Federal Secrecy and the States: The Impact of Information Closures on Local Government Operations

RYAN LOZAR*

ABSTRACT

Although federal secrecy keeps some highly sensitive information out of the hands of terrorists, it can also negatively and unnecessarily impact state and local government operations. One example of this occurs when federal secrecy's preemption of local open government laws is permitted to swell beyond what it is supposed to be, sometimes with state-level complicity, thereby limiting citizens' legitimate public information rights. This article presents various case studies where the federal preemption line has been blurred, causing unnecessarily expansive local information closures, and makes suggestions on how to avoid similar problems in the future. Federal secrecy also degrades local government operations by hiding federal information even from local government officials who need it to intelligently allocate resources to maximize citizen safety. This article suggests that the informational disability federal secrecy imposes on local homeland security efforts sometimes undermines the very goal of citizen safety that theoretically justified the federal secrecy in the first instance.

I. INTRODUCTION

Government secrecy harms democracy by diluting or disabling citizen participation in politics and government. It "breeds mistrust, dampens the fervor of its citizens, and mocks their loyalty," thereby injuring the government's "integrity and operation."[1] However embattled these principles may be in fact, the necessity of open government to an engaged citizenry and electorate is, by now, common knowledge. And it is on the basis of this widely accepted wisdom that the federal government's marked penchant for secrecy since September 11, 2001 (hereinafter "9/11") has been increasingly noted and scrutinized.

Although federal secrecy certainly keeps some highly sensitive information out of the hands of terrorists, it can also materially alter

---

* A sincere thank you to Michael Boucai and Viviana Giacaman for their invaluable help.

[1] S. Rep. No. 813 (1965), *as reprinted in* S. Comm. on the Judiciary, Freedom of Information Act Source Book: Legislative Materials, Cases, Articles, S. Doc. No. 93-82, 93d Cong., 2d Sess., at 45 (Comm. Print 1974).

how state and local governments relate to and serve their citizens – and, indeed, the ability of those levels of governments to advance priorities and prerogatives they share with the federal government. Federal secrecy requirements erode the public's right to access local government records when, in order to effectuate a nationally coordinated plan, they preempt the release of certain records via state open government laws. Federal secrecy requirements can also diminish state and local governments' ability to adequately address their citizens' public safety needs; when local officials are denied access to certain federal information, they may not know how to direct resources to maximize citizen safety. This article addresses these effects by analyzing their negative–sometimes arguably unnecessary–consequences in each instance, making brief recommendations as to how government officials, both federal and state, might mitigate them in the future.

This article starts from the assumption–or rather, the virtually unquestioned reality–that the United States' federalist system permits the states to pass open government laws concerning public access to their own records and meetings insofar as they do not conflict with a coordinated national plan to suppress information. All fifty states and the District of Columbia have exercised this right.[2] The states likewise have a police power allowing them to legislate to protect their citizens' health, safety and welfare. Again, in a federalist framework, that local autonomy must bend to a coordinated national action addressing the same issue.

Part one presents a non-exhaustive list of ways that the Bush Administration has expanded federal secrecy since 9/11: more annual document classification decisions; increased permissiveness at the Justice Department with reference to federal agencies' discretionary invocation of Freedom of Information Act exemptions; and the rise of standardless pseudoclassification systems. To the extent that federal secrecy impacts state and local level of government operations, Part One shows that since 9/11 there has been ample federal secrecy to trigger those effects.

My intention in documenting the striking increase of federal secrecy since 9/11 is not to criticize its use and concomitant effects in all instances–especially since some of it is surely necessary, and, as the reader will see in the subsequent sections (particularly Part Two), state governments are sometimes themselves to blame for aggravating or

---

[2] Roger A. Nowadzky, *A Comparative Analysis of Public Records Statutes*, 28 Urb. Law. 65 (1996).

inviting federal secrecy's effects. In the end, this article simply seeks to draw attention to the relationship between federal secrecy and state government operations so that federal- or state-level officials might consider this relationship more fully in any information closure decision.

Part two shows how certain federal secrecy requirements can confuse or entice local governments into excessively closing records in contravention of state open government law when federalist preemption does not actually require it. The article illustrates such federal secrecy trickledown by reference to: (1) states' excessive denial of access to government records due to uncertainty over the scope of the federal Critical Infrastructure Information Act of 2002 (the "CII Act"); (2) the submission of state records already in the government's possession for federal PCII (Protected Critical Infrastructure Information) protection pursuant to the CII Act, a practice at odds with the statute's espoused purpose; and (3) local governments' voluntary participation in federal partnerships marked by secrecy requirements that trump state openness principles.

Part Three explores how federal secrecy leaves state and local governments without the information they need to effectively craft legislation offering protections for citizen safety. It presents case studies in federal secrecy's frustration of local government's access to information related to public safety, including: (1) poorly-explained national color-coded terror alerts that kept local governments from knowing where their resources should be directed to maximize safety and (2) top-secret federal rail terrorism security plans that left Washington, D.C. officials unable to know whether the national Congress had made adequate provision to protect city residents.

II. BURGEONING FEDERAL SECRECY

Classification is an important mechanism by which the federal government protects security-sensitive records from public view. Each federal agency has a limited number of authorized personnel who use a largely uniform set of rules to make classification decisions, some of which are discretionary. Annual classification statistics released by the Information Security Oversight Office (ISOO), a branch of the National Archives and Records Administration charged with overseeing the classification process, report that the federal government's exercise of its classification power substantially

increased since 9/11.[3] According to ISOO's March 2005 report, the federal government made 15.7 million classification decisions in 2004, nearly double the 8.7 million made in 2001.[4] At the same time, the 28 million pages of documents declassified in 2004 paled in comparison to 2001's 100 million pages.[5] The federal government is not only clamping down on public information—it is also refusing to loosen its grip.

The federal Freedom of Information Act (FOIA), enacted by Congress in 1966, establishes the right of any person to access federal agency records with certain exceptions. Classified documents are just one class of record not subject to FOIA's mandate of public disclosure. Documents that fall under one of FOIA's nine outlined exemptions are also protected.[6] Although the Justice Department must defend federal agencies' *statutorily-mandated* FOIA withholdings in court, it is up to any given Attorney General whether the Department will defend a federal agency's invocation of the Act's *discretionary* exemptions. The FOIA policy authored and followed by the Bush Administration's Attorneys General contributes mightily to the already-burgeoning culture of federal secrecy reflected in the post-9/11 classification explosion; in October 2001, then-Attorney General John Ashcroft issued a FOIA guidance memorandum assuring federal agencies that the Justice Department would defend any technically-justified decision to withhold government records–although in some instances they could have just as easily exercised their statutorily granted discretion to release them.[7] The Ashcroft standard, continued by his successor Alberto Gonzales, is a far cry from the presumption of openness

---

[3] Information Security Oversight Office (ISOO), 2004 Report to the President (March 2005), *available at* http://www.archives.gov/isoo/reports/2004-annual-report.pdf. ISOO is a division of the National Archives and Records Administration and is largely guided by the National Security Council. Its mission is to oversee the government's security classification programs by, among other things, issuing annual status reports.

[4] *Id.* at 15.

[5] *Id.* at 17; *see also* Information Security Oversight Office (ISOO), 2001 Report to the President 4 (Sept. 2002), *available at* http://www.archives.gov/isoo/reports/2001-annual-report.pdf.

[6] *See, e.g.*, 5 U.S.C. § 552(b)(1)-(9) (2001) (listing nine exemptions under the FOIA).

[7] "[Y]ou can be assured that the Department of Justice will defend your decisions [to withhold government records] unless they lack a sound legal basis …" Memorandum from John Ashcroft, Att'y Gen., to Heads of All Federal Departments and Agencies, on the Freedom of Information Act (Oct. 12, 2001), *available at* http://www.usdoj.gov/04foia/011012.htm.

promulgated in Janet Reno's Justice Department.[8] The daughter of two reporters, Reno explicitly urged federal agencies to be conservative in their withholding of records, particularly when an exemption claim exclusively implicated government interests, as in the deliberative process privilege or attorney-work product privilege.[9]

The post-9/11 federal government has also witnessed a proliferation of vague secrecy jargon such as "Sensitive but Unclassified," "Sensitive Security Information," or "Sensitive Homeland Security Information."[10] Critics of these "pseudo-classifications" explain that they are used to signal to records custodians that they should make an effort to withhold a document under whatever FOIA exemption they can find.[11] In conjunction with a March 2005 hearing on overclassification and pseudo-classification of documents, Rep. Henry Waxman (D-Calif.) complained that many of these designations have "questionable legal pedigrees."[12] Undefined by statute, or even by executive order, these designations frequently lack "even minimal controls or monitoring," and the government can mark documents liberally with an ill-defined "sensitive" stamp.[13]

In a federalist system of government like ours, these classifications, FOIA exemptions, and pseudoclassifications create ripple effects felt powerfully at state and local levels of government.

---

[8] Memorandum from Janet Reno, Att'y Gen., to Heads of All Federal Departments and Agencies, on the Freedom of Information Act (Oct. 4, 1993), *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm.

[9] *Id.*

[10] Letter from Rep. Henry A. Waxman (D-Calif.) to The Hon. Christopher Shays (R-Conn.), Chairman, Subcomm. on National Security, Emerging Threats, and International Relations, Comm. on Government Reform 1 (Mar. 1, 2005), (on file with H.R., Wash., D.C., 20515), [hereinafter Waxman Letter], *available at* http://www.democrats.reform.house.gov/Documents/20050301112122-90349.pdf.

[11] *Emerging Threats: Overclassification and Pseudo-Classification: Hearing Before the H. Subcomm. on National Security, Emerging Threats and International Relations*, 109th Cong. (2005) (statement of Thomas S. Blanton, Director, National Security Archive, George Washington Univ.), *available at* http://reform.house.gov/uploadedfiles/2%20Blanton%20Shays%20testimony%202%20March%202005.pdf (last visited July 13, 2005).

[12] Waxman Letter, *supra* note 11, at 3.

[13] *Id.*

III. SECRECY BEGETS SECRECY

One of the dimensions in which post-9/11 federal secrecy impacts the states is in the area of open government law. The constitutional principle of federal preemption provides the doctrinal basis upon which federal secrecy policy is empowered to annul the operation of the Freedom of Information Act's fifty state counterparts to ensure that information suppression is executed uniformly throughout the country. States individually expand the preemptive power of federal secrecy, however, when they fail to carefully consider and therefore understand the intended scope of federal secrecy provisions, thereby increasing the number of records that "have to be" withheld. Even more troubling than such negligence is evidence that states knowingly compromise local openness through practices like the intentional submission of records for federal secrecy designations under homeland security programs. States similarly disregard their commitment to open government through voluntarily accession to federal contracts requiring confidentiality for records that would otherwise be open under state law.

A. UNCERTAINTY AND SILENCE UNDER THE CRITICAL INFRASTRUCTURE INFORMATION ACT

Since its enactment shortly after 9/11, the Critical Infrastructure Information Act of 2002 (the "CII Act") has fueled numerous expansions of state-level secrecy. The CII Act – part of the Homeland Security Act that created the new Department of Homeland Security ("DHS") – creates confidentiality under existing open records laws for "critical infrastructure information."[14] Critical infrastructure information is data pertaining to the security of telecommunications systems, banks, dams, water and sewer plans, nuclear power plants, ports, public utilities, and other entities necessary to the nation's well-being which, if incapacitated or destroyed, could jeopardize national security or public health.[15] The aim of the CII Act exemption–which is drafted to apply to both federal and state open government laws–is to encourage *private industry* to share its commercial infrastructure

[14] The Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-134 (2005).

[15] *Id*.; 6 U.S.C. § 133(a)(1)(E)(i) (2005) (providing that critical infrastructure information shall not, if shared by DHS with a State or local government, "be made available pursuant to any State or local law requiring disclosure of information or records."); 6 U.S.C. §131(3) (2005) (defining critical infrastructure information).

information with the federal government to facilitate the development of terrorism security plans pertaining to the nation's infrastructure.[16] Absent the promise of confidentiality, the theory goes, private industry would not voluntarily share what they view to be publicity-sensitive information related to its business.

Data is eligible for designation as protected critical infrastructure information ("PCII") when it is voluntarily submitted to the federal Homeland Security Department with an accompanying affidavit testifying to qualifying elements.[17] To qualify, the submitter must aver that the information is "not customarily in the public domain."[18] Once the Homeland Security Department labels data PCII, the CII Act protects it from disclosure under state public records law if and when the federal government later shares it with state and local officials.[19]

---

[16] Procedures for Handling Critical Infrastructure Information; Interim Rule, 69 Fed. Reg. 8074 (Feb. 20, 2004) (to be codified at 6 C.F.R. pt. 29) [hereinafter Interim Rule] ("[P]rivate industry has indicated that its reluctance to share critical infrastructure information with the Federal government is based upon a concern that the information will not be adequately protected from disclosure to the public … The Department recognizes the importance of receiving information from those with direct knowledge of the security of that critical infrastructure in order to help reduce our nation's vulnerability to acts of terrorism. The Department believes the voluntary sharing of critical infrastructure information (CII) has been slowed due to concerns that information might be released to the public."); Under a heading called "Why was the program created?," the Homeland Security Department's Web site says "Recognizing that the private sector may be reluctant to share information with the Federal Government if it could be publicly disclosed, Congress passed the CII Act in 2002 with its provisions for protection from public disclosure." *Available at* http://www.dhs.gov/dhspublic/display?theme=92&content=3763 (last visited July 28, 2005); The statute's actual language, however, does not explicitly condition CII protection on the private sector, as information must be submitted requesting CII protection.

[17] 6 U.S.C. § 133 (2005); Cara Muroff, Note, *Terrorists and Tennis Courts: How Legal Interpretations of the Freedom of Information Act and New Laws Enacted to Prevent Terrorist Attacks Will Shape the Public's Ability to Access Critical Infrastructure Information*, 16 U. Fla. J.L. & Pub. Pol'y 149, 158 (2005) ("The Homeland Security Act aims to assess weaknesses in homeland security by collecting critical infrastructure information from private entities … To achieve this goal, certain provisions of the Homeland Security Act protect critical infrastructure information that is voluntarily submitted by private entities to the Department of Homeland Security from disclosure under the FOIA or any state and local open records laws.").

[18] 6 U.S.C. § 133(a)(2)(A) (2005) (providing that an accompanying affidavit is a "written marking on the information or records substantially similar to the following: 'This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.'"); 6 U.S.C. §131(3) (2005) ("The term 'critical infrastructure information' means information not customarily in the public domain. . .").

[19] 6 U.S.C. § 133(a)(1)(E) (2005).

Under the law, a state records custodian who illegally releases federally designated PCII information faces up to one year in prison and/or up to $1,000 in personal fines.[20]

The federal penalty for unauthorized *disclosure* is extreme compared to the small or nonexistent fines ($100 in Georgia or Mississippi, nothing in Massachusetts or New York) imposed by most state open records laws for the improper *withholding* of public records law.[21] The effect of this imbalance is hardly surprising–faced with the choice between the sizable federal punishment and a paltry or nonexistent state fine; state records custodians, better safe than sorry, will withhold government information whose PCII status is vague.

But state officials are not wholly powerless against federal impositions of secrecy. They can and should be vigilant in protecting against the PCII vagueness that allows so many state records to be sucked into the federal secrecy vacuum. First, state public records' physical proximity to PCII-designated data can cause PCII-vagueness. PCII records should not be filed in the same folders or cabinets as other state public records, for instance. They should always be clearly segregated. Second, state public records' thematic similarity to PCII-protected files can also cause PCII-vagueness and excessive secrecy. One can speculate that when a PCII-labeled folder comes into a state records office pertaining to a local water utility, for instance, all state water utility records' openness might thereafter be questioned. The CII Act exemption, however, only protects records obtained from *federal* PCII files, not subject-similar records that the state obtained on its own.[22] Records custodians should be advised of this technical distinction by state and local government officials, and they should be urged to draw it themselves when processing information requests from the public. Such precautionary measures will not rescue all

---

[20] 6 U.S.C. § 133(f) (2005); 6 C.F.R. § 29.9 (2005).

[21] Ga. Code Ann. § 50-18-74 (West 2005) ($100); Miss. Code Ann. § 25-61-15 (West 2005) ($100); Mass. Gen. Laws Ann. Ch. 66. § 10 (LexisNexis 2005) (no fine); Mont. Code Ann. § 2-6-107 (2005) (no fine); Nev. Rev. Stat. § 239.011 (2005) (no fine); Del. Code Ann. tit. 29, § 10,005(d) (2005) (no fine); Cal. Gov't Code § 6258 (West 2005) (no fine); D.C. Code Ann. § 2-537(a-1), (c) (LexisNexis 2005) (no fine); N.Y. Pub. Off. Law § 89(4)(b), (c) (McKinney 2005) (no fine); 5 Ill. Comp. Stat. 140/11(a), (i) (2005) (no fine).

[22] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 2154 (2002) (codified at 6 U.S.C. § 133(c) (2005)) ("Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority … to obtain critical infrastructure information in a manner not covered [by the 'voluntarily submitted' portions of the statute] … and to use such information in any manner permitted by law.").

public information from the grasp of federal secrecy policies, but they will go far in counteracting the confusion that allows for some of the most patent abuses.

B. INVITING SECRECY UNDER THE CRITICAL INFRASTRUCTURE INFORMATION ACT

From the language of the CII Act, federal PCII secrecy designations are meant to protect from public disclosure state records that meet a very specific description: Infrastructure information that has been submitted to the Homeland Security Department *by private industry* and later shared with state officials.[23] This conventional wisdom underwent quite a mutation, however, when a New Jersey township recently dodged an open records request by submitting the data to the federal government itself for a PCII designation.[24] The controversy began when New Jersey resident R. Bradley Tombs requested electronic Geographic Information System (GIS) records–aerial government maps bearing geographically referenced data–from the Brick Township Municipal Utilities Authority ("township") in 2003. In response to the request, the township simply sent its GIS data to the federal Homeland Security Department asking for its

[23] "By offering an opportunity for protection from disclosure under the Freedom of Information Act for information that qualifies under [Homeland Security Act] section 214, [DHS] will assure private sector entities that their information will be safeguarded from abuse by competitors or the open market." Interim Rule, *supra* note 17, 8074; *see* Cara Muroff, *supra* note 18, at 168 (analyzing the U.S. Bureau of Reclamation's suppression of dam inundation maps under FOIA Exemption 7(F) and stating "[h]ad the Bureau been a private entity, the Bureau might have avoided the FOIA request and litigation completely by stamping the maps 'critical infrastructure information' and handing it over to the Department of Homeland Security under the new federal Protected Critical Infrastructure Information Program.").

[24] The incident insinuates the expansion of the CII program to permit what are called "indirect submissions" to the DHS for CII designation. To make an indirect submission, a company first submits its records to an agency other than DHS, and that agency does the CII submission. Interim Rule, *supra* note 17, at 8075 ("The Department received 20 comments expressing concern regarding the proposed provision that would enable other Federal government entities to act as conduits for submissions of CII to the Department.… Recognizing that, at this time, implementation of such a provision would present not only operational but, more importantly, also significant program oversight challenges, the Department has removed references throughout the rule to indirect submissions.").

designation as PCII.[25] In a June 2005 letter, the DHS approved the township's petition.[26]

Much to Tombs' frustration, requesters have no appeals process to challenge a federal PCII designation,[27] an incredible fact given Tombs' belief that the township fudged the truth in officially asserting that its GIS information "was not customarily in the public domain."[28] Tombs alleges that the township used to sell segments of the GIS database online.[29]

What is alarming about the township's request–and the federal government's approval of it–is that it appears to subvert the espoused purpose of the CII Act's federal and state open records exemptions. Although the CII Act's statutory language refers to submitters without explicitly clarifying who qualifies, the Homeland Security Department's implementing regulations and information Web page are riddled with references to the law's purpose as encouraging *private industry* to share proprietary infrastructure information with the Homeland Security Department that it might otherwise withhold absent the promise of confidentiality.[30] The township, on the other

---

[25] Case materials from the Federation of American Scientists' catalogue of *Tombs v. Brick Twp. Mun. Util. Auth.*, 2005 N.J. Agen Lexis 13 (N.J. Agen 2005), *available at* http://www.fas.org/sgp/othergov/dhs-brick.pdf (last visited July 27, 2005).

[26] *Id.*

[27] The CII Act provides criminal penalties for submissions founded on false representations. *See* 6 C.F.R. § 29.6(e) (2004). "Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. [§]1001 and are punishable by fine and imprisonment." Interim Rule, *supra* note 17, 8085. But CII status reversals are left to the discretion of the Homeland Security Department. Interim Rule, *supra* note 17, at 8080. ("[C]hanges may take place if the Program Manager subsequently determines that the information was customarily in the public domain, was required by Federal law or regulation to be submitted to DHS, or is now publicly available through legal means.").

[28] Telephone interview with R. Bradley Tombs, who requested the GIS data because he suspected corruption at the public utility and wanted more information about its operations, in Brick Township, New Jersey (July 14, 2005).

[29] *Id.*

[30] In his comments on the Homeland Security Department's implementing rules for the CII Act, the Department's Assistant Secretary for Infrastructure Protection, Robert Liscouski said in February 2004 that "[o]ur aim is to provide a platform for the private sector that will enable them to give us the information we need to advise and assist them to make the country safer. We are not trying to provide a mechanism that people can use to hide damaging information from regulators or the public." Robert Block, *U.S. Law Shields Company Data Tied to Security*, Wall St. J., Feb. 18, 2004 at B1.

hand, obviously used the statute to create a state freedom of information exemption for GIS data that was already in the government's possession.[31]

C. SACRIFICING OPENNESS PRINCIPLES FOR $77 A DAY

The willingness of two New Jersey prisons to participate in secret prison operations for the federal government beginning in late 2001 is another example of state complicity in federal secrecy's weakening of local open records law. Despite the fact that New Jersey law explicitly designates prisoner names as public information,[32] Passaic and Hudson County prisons contracted to house 400 to 700 federal immigrant detainees on their premises in the wake of 9/11, agreeing to hide their names from the public.[33] In exchange, the Immigration and Naturalization Service (INS) paid the prisons $77 per detainee per day.[34] When the American Civil Liberties Union of New Jersey requested access to the detainees' names in late 2001, the county prisons, in accordance with the conditions of their partnership, refused.

The ACLU sued for the information and in March 2002, Hudson County Superior Court Judge Arthur D'Italia ruled in favor of the information's disclosure.[35] He reasoned that the INS detainees were inmates of the state jails and state law clearly said that their names were public. Within thirty days, the INS promulgated a federal regulation making the detainees' names confidential.[36] By the time the

---

[31] Telephone interview with Steven Aftergood, Executive Director, Federation of American Scientists, in Washington, D.C. (July 14, 2005).

[32] "The keeper of every jail or other penal or reformatory institution supported by public moneys of any county or municipality, shall keep a book … in which he shall set forth the date of entry, date of discharge, the description, age, birthplace and such other information as he may be able to obtain as to the inmates committed to his care, which book shall be exposed in a conspicuous place in the institution and shall be open to public inspection." N.J. Stat. Ann. §30:8-16 (West 2005) (As of July 7, 2002, the Right-to-Know Law has been amended); N.J. Admin. Code §10A:31-6.5(a) (2005) ("other information" that must be set forth includes inmate names).

[33] Elizabeth Llorente, *ACLU Sues Over Detainees*, The Record, Jan. 23, 2002 at A01.

[34] *Id.*

[35] ACLU v. County of Hudson, 799 A.2d 629, 638 (N.J. Super. Ct. App. Div. 2002).

[36] 8 C.F.R. § 236.6 (2002) (No state prison housing a detainee on behalf of the INS "by virtue of any official or contractual relationship … shall disclose or otherwise permit to be made public the name of, or other information relating to, such detainee.").

appeal reached the New Jersey Appellate Division for oral argument, two U.S. Justice Department lawyers had replaced the Hudson County government attorney. They argued that federal law preempted the New Jersey Right-to-Know statute.[37] Writing for a unanimous panel, Judge Howard S. Kestin agreed; the fact that the INS's brand-new regulation was specifically drafted to abrogate state open records simply "demonstrate[d] that the suit brought a problem to light that should be addressed."[38]

The case certainly did bring a problem to light, which was New Jersey's voluntary choice to compromise its commitment to open government for $77 per inmate per day. Passaic and Hudson County prisons' agreement with the INS was obviously less calculating than the New Jersey township utility's purposeful pursuit of a federal secrecy designation for its GIS data, but the result is no less detrimental to government openness. States' active pursuit of or willing subscription to federal secrecy are equally effective strikes against their own open government policies.

D. RECOMMENDATIONS

The CII Act and the INS confidentiality regulation for detainee names are two contexts where federal secrecy has preempted and complicated state open records law since 9/11, with varying degrees of state complicity. State and local governments can mitigate federal secrecy's abrogation of their own open records laws by refocusing on compliance, especially when faced with new challenges and temptations such as these.

It's important, for instance, that state officials create a freedom of information culture where state records custodians and requesters understand the scope of PCII designations so as to avoid excessive state-level withholdings. The boundaries of the CII Act designation process also need clarification. On the federal level, the Homeland Security Department should exercise the CII Act's criminal enforcement provisions to elucidate what makes a good-faith

---

[37] Interestingly, Robert D. McCallum, Jr., Assistant Attorney General of the United States–not a state lawyer–argued the case before the Appellate Division. ACLU v. County of Hudson, 799 A.2d 629 (N.J. Super. Ct. App. Div. 2002).

[38] *See id.* at 655 ("[I]t is of no consequence … whether the disclosure sought by plaintiffs is required as a matter of State law. To the extent the State laws involved may be viewed as requiring public disclosure of information regarding INS detainees, they would be in conflict with 8 *C.F.R.* § 236.6. Therefore, the federal regulation must be seen as pre-empting State law bearing upon its subject matter.").

submission of critical infrastructure information, particularly whether state governments are authorized to make such submissions at all. Regardless of DHS's activism in enforcing the criminal provisions, a cause of action should be developed for individual requesters so that they can step in as private attorneys general and encourage CII Act compliance by supplementing the possibility of criminal enforcement with the threat of civil liability.[39]

As further evidence of their continuing commitment to open government, states should negotiate secrecy requirements out of their voluntary partnerships with the federal government when possible. Portland, Oregon, took just such a principled stand in April 2005 when it terminated its cooperation with the Federal Bureau of Investigation (FBI) on one of its highly classified Joint Terrorism Task Forces ("task force").[40] The FBI conducts community-specific anti-terrorism investigations through its task forces by deputizing local police officers and granting them security clearances.[41] But the FBI does not also grant security clearances to the local officers' superiors.[42] When rumors started swirling that the FBI's Portland task force was spying on religious and political organizations in violation of Oregon's law requiring "reasonable suspicion of criminal activity" for such surveillance,[43] city officials asked the FBI to security-clear three of them – the mayor, the police chief, and the city attorney–so that they could evaluate their local officers' compliance with state law.[44] The

---

[39] The FOIA empowers requesters to challenge exemptions, for instance, so that their lawsuits act as one of the law's primary enforcement mechanisms. *See* Buckhannon Bd. & Care Home, Inc., v. W. Va. Dep't of Health & Human Res., 532 U.S. 598, 635-36 (2001) (J. Ginsburg, dissenting) ("[C]ivil rights statutes vindicate public policies "of the highest priority," yet depend heavily upon private enforcement. Persons who bring meritorious civil rights claims, in this light, serve as "private attorneys general.") (quotations and citations omitted).

[40] Desiree Hellegers, *Civic Resistance to the Bush Administration's Culture of Fear and Secrecy*, Counterpunch.org, Jun. 24, 2005, http://www.counterpunch.org/hellegers06242005.html.

[41] *Id.*

[42] *Id.*

[43] O.R.S. § 133.545 (2005).

[44] "[A] now-forgotten New York Times exposé revealed that the FBI sent a memo to the task forces just before the big antiwar marches of 2003 detailing how to use antiterrorism tactics to spy on home-grown activists." Carol Rose & Chip Berlet, *Romney's Spy Center*, Boston Globe, Jun. 14, 2005, at A19; Unlike Oregon police, FBI agents *are* able to conduct such surveillance. The Justice Department eliminated regulations barring such surveillance in 2002. Those now-obsolete regulations were the product of public outrage over the FBI's

FBI refused. Choosing not to surrender its historic and legal duty of supervising its own local police force, Portland withdrew its voluntary participation in the FBI task force.[45] Portland Mayor Tom Potter assured citizens that the task force withdrawal would not compromise safety, however. Portland would still cooperate with the FBI on local investigative efforts, he said, just not in the context of a secret task force.[46]

Portland's pullout from the FBI task force, accompanied by its continuing willingness to enter an alternative partnership that would be marked by less federal secrecy, demonstrates that state governments have considerable room to negotiate their discretionary partnerships with the federal government on their own terms.

IV. SECRECY UNDERMINES SAFETY

Post-9/11 federal secrecy also weakens state and local governments' ability to effectively address public safety issues. Secrecy leaves state and local governments without the information necessary to effectively develop programs to combat terrorism at the regional level. They find themselves concentrating on misguided or duplicative emergency preparedness when resources would be better directed to actual community safety needs.

A. COLOR-CODED CONFUSION

The United States government employs a color-coded threat level system to publicize terrorist threat information to public officials and the public-at-large.[47] With the colors green, blue, yellow, orange, and

---

COINTELPRO program in the 1970's. COINTELPRO was "aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence." *Id.*

[45] Desiree Hellegers, *Civic Resistance to the Bush Administration's Culture of Fear and Secrecy*, Counterpunch.org, Jun. 24, 2005, http://www.counterpunch.org/hellegers06242005.html

[46] Interestingly, the government has denied citizens in Washington, New York, and Los Angeles the right to even see their police departments' task force agreements with the FBI. Because the task force agreements detail which city officials will be granted security clearances, if any, residents of those cities are not even permitted to know whether their task force eradicates the local police's oversight mechanism for its officers. Id.

[47] Department of Homeland Security, *About the Homeland Security Advisory System*, http://www.dhs.gov/dhspublic/display?theme=29 (last visited July 28, 2005).

red, federal officials communicate low, general, significant, high, and severe levels of risk, respectively.[48] The Homeland Security Advisory Council ("HSAC") is the government body responsible for deciding when to elevate the national terror threat level using the color-coded system. To raise the national terror threat level, a majority of the council must determine that the likelihood of terrorist attack has sufficiently increased, and then President Bush must agree. The Homeland Security Chief, Attorney General, FBI Director, CIA Director, Defense Secretary, and Secretary of State are all members of the council.[49]

In May 2005, former Homeland Security Secretary Tom Ridge revealed that state and local governments often outlaid large amounts of money on temporary security upgrades when the national terror threat was raised from yellow to orange–the second-highest level–on flimsy intelligence without the nature of the threat being publicly explained.[50]

"There were times when some people were really aggressive about raising it, and we said 'For that?'" Ridge said, without offering details.[51] One can safely speculate that one of the incidents Ridge had in mind occurred in May 2003, when then-Attorney General John Ashcroft and FBI Director Robert Mueller, two of the HSAC's members, famously called a press conference during which Ashcroft announced that al-Qaeda members were planning "to hit the United States hard."[52] The tenor of the conference, as the *Chicago Sun Times* colorfully put it, was such that Ashcroft stopped just "short of painting his and Mueller's faces orange" for effect.[53] In response, Ridge made

---

[48] *Id.*

[49] The White House, *Fact Sheet: Homeland Security Council*, http://www.whitehouse.gov/news/releases/2001/10/20011029-16.html (last visited Jan. 27, 2006).

[50] Mimi Hall, *Ridge Reveals Clashes on Alerts*, U.S.A. Today, May 10, 2005, *available at* http://www.usatoday.com/news/Washington/2005-05-10-ridge-alerts_x.htm (last visited Oct. 9, 2005).

[51] *Id*.

[52] *3RD LD: U.S. Says Another Al-Qaida Attack Could Be Imminent*, Asian Political News, June 1, 2004, *available at* http://www.findarticles.com/p/articles/mi_m0WDQ/is_2004_June_1/ai_n6279470.

[53] William O'Rourke, *Kerry Can Let Bush's Bad News Speak for Itself*, Chi. Sun Times, June 6, 2004, at 43.

a television appearance of his own and all but shrugged his shoulders out of confusion. To his knowledge, there was no new intelligence to justify Ashcroft and Mueller's alarmism.[54]

In June 2005, Ridge gave MSNBC's Lisa Myers the particulars of another yellow-to-orange moment that had given him pause. This particular warning was significantly motivated by what he called "bizarre, unique, unorthodox, unprecedented"–and later disproved–intelligence that the Al-Jazeera television network was scrolling coded messages to terrorists at the bottom of its televised news programs.[55]

Erring on the side of caution has its place, but also its cost. When the federal government elevates the terror threat level without any detailed explanation, state and local governments have to expand their short-term terrorism emergency preparedness spending on blind faith alone, "just to be safe."[56] In Chicago, for instance, elevated terror levels triggered $20,000 in additional expenditures a week.[57] Washington, D.C. Mayor Anthony Williams has noted that there is always an opportunity cost to local terror alert preparedness efforts. State and local governments are always also "dealing with garden variety… crime, which is inflicted on our neighborhoods and on our local communities" regardless of the federal terror alert.[58] There is no way for state and local governments to weigh those opportunity costs, however, when they are denied federal information that is classified or otherwise off limits pertaining to terror threats. Without such information as to why the terror threat level was elevated, communities are unable to gauge when additional security measures would be money well-spent.

---

[54] Nicholas Davis, *Credible Intelligence?*, The Batallion, June 3, 2004, *available at* http://www.thebatt.com/media/paper657/news/2004/06/03/Opinion/Credible.Intelligence-684257.shtml.

[55] Interview by Lisa Myers with Tom Ridge, former Secretary of Homeland Security (Jun. 27, 2005), *available at* http://www.msnbc.msn.com/id/8380328.

[56] *See* Department of Homeland Security, *supra* note 48 ("Raising the threat condition has economic, physical, and psychological effects on the nation.").

[57] Frank James et al., Terror Threat Raised to 'High', Chi. Trib., May 21, 2003, at C1.

[58] CNN News: Soledad O'Brien Interview with Mayor Anthony Williams, 2003 WLNR 7642225 (CNN television broadcast Dec. 22, 2003).

B. TIGHT LIPS SINK TRAIN SECURITY

Even when state and local governments know the nature of a terror threat in their community, federal secrecy leaves them uninformed as to what, if anything, has already been done at the federal level to address their citizens' safety risk in that regard. Making additional efforts could be duplicative. Not making any effort could leave people unsafe. The result, again, is that state and local governments, in their confusion, can become mired in ill-advised, resource-intensive projects. Such secrecy-induced waste colored a recent legal battle in Washington, D.C., that began when the D.C. City Council moved to address the extreme safety risk of a terrorist attack on a rail car carrying hazardous materials ("hazmat") within city limits. According to a July 2004 Homeland Security Council study, one such rail attack could cause 17,500 deaths, 10,000 severe injuries and 100,000 hospitalizations in an urban area.[59]

In studying the issue, the D.C. City Council learned that a March 2003 U.S. Transportation Department regulation on hazmat required that all hazmat rail carriers submit a rail terrorism security plan to the federal government. The council asked the federal government for full access to the security plan for CSX Transportation, Inc. ("CSX"), which was the only rail carrier that moved hazmat through the D.C. city limits, so that the city could determine whether it needed to enact supplemental safety laws.[60] The federal government refused to grant the council adequate access to its security-sensitive plans.[61] Left in the dark with regard to the adequacy of CSX's rail terrorism security plans, yet entrusted by Washingtonians to protect their safety, the D.C. City Council banned all hazmat rail traffic from passing within 2.2

---

[59] *Planning Scenarios, Executive Summaries Created for Use in National, Federal, State and Local Homeland Security Preparedness Activities*, Scenario 8, The Homeland Security Council, July 2004, http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04.htm (last visited Oct. 9, 2005).

[60] Whether CSX's plan comprehensively addressed rail terrorism security was not clear from the text of HM-232 itself. Although HM-232 required hazmat carriers to create and implement security plans, and gave a basic structural guide, it imposed no qualitative standards on the plans' substantive content. 49 C.F.R. § 172.800 et seq. (2005); 49 C.F.R. § 172.802.

[61] CSX Transp., Inc. v. Williams, No. 1:05CV00338, 2005 WL 902130 at *25 (D.D.C. 2005).

miles of the U.S. Capitol building (the "D.C. Act") on February 1, 2005.[62]

CSX sued, arguing that the D.C. Act was unconstitutional under federal preemption doctrine because it regulated the same subject matter – rail terrorism security – as the federal government had already regulated by ordering it to develop a rail security plan. The U.S. offered friend-of-the-court support for CSX's position.

The Sierra Club, which intervened in the litigation in support of D.C.'s position, became incensed when the federal government offered U.S. District Court Judge Emmet G. Sullivan an *in camera*, *ex parte* presentation of federal rail security measures. It was "indispensable" that D.C. also have access to the information, the Sierra Club said in a letter filed with Sullivan, so that the city itself could itself study to what extent the D.C. Act's effort was duplicative of or preempted by the federally required CSX plan.[63] Sullivan repeatedly pleaded with the federal government to share more information with the D.C. government so it could know just how comprehensive CSX's HM-232 plan really was, but the federal government declined. "I can't remember the last time parties in my court refused to even talk about settlement," he said shortly before issuing his decision.[64]

Sullivan denied CSX's petition for an emergency injunction of the D.C. Act on April 18.[65] CSX had not proven HM-232's preemptive effect on the issue of rail terrorism security, Sullivan said, because the federal government had so completely hidden the content of CSX's report, even from him.[66] Until that burden of proof was met, he

---

[62] Terrorism Prevention in Hazardous Materials Transportation Act of 2005, May 14, 2005, D.C. Law 16-2, 52 DCR 3154 (expired on Dec. 25, 2005), *available at* http://dccode.westgroup.com. Although no other jurisdictions have taken similar action, many have considered it, including Nevada, Cleveland, Baltimore, California, Pittsburgh, and Philadelphia.

[63] Defendant-Intervenor Sierra Club's Limited Response to United States Notice of Filing of Declaration of TSA Director of Rail Security and Proffer of Additional In Camera, Ex Parte Testimony, CSX Transp., Inc. v. Williams, No. 1:05CV00338 (EGS) (D.D.C. April 3, 2005), *available at* http://www.dccouncil.dc.gov/patterson/pages/prinfo/Hazmat%20SierraClub%20filing%20on%20plan04.04.05.pdf.

[64] Carol D. Leonnig, *Judge's Hazmat Rail Plan Rebuffed*, Wash. Post, Apr. 8, 2005 at B1, *available at* http://www.washingtonpost.com/wp-dyn/articles/A35507-2005Apr7.html.

[65] CSX Transp., Inc. v. Williams, No. 1:05CV00338, 2005 WL 902130 (D.D.C. 2005).

[66] On the other hand, Sullivan considered evidence that indicated that the HM-232 reports did not constitute a comprehensive rail security plan. Just three days after issuing his opinion, Sullivan issued a supplemental order to append a Washington Post article to the record. The article, which quoted former deputy administrator of the U.S. Transportation Security

concluded, "the Court will not blindly interfere with the actions of the District of Columbia to safeguard its citizens from a catastrophe."[67] CSX appealed immediately to the U.S. Court of Appeals in Washington (D.C. Circuit), where the issue of federal secrecy percolated once again before the three-judge appellate panel at oral argument on April 27, 2005. Of the CSX plan's alleged preemptive effect of the D.C. Act, Judge A. Raymond Randolph observed that "[f]or all we know [the plan] could say 'we're going to get around to addressing hazardous materials cars being driven'" through downtown D.C. next year.[68] And in an exchange with the U.S. government's counsel Douglas Letter, Judge John G. Roberts later added, "You're just telling the D.C. government and everybody else, don't worry, we've got everything under control."[69]

Despite Roberts and Randolph's ostensible understanding of federal secrecy's effects, the appellate court unanimously invalidated the D.C. Act in a May 3, 2005, *per curiam* opinion.[70] In reversing Sullivan's opinion, the court held that because the federal government meant to give CSX broad discretion in addressing rail terrorism security in its HM-232 plan, the D.C. Act was preempted regardless of the adequacy of CSX's efforts.[71]

In the wake of the court's preemption ruling, federal secrecy continues to compromise Washingtonians' safety. If CSX's "security-sensitive, highly confidential" HM-232 plan is woefully inadequate, the D.C. City Council might still develop strong emergency response plans on the ground to compensate. Left in the dark as to what is

---

Administration Stephen J. McHale's comments at a panel discussion, further substantiated that the federal government had not sufficiently addressed the threat of terrorist attacks on trains, Sullivan said. Supplemental Order, *CSX Transp., Inc. v. Williams*, No. 1:05CV00338 (EGS); Spencer S. Hsu, *Ex-Official Faults Hazmat Rail Security*, Wash. Post, Apr. 22, 2005, at A8 (McHale told panel attendees "There is no comprehensive, national plan.…"). In the end, Sullivan wrote, "the plan has never been submitted to the Court for its review nor is it clear from the records what the document entails. In fact, at the March 23rd hearing no one in the courtroom – not even the attorneys for the government or CSXT–had ever seen the plan." *CSX Transp., Inc.*, 2005 WL 902130, at *11.

[67] CSX Transp., Inc., 2005 WL 902130, at *25.

[68] Transcript of Oral Argument at 16, *CSX Transp., Inc.*, 406 F.3d 667 (No. 05-5131).

[69] *Id.* at 27.

[70] CSX Transp., Inc. v. Williams, 406 F. 3d 667 (D.C. Cir. 2005).

[71] *Id.* at 672.

going on, the council cannot effectively address any of the risks posed by the threat of rail terrorism.

C. RECOMMENDATIONS

The irony of federal secrecy is that it can undermine the security the federal government meant to strengthen by shutting down access to information in the first place. The national color-coded terror alert and D.C. hazmat case studies both present situations where local communities were arguably left less secure because of the federal government's refusal to share information.

Mechanisms already exist–and, indeed, have been suggested by various federal officials involved in the aforementioned cases–to permit the federal government to share more information with state and local governments without compromising security. In an August 2003 address to the National Governor's Association, Ridge pledged that the federal government would begin to tailor its elevation of the terror alert "to a city, a state, a region, a sector of the economy."[72] Current Homeland Security Secretary Michael Chertoff experimented with this idea recently when, in response to the July 7, 2005, terror attacks on London's subway system, he announced the elevation of the terror threat for the nation's public transportation systems only.[73] This more targeted warning is still rather vague in terms of communicating whether it relies on any specific intelligence, but at least its "more focused vagueness" respects state and local governments' need to wisely spend and conserve resources.

The federal government should try to share substantive information with state and local governments as much as possible. Judge Sullivan advocated for such openness in the DC hazmat case, where he opined that the federal government's absolutism in its secrecy policies needn't be so absolute:

> "The Court takes very seriously the sensitive nature of the government's measures to disrupt terrorist activities. The effectiveness of many of these measures depends on their continued secrecy. However, there are means available, including protective orders and other appropriate measures,

---

[72] Tom Ridge, Sec'y of Homeland Sec., Address at the Nat'l Governors' Ass'n (Aug. 18, 2003), *available at* http://www.dhs.gov/dhspublic/display?content=1200.

[73] Eric Lipton, *Authorities Step Up Security on American Transit Systems*, N.Y. Times, July 8, 2005, at A10.

> for plaintiff to attempt to meet its burden of proof and to share sensitive information with appropriate representatives of the other parties without compromising national security interests."[74]

In that case, despite Sullivan's view that it was appropriate, the federal government consistently refused to pursue any of those measures so that it could share additional information with the D.C. government. The FBI took a hard line with Portland in the task force controversy, too, offering to security-clear only one city official despite the city's protestations that it needed three clearances to adequately oversee its own employees' work.

It is impossible to make an armchair determination (especially with so many secret facts) as to whether the federal government was reasonable in refusing to grant additional security clearances or use protective orders in these cases to expand information sharing with state and local governments. It is clear, however, that federal officials should keep in mind that federal secrecy is not necessarily coextensive with security. Because federal secrecy disables state and local governments' ability to implement safety measures that are well-tailored to their citizens' needs just as much as it theoretically disables scheming terrorists from information allegedly indispensable to their attacks, the federal government should keep all information stakeholders in mind as they weigh the costs and benefits of squirreling records away.

V. CONCLUSION

Though a coordinated national plan of information withholding has the constitutional force to supplant or cripple local autonomy over state-level open government and safety initiatives, the good news is that federal secrecy's negative effects, when unnecessary, can be cured by federal and state government officials who rethink information withholding decisions. For federal officials, this means exercising the option to reassess an information closure decision in the face of its ostensibly nonsensical effects, as in the case of the color terror alert system or the D.C. hazmat controversy. "To reassess information closure" does not mean to revoke any and all secrecy challenged by a local government for being too restrictive, but rather to be receptive to

---

[74] CSX Transp., Inc., 2005 WL 902130, at *25.

information-sharing proposals that might scale back secrecy in measured, safe, and productive ways.

State officials, meanwhile, should closely study the extent to which federal secrecy actually annuls their own open government laws. A careful boundary determination works to maximize openness by refusing to accept a sloppily interpreted federal supremacy mandate as a bogus excuse for what is actually an illegal information withholding. Similarly, state officials should not treat their local commitment to open government law so nonchalantly as to carelessly surrender state government records to federal secrecy designations, either by submitting them to the Homeland Security Department for CII Act protection or by voluntarily signing onto a contract with the federal government when the terms of that contract impose stringent secrecy requirements.

When he signed the original version of the federal Freedom of Information Act into law on July 4, 1966, President Lyndon Baines Johnson said that "a democracy works best when the people have all the information that the security of the Nation permits." Forty years later in the midst of the United States' "global war on terror," we are still asking how much freedom of information national security permits; unfortunately for the American people, the Bush Administration's answer, perhaps understandably in the initial aftermath of 9/11, has frequently been "not much." Four years since the Bush Administration's public information policy moved so sharply towards secrecy in response to the terrorist attacks, perhaps it is time for federal- and state- government officials alike to consciously, cautiously work to limit that secrecy's negative effects on state and local government operations.