of secret material is improperly classified."[195] But the conservative trend in classification rates through S.O.'s is in stark contrast to the classification rates reported by the Information Security Oversight Office (ISOO) in other branches of government.

Clearly, the rate of classification should always be questioned in a democracy, but evaluations and comparisons need to be accurate and controlled for changes over time. For instance, the *New York Times* reported that "[a] record 15.6 million documents were classified [in 2004], nearly double the number in 2001."[196] This statistic can be seen in a much different light, however, when compared to classification statistics from 1984, another period when the nation was on a defense footing. The Stilwell Report stated, "DoD [Department of Defense] reported that some 16 million documents were classified in 1984."[197] The raw number of secrets will rise over time despite the most aggressive declassification programs.

The growth of technology and increased sharing of classified information will lead to higher raw numbers of secrets resulting in an inflation of secrets which has to be adjusted before making comparison to historical numbers. For instance, Frederick L. Jones cited an increase in e-mail usage for the rise in classification statistics since 9-11.[198] By comparison, the DoD only started to integrate computers into their offices in the mid-1980's.[199] Today, however, e-mails are widely used throughout government. For example, Los Alamos Laboratory alone generates over 300,000 e-mails per day.[200] In addition, more secrets will be generated as more agencies share classified information. The result of which will be "derivative classification decisions" resulting from incorporating, paraphrasing,

---

[195] Editorial, *supra* note 103.

[196] Shane, *supra* note 19.

[197] COMMISSION TO REVIEW DOD SECURITY POLICY AND PRACTICES, KEEPING THE NATION'S SECRETS (1985), *available at* http//www.fas.org/sgp/library/stilwell.html.

[198] Shane, *supra* note 19.

[199] COMMISSION TO REVIEW DOD SECURITY POLICY AND PRACTICES, *supra* note 197.

[200] Bowles, *supra* note 62 (Classified information is, however, transmitted via secure networks at Los Alamos rather than e-mails which are screened by senders or "Authorized Derivative Classifiers" for clearance.).

restating, or regenerating previously classified information.[201] Moreover, for the sake of balance, notice needs to be taken of other changes that have likely played a role in the classification statistics. For instance, the fact that in March of 2003, 180,000 federal employees merged from 22 agencies to form a new Department of Homeland Security (DHS), committed to sensitive security issues, should be taken into consideration.[202] Thus, inclusion of the new sources of classified information should be noted, if not controlled for, in classification statistics to help provide perspective.

After taking a step back from the raw statistics and critical judgments, it is ironic that an alleged crisis of over-classification is taking place at a point in time when more information than ever is available to the average citizen about everything from anthrax[203] to zip codes[204] at the click of a mouse. Moreover, there is greater access to government due to those who vigilantly watch the government[205] and to the government itself[206] as compared to a mere decade ago, despite the recent web scrubbing of SBU information.[207] Contributing to the complexity of this debate is the fact that scientific institutions want openness, but not when open access initiatives like PubChem cuts into the lucrative business of selling scientific information.[208] Regardless,

---

[201] Agency Security Classification Management Program Data, National Archives and Records Administration, Standard Form 311 (Rev. 11-04).

[202] Dep't of Homeland, *The U.S. Department of Homeland Security: Preserving Our Freedoms, Protecting Our Nation – Strategic Plan* (Feb. 23, 2004), http://www.dhs.gov/dhspublic/display?theme=10&content=3240.

[203] *See* Center for Disease Control and Prevention, *Disease Listing: Anthrax*, http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_g.htm (last visited Oct. 18, 2005).

[204] *See* U.S. Postal Service, *ZIP Code Lookup*, http://zip4.usps.com/zip4/welcome.jsp (last visited Oct. 18, 2005).

[205] *See* Federation of American Scientists, http://www.fas.org (last visited Oct. 18, 2005); OMB Watch, http://www.ombwatch.org (last visited Oct. 18, 2005).

[206] FirstGov.Gov: The U.S. Government's Official Web Portal, http://www.firstgov.gov (last visited Oct. 18, 2005); Federal Citizen Information Center, FirstGov.Gov Fact Sheet, http://www.pueblo.gsa.gov/firstgov-fs.htm (last visited Oct. 18, 2005) ("FirstGov.Gov provides access to over 180 million pages of web based federal, state and local government resources available 24/7."); PubMed Central, http://www.pubmedcentral.nih.gov (last visited Oct. 18, 2005).

[207] The Card Memo, *supra* note 84.

[208] Letter from William F. Carroll, Jr., American Chemical Society President (June 20, 2005), *available at* http://acswebcontent.acs.org/PDF/pubchem_open_letter.pdf (opining loss of

the quantity and quality of information is proliferating, as evidenced by live and archived web casts of the Federal Advisory Committee known as the National Science Advisory Board for Biosecurity.[209] Television remains an important source of information through 24 hour news channels and new programming such as C-SPAN which provides "gavel to gavel" coverage of government events.[210] Thus, more careful attention needs to be paid to the functions of government that need transparency for the survival of democracy.[211]

XVIII. BRIDGING THE DIVIDE

In the absence of cooperation between the private sector and the government, the government may need to utilize both traditional and novel approaches to reach its national security obligations in the information society. For instance, the government relies upon deterrence tactics to encourage compliance with government secrecy when the country is on a war footing, as evidenced by the rare prosecution in the Morison and Franklin spy cases during the Cold War and post 9-11 era respectively. The government, however, also displayed its capacity for creativity in secrecy matters during Operation Enduring Freedom in Afghanistan. In an effort to restrict access to views of military actions in Afghanistan, the U.S. government actually captured the desired information by purchasing all of the available satellite images from a civilian source, Ikonos,

---

revenue to government's open access initiative PubChem); *see also* IRS Form 990, 2003 Return of Organization Exempt From Income Tax, American Chemical Society, 1155 Sixteenth Street, N.W., Washington, D.C. 20036-4892 (Gross Receipts Line L: 2,890,079,272).

[209] Meeting of National Science Advisory Board for Biosecurity (July 1, 2005), http://www.webconferences.com/nihnsabb/july_1_2005.html (last visited Oct. 18, 2005).

[210] C-SPAN Mission, http://www.c-span.org/about/company/index.asp?code=Mission (last visited Oct. 18, 2005) ("[L]ive gavel to gavel proceedings of the U.S. House of Representatives and the U.S. Senate, and other forums where public policy is discussed, debated and decided…").

[211] Dennis F. Thompson, *Democratic Secrecy*, 114 POL. SCI. Q., 181, 192 (1999) ("Democratic accountability does not require unconditional publicity in the conduct of democratic government. Secrecy of various kinds is sometimes justified and even desirable in a democracy. But it is justified only under carefully specified conditions, which ensure that the secrecy itself is subject to democratic accountability."); Branzburg v. Hayes, 408 U.S. 665 (1972).

covering the coordinates of concern.[212] The government took this approach over "shutter control," the black out of the media, because they anticipated lawsuits from news organizations claiming unlawful prior restraint.[213] The only other source of satellite images of the area came from a French firm called Spot Image, but the U.S. convinced the French Defense Ministry to ban Spot Image from selling their images of the areas that the U.S. was trying to control.[214] Thus, there are many approaches to capturing sensitive information that must be considered in formulating secrecy policy with dual use science.

New and creative paradigms need to be created to reward compliance for joint vetting with the government and prepublication review of contentious research to avoid adversarial standoffs and rushed vetting as exemplified, respectively, by the Toxic Milk and Spanish flu controversies. Moreover, the Executive should use progressive management practices with government personnel responsible for classifying information to reward accurate classification decisions.

Clearly, the government has many options from police powers to the art of persuasion at its disposal to meet the challenge presented by domestic terrorism in the age of information. In the case of dual use science, the government has made a historic and unprecedented effort to listen to any and all advice from a highly respected advisory board in the NSABB. Thus, the window is open for the infusion of innovative ideas to create a new paradigm to manage the dual use issue. But time is of the essence, and immediate action needs to be taken to close the gaping loop holes through which the integrity of national security and public health may flow.

XIX. THE EXECUTIVE OPTION

The NSABB convened for the first time in June 2005 to address the dual use issue; however, years have passed since the government first asked the scientific community for guidance on this issue. Thus, a new paradigm on open science remains an ideal without form or

---

[212] Duncan Campbell, *US Buys Up All Satellite War Images*, THE GUARDIAN, Oct. 17, 2001, at 1.

[213] *Id.*

[214] Theresa Hitchens, Vice President, Center for Defense Information, Presentation to a Conference "U.S. Space Operations in the International Context," (Feb. 24, 2004), *available at* http://www.cdi.org/friendlyversion/printversion.cfm?documentID=2111.

substance. Meanwhile, science marches on, continuing to produce contentious research without the safeguards of reliable risk measures to judge the appropriate level of protection these articles should have against potential adversaries and terrorists. Moreover, after all this time, the government does not even have a mechanism in place to trigger notice of impending contentious publications by U.S. scientists. This flaw was partly responsible for the recent vetting debacle with the Spanish flu articles.

It is indeed striking that the U.S. government was reduced to feckless vetting of research on the deadliest virus on record[215] conducted by U.S. scientists in its own CDC biosafety level-3 lab. The fact that the Assistant Secretary of HHS was only informed of the impending publication of the Spanish flu articles after the publisher's point of no return[216] begs many questions. While the communication problems within the government can be addressed in short order, the question remains over how the government will be assured of adequate prepublication notice of contentious research from government and non-government sources before formal systems are implemented.[217]

The Bush administration has a duty to act on this issue as soon as possible in the interests of national security. At a minimum, it is necessary for the government to have pre-publication notice of articles on high risk materials that are already under federal controls.[218] Relatively quick measures could be coordinated on an international level through an intersession agreement from the Australia Group[219]

---

[215] Roger Highfield, *Most Deadly Virus is Resurrected*, THE DAILY TELEGRAPH (London), Oct. 6, 2005, at 4 ("The deadliest virus on record has been resurrected from a strain of influenza that was preserved in the frozen body of a victim of the 1918 pandemic and triggered a row about whether the benefits of its recreation outweigh the risks.").

[216] Russo, *supra* note 38 ("Kennedy noted in an Oct. 6 interview that even if the board had voted to stop the paper, the journal was too late in the printing process to do anything about it.").

[217] Russo, *supra* note 38 ("'[Osterholm] acknowledged that the [NSABB] does not yet have a process in place to monitor pre-publication research by non-government researchers who do not feel obligated to have HHS vet their findings.' Donald Kennedy editor of *Science* said, 'I think there's some questions to be raised about how this should be organized.'").

[218] *See* Use and Transfer of Select Agents and Toxins, 42 C.F.R. § 73 (Mar. 18, 2005); Use and Transfer of Select Agents and Toxins, 9 C.F.R. § 121 (Mar. 18, 2005).

[219] Definitions of Terms as Used in the Export Administration Regulations (EAR), 15 C.F.R. §722.1 (2005) ("The countries participating in the Australia Group have agreed to adopt harmonized controls on certain dual-use chemicals (i.e. precursor chemicals), biological agents, related manufacturing facilities and equipment, and related technology in order to

on the pre-publication review and sharing of contentious life science research among its thirty-nine members. Consistent with such an agreement, the EAR may be used to provide a pre-publication trigger mechanism by proscribing unlicensed release of contentious science before safeguarded sharing at an international level, but this route would take a significant amount of time to implement.[220] In the interim, however, the Executive could immediately create a trigger mechanism assuring prepublication notice of articles on select agents, toxins, and microorganisms associated with pandemics and bioweapons by amending the EAR. The Executive could amend the EAR in the interests of national security under authority of the International Emergency Economic Powers Act (IEEPA),[221] just as President Clinton did when he amended export policy on cryptology technology.[222]

Thus, the President could fashion a stopgap measure by merely removing the basic research exemption[223] from the limited area of select agents, pandemic-related materials, toxins and microorganisms subject to export control.[224] This action would require a license for the publication of such information and provide prepublication notice to the national security community of potentially contentious research. Thus, no science is subject to arbitrary classification by the government or censorship by scientific publishers. Rather, the removal of the loophole exemption related to the aforementioned materials will prevent further vetting debacles and nullify the publisher's veto until the government codifies new laws to address this dilemma. Years have passed since the dual use issue in the life sciences was identified and it may take many more years to create a

---

ensure that exports of these items do not contribute to proliferation of chemical or biological weapons.").

[220] *See* Dep't of Commerce, Bureau of Industry and Security, Control Policy: End User, 15 C.F.R. pt. 744 (2005), (The rule is an amendment of EAR through administrative action in response to a new agreement through the Australia Group.).

[221] International Emergency Economic Powers Act, 50 U.S.C. § 1701 et. seq. (2003).

[222] Clinton, *Letter to Congressional Leaders*, *supra* note 190.

[223] *See* Scope of the Export Administration Regulations: Information Resulting from Fundamental Research, 15 C.F.R. § 734.8(b)(6) (2005) (concerning nullification of fundamental research exemption for acceptance of national security controls or on government sponsored research projects).

[224] *See* HHS and USDA Select Agents and Toxins Commerce Control List, *available at* http://www.cdc.gov/od/sap/docs/salist.pdf (last visited Oct. 16, 2005).

new paradigm to the satisfaction of all stakeholders. It is, however, incumbent upon the Executive to act immediately to obtain prepublication notice of critical national security information in the interim. Then and only then can the national security implications of contentious life science articles be evaluated properly on a case by case basis.

This proposal will, no doubt, be met with resistance by members of the scientific community who have lobbied against governmental involvement in the publication process. Unfortunately, however, it may take unilateral Executive action such as this to preempt specious censorship agreements, the publisher's veto, and moot vetting scenarios until a new paradigm that assures a meaningful partnership between the scientific and national security communities is adopted.