

University of Missouri School of Law Scholarship Repository

Faculty Publications

2006

CIA v. Sims: Mosaic Theory and Government Attitude

Christina E. Wells

University of Missouri School of Law, wellsc@missouri.edu

Follow this and additional works at: <http://scholarship.law.missouri.edu/facpubs>

 Part of the [National Security Law Commons](#)

Recommended Citation

Christina E. Wells, *Cia v. Sims: Mosaic Theory and Government Attitude*, 58 Admin. L. Rev. 845 (2006)

This Article is brought to you for free and open access by University of Missouri School of Law Scholarship Repository. It has been accepted for inclusion in Faculty Publications by an authorized administrator of University of Missouri School of Law Scholarship Repository.

CIA v. SIMS: MOSAIC THEORY AND GOVERNMENT ATTITUDE

CHRISTINA E. WELLS*

TABLE OF CONTENTS

Introduction	846
I. <i>CIA v. Sims</i> , FOIA, and Mosaic Theory	848
A. <i>CIA v. Sims</i>	848
B. Mosaic Theory, Government Secrecy, FOIA, and Judicial Deference.....	853
II. Mosaic Theory Beyond FOIA	856
A. The Reagan/Bush I Years	856
1. National Security Decision Directive 145	856
2. The Library Awareness Program	860
B. Post 9/11 Use of Mosaic Theory	863
1. Mosaic Theory in the Courts	863
2. Mosaic Theory Outside of the Courts.....	867
a. Sensitive but Unclassified Information.....	867
b. USA PATRIOT Act.....	869
III. Implications and Solutions.....	872
Conclusion	879

* Enoch H. Crowder Professor of Law, University of Missouri-Columbia School of Law. I am grateful to Jennifer Robbennolt, David Pozen, Jim O'Reilly, and Kent Gates for their comments on earlier versions of this Article. My thanks also go to all of the participants in the Administrative Law Discussion Forum whose lively discussion and insightful critiques dramatically improved the Article. Sarah Baron, Ben Cox, and Ted Norwood provided valuable research assistance for this Article. Finally, I am grateful for the generous financial support provided by the University of Missouri Law School Foundation.

“A little knowledge is a dangerous thing.”¹

INTRODUCTION

In *CIA v. Sims*,² the United States Supreme Court held that the CIA could withhold information about controversial government-sponsored psychological experiments in response to Freedom of Information Act (FOIA) requests.³ The Court reasoned that the requested information would reveal intelligence sources related to national defense, which were specifically protected from disclosure under the National Security Act of 1947.⁴ Accordingly, the Court concluded that the CIA could refuse to disclose the information under FOIA Exemption 3, which allows withholding of information “specifically exempted from disclosure by statute.”⁵

Numerous scholars assailed *Sims*, arguing that the Court’s broad reading of the National Security Act gave the CIA carte blanche to withhold information and operate with no accountability.⁶ *Sims*’ implications, however, go far beyond giving the CIA the ability to conceal its activities from scrutiny. *Sims* relied, in part, on a controversial theory known as mosaic theory—the notion that the government may withhold otherwise trivial or innocuous information because it *might* prove dangerous if combined with other information by a knowledgeable actor (especially a hostile intelligence agency).⁷ Reliance on mosaic theory expands the universe of exempt information and often leads to non-disclosure of information that otherwise would have been disclosed.

1. This quotation is a common adaptation of Alexander Pope’s “A little learning is a dangerous thing.” ALEXANDER POPE, *An Essay on Criticism*, in POETRY AND PROSE OF ALEXANDER POPE 37, 44 (Aubrey Williams ed., 1969).

2. 471 U.S. 159 (1985).

3. 5 U.S.C. § 552 (2000).

4. *Sims*, 471 U.S. at 173; see also 50 U.S.C. § 403-3(d) (2000) (granting to the director of the Central Intelligence Agency (CIA) the power to collect intelligence through human and other sources).

5. 5 U.S.C. § 552(b)(3).

6. See generally Brent Filbert, *Freedom of Information Act: CIA v. Sims, The CIA Is Given Broad Powers to Withhold the Identities of Intelligence Sources*, 54 UMKC L. REV. 332, 332 (1986); Martin E. Halstuk, *Holding the Spymasters Accountable After 9/11: A Proposed Model for CIA Disclosure Requirements Under the Freedom of Information Act*, 27 HASTINGS COMM. & ENT. L.J. 79, 83 (2004); Amy E. Rees, *Recent Developments Regarding the Freedom of Information Act: “A Prologue to a Farce or a Tragedy; or, Perhaps Both,”* 44 DUKE L.J. 1183, 1192 (1995).

7. See, e.g., *Sims*, 471 U.S. at 178 (reasoning that “[f]oreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details”).

The core of mosaic theory—that hostile intelligence agencies can piece together puzzles from smaller bits of information—can be a legitimate one. As asserted by the government in FOIA (and, increasingly, state secrets) cases,⁸ however, mosaic theory too often is a crude tool that results in excessive secrecy by demanding extreme deference from judges when national security is involved. Often, lower courts, concerned with their own inadequacy to make national security decisions, unquestioningly accept government assertions regarding the need for complete secrecy. *Sims*' acceptance of mosaic theory at the Supreme Court level embraced this notion of extreme judicial deference and made clear its validity. More importantly, *Sims*' approval of mosaic theory reinforced a concomitant government attitude that "a little knowledge is a dangerous thing." Mosaic theory thus crept into the government's collective consciousness as various officials and agencies used it to justify other secrecy-based actions in the name of national security, many of which occurred outside of FOIA.

Several observers criticize the courts' use of mosaic theory in the FOIA context.⁹ Given the indiscriminate manner in which the government has wielded mosaic theory and the courts' refusal to check the government's actions, such criticism is understandable—particularly when one traces the use of that theory beyond FOIA. Reining in government abuse of the mosaic theory, however, need not require disposing of it altogether. Not

8. Because the articles in this forum pertain to the "most underrated *administrative* law decision," and because *Sims* involved FOIA, I chose to focus on mosaic theory as it arose in the FOIA context. However, mosaic theory was asserted in a lower court case involving the state secrets litigation privilege prior to its use in FOIA cases. See *Halkin v. Helms*, 598 F.2d 1, 8 (D.C. Cir. 1978) ("It requires little reflection to understand that the business of foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair."). The state secrets privilege allows the executive to resist discovery of information in civil litigation by asserting privilege with respect to state and military secrets that would adversely affect national security if divulged. See *United States v. Reynolds*, 345 U.S. 1, 6-7 (1953). Mosaic theory is often invoked when the privilege is asserted. See, e.g., *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Edmonds v. Dep't of Justice*, 323 F. Supp. 2d. 65, 77-78 (D.D.C. 2004); *Maxwell v. First Nat'l Bank of Maryland*, 143 F.R.D. 590, 597 (D. Md. 1992). Much of the criticism of mosaic theory regarding FOIA applies to the state secrets privilege. For more discussion on state secrets, see *infra* notes 102-06.

9. For an excellent, in-depth critique of mosaic theory in the FOIA context, see David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005). See also Kenneth W. Graham, Jr., *Government Privilege: A Cautionary Tale for Codifiers*, 38 LOY. L.A. L. REV. 861 (2004); Peter Margulies, *Above Contempt?: Regulating Government Overreaching in Terrorism Cases*, 34 SW. U. L. REV. 449 (2005); Alice Ristorph & Jameel Jaffer, *Security's Province in a Democratic Society*, in DEMOCRACY AND HOMELAND SECURITY: STRATEGIES, CONTROVERSIES, AND IMPACT (Nawal H. Ammar ed., 2004), available at <http://upress.kent.edu/Ammar/05%20Ristorph.Jaffer.htm>; Steven J. Lepper, Note, *Developments Under the Freedom of Information Act—1982, 1983* DUKE L.J. 390 (1983); Jonathan Turley, *Through a Looking Glass Darkly: National Security and Statutory Interpretation*, 53 SMU L. REV. 205 (2000); Shannon Vibbert, Comment, *A Twisted Mosaic: The Ninth Circuit's Piecemeal Approval of Environmental Crime in Kasza v. Browner*, 17 J. NAT'L RESOURCES & ENVTL. L. 95 (2003).

only does widespread judicial acceptance of the theory suggest that such a result is infeasible, there are times when mosaic theory may serve legitimate purposes. Accordingly, our goal should be to focus government assertions of mosaic theory so that they relate to potential, identifiable harms and account for possible costs rather than act merely as a convenient justification to shut down inquiry into the government's case. Such a task is neither Herculean nor wrongheaded; application of mosaic theory in the counterintelligence arena itself relies upon adequate threat assessment for proper functioning. If we begin this task of focusing government assertions in the FOIA arena, the change ideally will trickle down to other government behavior as well.

Part I of this Article discusses *Sims*, its relationship to FOIA, and its importance to mosaic theory. It concludes with a discussion of the relationship of mosaic theory and judicial deference. Part II examines the government's post-*Sims* use of mosaic theory beyond the FOIA context. It first examines the Reagan Administration's aggressive use of the theory with "sensitive but unclassified" technical information and the "Library Awareness Program," both of which were controversial and eventually abandoned. Part II then examines the government's post-9/11 assertions of mosaic theory, many of which mirror the Reagan Administration's ill-fated attempts. In an effort to effect governmental attitude change more globally, Part III discusses a more legitimate role for mosaic theory in FOIA cases. Part III proposes a more nuanced role for mosaic theory that requires government officials to identify more specifically the harms they seek to prevent and further proposes mechanisms that force courts into engaging in meaningful judicial review to ensure that government officials are accountable for their decisions.

I. *CIA v. SIMS*, FOIA, AND MOSAIC THEORY

A. *CIA v. Sims*

Sims involved a FOIA request regarding MKULTRA, a CIA-funded project involving psychological research, including research on human subjects. Through the various MKULTRA research projects, contracted out to 185 researchers at 85 institutions between 1953 and 1966, the CIA hoped to gain an understanding of brainwashing and interrogation techniques used by the Chinese and Soviet governments.¹⁰ The CIA also hoped that the research might develop chemical and biological methods of

10. *CIA v. Sims*, 471 U.S. 159, 163 (1985); *Sims v. CIA*, 479 F. Supp. 84, 85 (D.D.C. 1979).

obtaining information from foreign intelligence agents.¹¹ Because the CIA operated MKULTRA through a front organization, most of the institutions and researchers participating in the experiments were unaware that they were working at the behest of the CIA.¹² Further, while some human subjects willingly participated in the chemical and biological experiments, others were unaware that they were part of a government-operated research project.¹³ At some point, the CIA's experimental program became public, prompting congressional investigation.¹⁴ However, in 1973, prior to those investigations, the CIA destroyed most of the documents relating to MKULTRA, and thus these public investigations "depended largely on oral testimony" to flesh out MKULTRA's parameters.¹⁵ In 1977, however, the CIA discovered the existence of certain documents related to the identities of the researchers and their affiliated institutions, along with other fiscal and financial records.¹⁶

This newly discovered information prompted individuals associated with Public Citizen, a public interest group, to file FOIA requests for the identities of the MKULTRA researchers and their affiliated institutions.¹⁷ After consulting with the institutions, the CIA disclosed the names of fifty-nine institutions that consented to their release, but it did not confer with or disclose the names of any individual researchers.¹⁸ The CIA refused to disclose the remaining information claiming that the researchers and affiliated institutions were "intelligence sources" within the meaning of the National Security Act and, therefore, it could withhold the information pursuant to FOIA Exemption 3.¹⁹

The district court acknowledged that the National Security Act, which vests the CIA director with responsibility "for protecting intelligence sources and methods from unauthorized disclosure,"²⁰ qualified as an Exemption 3 statute. However, the court ruled that the CIA did not show

11. *Sims*, 479 F. Supp. at 85; *Sims v. CIA*, 642 F.2d 562, 564 (D.C. Cir. 1980) (*Sims I*).

12. *Sims I*, 642 F.2d at 564.

13. *Id.*

14. See SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT, S. REP. NO. 94-755, Book I, at 389-409 (1976); "Project MKULTRA, The CIA's Program of Research in Behavioral Modification": Joint Hearings Before the S. Comm. on Intelligence and the Subcomm. on Health and Scientific Research of the S. Comm. on Human Resources, 95th Cong., 1-5 (1977); see also COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES: REPORT TO THE PRESIDENT 226-28 (1975).

15. *Sims I*, 642 F.2d at 564.

16. *Id.*

17. *Sims*, 479 F. Supp. at 84. The plaintiffs also requested grant proposals and contracts for those who performed MKULTRA research, which the CIA turned over without contest. *Id.* at 84 n.1.

18. *Id.* at 85; *Sims I*, 642 F.2d at 565.

19. *Sims*, 479 F. Supp. at 85.

20. 50 U.S.C. § 102(d)(3) (2000).

that the researchers and their affiliated institutions qualified as “intelligence sources” under the Act. According to the court, the CIA had not demonstrated particular facts or clear guidelines supporting the characterization of researchers and institutions as “intelligence sources,” nor had the CIA provided anything but the broadest definition of the phrase “intelligence sources.”²¹ Concerned that the CIA’s definition was “susceptible to discretionary application and overbroad interpretation” that might conflict with FOIA’s emphasis on disclosure, the court ruled Exemption 3 inapplicable.²² It held out the possibility, however, that the CIA could reclassify the identities of the researchers and institutions and withhold them under FOIA Exemption 1.²³

On appeal, the Court of Appeals for the District of Columbia determined that the district court had operated without a sufficient definition of “intelligence source.”²⁴ After reviewing the purposes and text of FOIA, the National Security Act and the Central Intelligence Agency Act of 1949,²⁵ the Court determined that:

“[I]ntelligence source” is a person or institution that provides, has provided, or has been engaged to provide the CIA with information of a kind the Agency needs to perform its intelligence function effectively, yet could not reasonably expect to obtain without guaranteeing the confidentiality of those who provide it.²⁶

It thus remanded with directions to the lower court to reconsider the Exemption 3 issue in light of this new definition.

On remand, the district court asked the CIA to submit evidence that the individuals and institutions withheld were “intelligence sources” within the new definition.²⁷ It further suggested that the CIA actually contact individual researchers to determine their understanding of the nature of their relationship with the CIA—something the CIA apparently had never

21. *Sims*, 479 F. Supp. at 87. The CIA characterized an intelligence source as “any contributor . . . to the intelligence process.” *Id.* The CIA admitted that such a definition was broad enough to apply to “periodicals including Pravda and the New York Times from which it culls information that informs its view of foreign nations and their policy intentions.” *Sims I*, 642 F.2d at 569.

22. *Sims*, 479 F. Supp. at 87.

23. *Id.* at 88. FOIA Exemption 1 allows an agency to withhold national security information that has been properly classified pursuant to executive order. 5 U.S.C. § 552(b)(1). The identities of the researchers and their affiliated institutions were originally classified, but the CIA had declassified them by the time of the FOIA request so they did not qualify for Exemption 1 withholding. *Sims*, 479 F. Supp. at 88. The district court also found wanting the CIA’s evidentiary support for its claim that the information could be withheld under Exemption 6, which protects “personnel and medical files” and similar information under an invasion of privacy theory. *Id.* at 88-89.

24. *Sims I*, 642 F.2d at 564.

25. 50 U.S.C. §§ 403a-403j (2000).

26. *Sims I*, 642 F.2d at 571.

27. *Sims v. CIA*, 709 F.2d 95, 97 (D.C. Cir. 1983) (*Sims II*).

done.²⁸ After reviewing the evidence, the district court determined that certain individuals and institutions did not qualify as “intelligence sources” because they had not actually been promised confidentiality.²⁹ On appeal, the D.C. Circuit found that the district court had erred in looking at “whether the agency had, in fact, promised confidentiality to individual researchers.”³⁰ Rather, this important issue was governed by an objective standard: whether the CIA could reasonably expect to obtain the particular information at issue from sources without pledging them confidentiality.³¹ The court of appeals made clear, however, that to qualify as an “intelligence source,” the expectation of confidentiality must come from the source of information rather than the agency.³² The court of appeals remanded the case again to the district court for application of the correct standard regarding the researchers’ status.

The CIA appealed the case to the Supreme Court, which ruled in the agency’s favor, finding that the identities of researchers and institutions were exempt under FOIA.³³ The Court first noted that the lower court’s definition of “intelligence sources” under the National Security Act “not only contravene[d] the express intention of Congress, but also overlook[ed] the practical necessities of modern intelligence gathering.”³⁴ According to the Court, both the text and legislative history of the Act reflected a clear congressional intent that the CIA would call on a wide variety of intelligence sources and that the CIA was to protect those sources, regardless of the need to guarantee confidentiality.³⁵ Consequently, the Supreme Court held that the MKULTRA researchers were “intelligence sources” because they “provided, or were engaged to provide, information the Agency needs to fulfill its statutory obligations with respect to foreign intelligence,” regardless of any promises of secrecy made to the researchers.³⁶ As scholars have noted, this aspect of the Court’s decision

28. *Id.* The district court repeatedly suggested that the CIA contact individual researchers and also intimated that such an action might establish a common law or constitutional right to protection of their anonymity. *Sims*, 479 F. Supp. at 85. The CIA never presented evidence “that researchers and institutions in this case were given promises of confidentiality” and instead chose to rely on Exemption 3 to withhold the information. *Id.*

29. *Sims II*, 709 F.2d at 98.

30. *Id.*

31. *Id.* at 100.

32. *Id.*

33. *CIA v. Sims*, 471 U.S. 159, 181 (1985).

34. *Id.* at 168-69.

35. *Id.* at 169-73.

36. *Id.* at 173-74.

gave the CIA nearly unfettered discretion to determine who an intelligence source is and grants the agency a nearly wholesale exemption from FOIA scrutiny.³⁷

The Court's reasoning with respect to whether the researchers' institutional affiliations were exempt under FOIA, however, had even broader implications. As with the identity of the researchers, the Court found the affiliation information exempt under FOIA. In fact, the answer was so closely linked to the issue of individual researchers that it "render[ed] unnecessary any extended discussion of this discrete issue."³⁸ Given that close relationship and the CIA's broad discretion under the National Security Act, the most logical step would have been to allow withholding of affiliation information to protect the identities of individual researchers.³⁹ Instead, the *Sims* Court relied on mosaic theory.

According to the Court,

Foreign intelligence services have an interest in knowing what is being studied and researched by our agencies dealing with national security and by whom it is being done. Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details.

In this context, the very nature of the intelligence apparatus of any country is to try to find out the concerns of others; bits and pieces of data "may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself." Thus

"[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."

... The decisions of the [CIA, which] must of course be familiar with "the whole picture," as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake. It is conceivable that the mere explanation of why information must be withheld can convey valuable information to a foreign intelligence agency.⁴⁰

Although the CIA had identified many institutions during the FOIA litigation or earlier congressional investigations, the Court allowed CIA officials to withhold identification of other institutions. Selective revelation of information, the Court reasoned, was part of the intelligence

37. See sources cited *supra* note 6.

38. *Sims*, 471 U.S. at 178.

39. See *id.* at 179 (noting the lower court's reasoning that the CIA need not disclose affiliations of exempt researchers because disclosure might lead to indirect identification of individual researchers).

40. *Id.* at 178-79 (quoting *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) and *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978)) (internal citations omitted).

game, and the Court would not question the CIA's decision "to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process."⁴¹

By adopting mosaic theory, *Sims* did more than give the CIA broad discretion when determining who an intelligence source is. Rather, *Sims* embraced a theory that allowed the government to broaden considerably the universe of information considered to be dangerous if disclosed and adopted notions of judicial incompetence with respect to national security determinations. Furthermore, *Sims*' ruling was not limited to the identification of intelligence sources under the National Security Act. Rather, its reasoning can be applied whenever the government seeks to withhold information relying on a national security rationale—for example, under Exemption 1.

B. Mosaic Theory, Government Secrecy, FOIA, and Judicial Deference

Mosaic theory has long been associated with the intelligence gathering process. As one observer noted:

[The modern] business of foreign intelligence . . . is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair. Thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate.⁴²

Thus, mosaic theory is a theory of informational synergy in which intelligence agencies convert independently innocuous information into potentially significant intelligence information.⁴³ For national security purposes, United States intelligence agencies find construction of such mosaics particularly useful as they attempt to discover what others are doing. What can be done by United States intelligence agencies, however, can be done by hostile intelligence agencies. Thus, our government also sees mosaic theory as a justification for government secrecy.

Under FOIA, however, government officials may withhold requested information only if it falls within a specific exemption. For national security purposes, agencies generally rely on Exemption 3, if there exists a statute specifically authorizing withholding such as in *Sims*, or on Exemption 1, which applies to classified national security information.⁴⁴ If the requested information does not credibly fall within the terms of an exemption, the government should disclose it. In response to FOIA

41. *Sims*, 471 U.S. at 180-81.

42. *Halkin*, 598 F.2d at 8.

43. See Pozen, *supra* note 9, at 630.

44. See *supra* note 23 and accompanying text.

requests involving national security, government officials find mosaic theory particularly useful because it allows them to argue that information not evidently posing a threat to national security should nevertheless be considered appropriately classified or exempt. Their reasoning is that otherwise apparently innocuous information can be pieced together with other information to form part of a larger, more dangerous picture. Thus, the information, though admittedly innocuous in isolation, *could* prove to be dangerous and must be withheld. Accordingly, mosaic theory is an attempt to expand the government's ability to withhold information under existing law.

Even so, the assertion that an item of information poses a potential danger and thus must remain secret need not go wholly unreviewed. FOIA requires that judges faced with FOIA lawsuits review the government's claim of exemption *de novo*.⁴⁵ Thus, judges are justified in demanding that the government connect the dots between the apparently innocuous piece of information withheld and the larger, more dangerous picture to which it is allegedly connected. In *Sims*, however, the CIA preempted such demands by asserting that only it was "familiar with 'the whole picture' as judges [were] not" and that "mere explanation of why information must be withheld [could] convey valuable information to a foreign intelligence agency."⁴⁶ Accordingly, agency officials argue, judges must defer to the agency's superior information and skill.

Invocation of mosaic theory thus creates a vacuum of knowledge that effectively paralyzes judicial assessment of the government's claims. All mosaic theory claims by their very nature are speculative regarding possible harms. Typically, speculative claims and lack of information weigh against the government. Mosaic theory turns this lack of information and speculation to the government's advantage by explicitly casting the judge as an outsider, ill-suited to understanding the bigger picture. It also uses the judge's lack of expertise as a reason to refuse to provide information that might educate the judge (on the never-quite-spoken assumption that it would be mishandled), thus further hampering judicial resolution of disputes.

In addition, mosaic theory raises the specter of hostile intelligence agencies lying in wait (as one court put it, like "zealous ferrets")⁴⁷ for the opportunity to wreak havoc with that one, seemingly innocent piece of judicially released information. Psychological research shows that such visions of potentially catastrophic events play on extremely vivid fears, causing people to react to them regardless of an assessment of the actual

45. 5 U.S.C. § 552(a)(4)(B) (2000).

46. *Sims*, 471 U.S. at 179.

47. *Gardels v. CIA*, 689 F.2d 1100, 1106 (D.C. Cir. 1982).

risk.⁴⁸ Invocation of a possibly serious threat to national security would tend to cause judges to defer to agency claims, especially given the absence of information and the lack of adequate guideposts for judicial review.⁴⁹ In fact, the presence of so many variables in mosaic theory—a hostile intelligence agency that might be lurking about (or not), a potentially dangerous result (or not), a bigger picture that could be constructed (or not) with this innocuous (or not) piece of the puzzle—leads to extreme judicial deference.⁵⁰

Even absent the invocation of mosaic theory, judges have never shown a strong desire to scrutinize overly careful government withholdings relying on a national security rationale.⁵¹ But FOIA contemplates that judges have a role in reviewing FOIA disputes involving national security, especially after Congress amended the Act in response to *EPA v. Mink*.⁵² A court that

48. Paul Slovic, *Perception of Risk*, in *THE PERCEPTION OF RISK* 220 (Ragnar E. Löfstedt ed., 2000).

49. For an argument regarding government use of “catastrophic” fears designed to cause judicial deference in a slightly different context involving national security, see Christina E. Wells, *Fear and Loathing in Constitutional Decision-Making*, 2005 Wis. L. REV. 115.

50. Pozen, *supra* note 9, at 641 (noting that mosaic theory presents the courts with a reason “to fear disclosure and mistrust their own judgment”).

51. See Christina E. Wells, “National Security” Information and the Freedom of Information Act, 56 ADMIN. L. REV. 1195, 1207-08 (2004) (discussing uneven application of the de novo review standard to national security cases under FOIA Exemption 1); see also ALFRED C. AMAN, JR. & WILLIAM T. MAYTON, ADMINISTRATIVE LAW § 17.4.1, at 661-62 (2d ed. 2001) (noting the deference with which judges review FOIA national security exemption claims); 1 JAMES T. O’REILLY, FEDERAL INFORMATION DISCLOSURE § 11.26, at 539-41 (3d ed. 2000) (explaining that “[d]eference by courts to classification exceptions is the norm” and that “an agency claim of damage to national security from release of intelligence sources and methods would be deferentially accepted by many courts”). In the FOIA Exemption 1 context, for example, although courts acknowledge FOIA’s requirement of de novo review, they also pay heed to Congress’s admonition that “in making *de novo* determinations . . . [courts] will accord substantial weight to an agency’s affidavit concerning the details of the classified status of the disputed record.” H.R. REP. NO. 93-1200, at 12 (1974). Many courts rely on this language to grant summary judgment for the government as long as the government’s arguments are logical and plausible and its affidavits are reasonably detailed, indicate good faith, and conform to existing classification requirements. See, e.g., *Frugone v. CIA*, 169 F.3d 772, 775 (D.C. Cir. 1999) (deferring to the counterintelligence expertise of the CIA and noting that “government affidavits regarding harm that disclosure could cause to national security [are] entitled to ‘substantial weight’”); *Abbotts v. NRC*, 766 F.2d 604, 606 (D.C. Cir. 1985) (citing the same language from the House report and granting summary judgment to the Nuclear Regulatory Commission based on the Commission’s affidavits); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984) (applying the standard cited in the House Report and approving the CIA’s non-disclosure of information).

52. 410 U.S. 73 (1973). In *Mink*, the Supreme Court interpreted an earlier version of FOIA Exemption 1 as allowing judges only to review the procedural propriety of an official’s decision to classify material in the name of national security and not whether the classification was substantively proper under the Executive Order. *Id.* at 82. Congress amended FOIA to reflect the current requirement that information is exempt only if it is “specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and . . . [is] in fact properly classified pursuant to such Executive order.” 5 U.S.C. § 552(b)(1). Congress intended to overrule

fully embraces the government's version of mosaic theory, however, is unlikely ever to question seriously the government's assertions or require the government to justify its refusal to disclose information. The theory is designed to short-circuit such questioning.

Sims was not the first case to endorse mosaic theory—it relied on a trilogy of lower court cases that popularized the theory.⁵³ But its willingness to embrace mosaic theory had significant implications. *Sims* gave the Supreme Court's imprimatur to what was merely a theory in the lower courts, removing any doubt about its vitality. Furthermore, although *Sims*' discussion of mosaic theory involved the CIA's FOIA obligations under the National Security Act, *Sims* did not limit the theory to that context and, indeed, mosaic theory—and attendant notions of judicial deference—have spread to any FOIA dispute involving national security.⁵⁴ Finally, *Sims*' unquestioning acceptance of mosaic theory must have solidified the government's attitude toward its obligation to disclose information—that is, *Sims*' extreme deference to the CIA's assertions reinforced the government's attitude that it need not disclose information or justify its decisions. The next section discusses this attitude and the concomitant spread of mosaic theory beyond the FOIA context.⁵⁵

II. MOSAIC THEORY BEYOND FOIA

A. The Reagan/Bush I Years

1. National Security Decision Directive 145

In the final decade of the Cold War, the Reagan Administration became increasingly concerned about Soviet espionage regarding scientific and

Mink and broaden judicial review in this area. See H.R. REP. NO. 93-876, at 7-8 (1974) (citing two proposed amendments to FOIA that aim to increase judicial authority to “engage in a full review of agency action with respect to information classified by the Department of Defense and other agencies under Executive authority”). Similarly, FOIA gives courts discretion to exercise *in camera* review of documents or require segregation and release of all non-exempt portions of documents. 5 U.S.C. § 552(a)(4)(B) (2000).

53. See *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) (taking into account that “each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of intelligence information even when the individual piece is not of obvious importance in itself”); *Halkin v. Helms*, 598 F.2d 1, 8 (D.C. Cir. 1978) (analogizing “the business of foreign intelligence gathering in this age of computer technology” to the “construction of a mosaic”); *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972) (“What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene . . .”).

54. For a discussion of judges' deferential application of mosaic theory in cases involving national security, see Pozen, *supra* note 9, at 643-45.

55. Whether the spread of mosaic theory resulted from *Sims* or simply happened at relatively the same time is likely unknowable. However, it is reasonable to assume that the Court's extremely deferential approach to mosaic theory at least reinforced the government's attitude toward using it.

technical data. Consequently, it pursued a variety of tactics designed to protect information from potential spies.⁵⁶ President Reagan issued a new Executive Order broadening the federal government's ability to keep national security information secret.⁵⁷ Among other things, the Reagan order explicitly adopted mosaic theory as a basis for classifying information, thus writing into law what courts had earlier accepted as justification for withholding information.⁵⁸

In 1984, recognizing that new telecommunications and computer technologies increased vulnerabilities, President Reagan also issued National Security Decision Directive 145 (NSDD 145). NSDD 145 directed that those in possession of "sensitive but unclassified" government information—the "loss of which could adversely affect the national security interest"—should protect it "in proportion to the threat of exploitation and the associated potential damage to the national security."⁵⁹ It also vested control of computer security in the Department of Defense and the National Security Administration (NSA).⁶⁰ As time passed, it became clear that Reagan Administration officials intended to treat NSDD 145 as a means of withholding information.⁶¹ The Reagan Administration's

56. Janet Raloff, *Coming: The Big Chill?*, in FREEDOM AT RISK 86 (Richard O. Curry ed., 1988).

57. Exec. Order No. 12,356, 3 C.F.R. 166 (1982). For commentary on the Reagan order, see Harold C. Relyea, *Historical Development of Federal Information Policy*, in UNITED STATES GOVERNMENT INFORMATION POLICIES 25, 40 (Charles R. McClure et al. eds., 1989) (remarking that Reagan's Executive Order No. 12,356 reversed a thirty-year trend of narrowing classification criteria).

58. Exec. Order No. 12,356 § 1.3(b), 3 C.F.R. at 169 ("Information that is determined to concern one or more of the [classification] categories . . . shall be classified when [it is determined] . . . that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security."). President Clinton abandoned the Reagan Administration's expansive use of mosaic theory as a basis for classification in favor of a more restrictive and contextual use of the theory. For discussion, see Pozen, *supra* note 9, at 645.

59. National Security Decision Directive 145: National Policy on Telecommunications and Automated Information Systems Security ¶ 2b (1984), available at <http://www.fas.org/irp/offdocs/nsdd145.htm> (last visited Oct. 7, 2006). For a historical discussion of NSDD 145, see Genevieve J. Knezo, "Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy 10-12 (2003), available at <http://www.fas.org/irp/crs/RL31845.pdf> (last visited Oct. 7, 2006).

60. H.R. REP. NO. 100-235, pt. 2, at 13, reprinted in 1987 U.S.C.C.A.N. 3165; HAROLD C. RELYEA, SILENCING SCIENCE: NATIONAL SECURITY CONTROLS AND SCIENTIFIC COMMUNICATION 160 (1994).

61. A 1986 policy statement issued by then-National Security Advisor John Poindexter stated that "[s]ensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security." *National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems*, NTISSP No. 2 (1986), reprinted in Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (1987), available at www.blackvault.com/documents/ota/ota_3DATA/1987/8706.PDF at App. B (emphasis added). See also H.R. REP. NO. 100-235, pt. 2, at 14-15, reprinted in 1987 U.S.C.C.A.N. 3166-67 (declaring that NTISSP No. 2 expanded government control over a "wide spectrum

justification for this extension of authority sounded in mosaic theory: “[I]nformation, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate.”⁶²

In 1986, NSDD 145 found its way beyond government information. Relying on a provision exhorting government officials to encourage and assist the private sector regarding sensitive but unclassified information,⁶³ officials from the FBI, Department of Defense, NSA, and CIA visited private database vendors to discuss the Reagan Administration’s continuing concern that hostile intelligence agents might piece together government secrets from publicly available information.⁶⁴ Government officials visited companies—such as Mead Data Central (owner of LEXIS/NEXIS), Lockheed Corporation (owner of DIALOG), CompuServe, and various banks—and asked them to consider restricting the sale of sensitive but unclassified information to Eastern Bloc countries or to monitor requests so that the government surreptitiously could identify those requesting potentially sensitive information.⁶⁵ Government officials were concerned that, while a single newspaper article might prove innocuous, when coupled with the material available in an entire database, “the sum might turn out to be more dangerous—and therefore more in need of controls—than the individual pieces.”⁶⁶

This move significantly expanded mosaic theory. Not only did the government use it outside the context of Executive Order classification, it attempted to control material in the hands of non-governmental parties.⁶⁷ Not surprisingly, these actions were controversial. The Information Industry Association, an organization representing private data companies, protested the government’s requests for “voluntary compliance”⁶⁸ with its

of scientific, economic and cultural information”); David Banisar, *Stopping Science: The Case of Cryptography*, 9 HEALTH MATRIX 253, 259-60 (1999) (claiming that the Reagan Administration used NSDD 145 and NTISSP No. 2 directives to expand government control over a larger scope of information than was previously allowed).

62. National Security Decision Directive 145, *supra* note 59; *see also* Banisar, *supra* note 61, at 259 (“[NSDD 145] was based on the assumption that aggregating unclassified information could affect national security and, therefore, those systems should be controlled by the military.”).

63. National Security Decision Directive 145, *supra* note 59, at ¶ 2c.

64. H.R. REP. NO. 100-235, pt. 2, at 7, 14, *reprinted in* 1987 U.S.C.C.A.N. at 3159, 3167; Raloff, *supra* note 56, at 89; Banisar, *supra* note 61, at 260.

65. Raloff, *supra* note 56, at 89; Banisar, *supra* note 61, at 260; H.R. REP. NO. 100-235, pt. 2, at 7, 14, *reprinted in* 1987 U.S.C.C.A.N. at 3159, 3167.

66. Raloff, *supra* note 56, at 89; *see also* HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI’S LIBRARY AWARENESS PROGRAM 72 (1991) (citing the government’s concern that publicly available information, “once aggregated . . . could be used against national interests”) (internal citation omitted).

67. Raloff, *supra* note 56, at 90.

68. While the government asked for voluntary compliance, it apparently was willing to back its requests with coercion, including limiting the availability of government resources for those refusing to help, threatening export control prosecutions for failure to limit access to data, and limiting access to government information for refusing to comply. H.R. REP.

program, arguing that the Reagan Administration's "restrictions on the flow of unclassified information could severely limit the information available to citizens, have a chilling effect on those who wish to acquire information, restrict our nation's technological development, and hinder the ability of U.S. companies to do business."⁶⁹

At congressional hearings, others expressed similar concerns. Many were concerned that the restrictions on sensitive but unclassified information threatened industrial and scientific endeavors.⁷⁰ They also were bothered by the vague and amorphous definition of sensitive but unclassified information, a problem especially highlighted after a second Reagan Administration directive expanded the term to include a variety of economic, financial, industrial, agricultural, or technological information that *might* relate to the national defense or foreign relations.⁷¹ Others expressed concern about military involvement in civilian activities, especially in light of the federal government's surveillance abuses of the 1960s and 1970s.⁷² Eventually, the Reagan Administration reconsidered the need for NSDD 145.⁷³

No. 100-235, pt. 2, at 15-16, *reprinted in* 1987 U.S.C.C.A.N. at 3167-68.

69. Raloff, *supra* note 56, at 90 (quoting Paul G. Zurkowski, President, Information Industry Association).

70. H.R. REP. NO. 100-235, pt. 2, at 16-18, *reprinted in* 1987 U.S.C.C.A.N. at 3168-70.

71. *See* NTISSP No. 2 (Oct. 29, 1986), *reprinted in* *Defending Secrets*, *supra* note 61, at App. B (expanding the realm of classifiable information to include government interests related, but not limited to, the "wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information . . ."); *see also* H.R. REP. NO. 100-235, pt. 2, at 14-15, *reprinted in* 1987 U.S.C.C.A.N. at 3166-67 (commenting on the same directive and remarking that it expanded the Department of Defense's control over a wide spectrum of information).

72. H.R. REP. NO. 100-235, pt. 1, at 19, *reprinted in* 1987 U.S.C.C.A.N. at 3134 (citing several experts' concerns that NSDD 145 would impinge upon civil liberties and the free flow of information vital to scientific and economic development); H.R. REP. NO. 100-235, pt. 2, at 16-17, 19-31, *reprinted in* 1987 U.S.C.C.A.N. at 3168-69, 3171-83 (noting that NSDD 145 would "strangle the free flow of information in this country—all in the name of national security" and echoing similar concerns of organizations such as the ACLU, Aetna Life and Casualty Company, the American Banking Association, and the American Physical Society).

73. Raloff, *supra* note 56, at 91. The Reagan Administration also rescinded NTISSP No. 2. *Id.* This may have occurred because Congress passed the Computer Security Act of 1987, which vested in the National Bureau of Standards the power to establish uniform security standards for government computers and made clear that the Act did not convey the authority to limit information in the hands of private entities. Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724-30 (codified at 15 U.S.C. § 278g-3) (specifying that "[n]othing in amendment by Pub. L. 100-235 which enacted this section to be construed to constitute authority to . . . authorize any Federal agency to limit, restrict, regulate, or control collection, maintenance, disclosure, use, transfer, or sale of any information that is privately owned information . . .").

2. *The Library Awareness Program*

In 1985, also due to concern regarding Soviet acquisition of technical information, the FBI attempted to instigate a counterintelligence program in libraries designed to keep information out of Soviet hands (the Library Awareness Program).⁷⁴ According to the FBI, Soviet agents were engaged in ongoing efforts to collect unclassified, technical information from libraries, including the Library of Congress, specialized departments of university libraries, and large information clearinghouses.⁷⁵ FBI concerns ranged from Soviet intelligence officers posing as diplomatic officials while searching intelligence databases to Soviet attempts to enlist students and librarians to do research and potentially spy on their behalf.⁷⁶

As a result, the FBI visited libraries, focusing primarily on those in the New York City area.⁷⁷ FBI agents explained to librarians that they “were often targets of intelligence officers who seek ‘unclassified, publicly available information relating more often than not to science and technical matters.’”⁷⁸ Accordingly, the FBI attempted to enlist the librarians’ aid to protect against technology transfer and to engage in counter-surveillance for the FBI by reporting suspicious or unusual activity of foreigners.⁷⁹

74. The FBI had been concerned with such Soviet activities since the 1960s but the organized counterintelligence program ran from 1973-1976 and began again in 1985, around the time *Sims* was decided. FOERSTEL, *supra* note 66, at 14.

75. FEDERAL BUREAU OF INVESTIGATION, THE KGB AND THE LIBRARY TARGET, 1962-PRESENT 4-5, 30-31 (1988) [hereinafter THE KGB AND THE LIBRARY TARGET].

76. See Ulrika Ekman Ault, Note, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532, 1534-38 (1990).

77. See generally THE KGB AND LIBRARY TARGET, *supra* note 75 (indicating that the Scientific and Research Branch of the KGB was headquartered in New York City, KGB agents actively sought information in New York City libraries, and that the FBI sent agents to interview librarians in New York City to learn about these KGB visits). When the program initially was revealed, the FBI claimed that it was limited to New York City, but it appears that the FBI also pursued it elsewhere, although the extent of the program was never clear. FOERSTEL, *supra* note 66, at 51-71.

78. FOERSTEL, *supra* note 66, at 55, 79 (quoting Memorandum from FBI New York Office to FBI Headquarters (Sept. 21, 1987)); see also *FBI Counterintelligence Visits to Libraries: Hearings Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 100th Cong., 77-78 (1988) [hereinafter *FBI Counterintelligence Visits to Libraries*] (testimony of Paula T. Kaufman, Acting Vice President for Information Services and University Librarian, Columbia University) (noting that the FBI “explained that libraries such as ours were often used by KGB and other intelligence agents for recruiting activities”).

79. The FBI initially denied that the Library Awareness Program was designed to do anything other than educate libraries regarding their role as potential targets. Ault, *supra* note 76, at 1535-38. However, later documents and testimony belie this characterization. The FBI’s own publication indicates that it desired to enlist the aid of librarians in identifying possible Soviet activity regarding sensitive information. THE KGB AND THE LIBRARY TARGET, *supra* note 75, at 33. Similarly, reports from librarians indicate that the FBI requested that they monitor patron activity for suspicious behavior. *FBI Counterintelligence Visits to Libraries*, *supra* note 78, at 75, 81-82 (testimony of Paula Kaufman); FOERSTEL, *supra* note 66, at 56 (citing Interview with Nancy Gubman, librarian at NYU’s Courant Institute of Mathematical Sciences Library).

When faced with the libraries' responses that the material in their collections was unmonitored and freely available precisely because it was unclassified, the FBI countered with mosaic theory. At Columbia University, for example, the FBI explained that "singular information may be of little value, however, a compilation of these materials often assist [sic] these countries in their research programs."⁸⁰ Similarly, in describing the situation to librarians at NYU, the agents explained that "though the materials were unclassified, some items might be 'more sensitive than general library materials,' particularly when organized through data-base searches."⁸¹ In general, mosaic theory provided the framework for the entire FBI program.⁸²

Librarians, much of Congress, and the public responded negatively to the Library Awareness Program. Librarians objected to acting as counterintelligence agents, especially given that the FBI asked them to watch and report on patrons based on vague standards, such as whether someone was "acting against the security of the United States,"⁸³ sounded foreign, or had a foreign sounding name.⁸⁴ As one observer noted,

To comply with the requests the FBI makes of libraries—to identify Soviet agents or suspicious activity by persons that may be cooperating with Soviet agents—would require library staff to ascribe motives to the use of library resources and then report their judgments to the FBI. In effect, the FBI is asking librarians to police the use of libraries. [We] reject[] this information policing role, because the assignment cannot be undertaken without impinging on citizens' rights to privacy.⁸⁵

Others argued that such surveillance would inhibit the free exchange of ideas and "seriously and unnecessarily invade the intellectual life of citizens."⁸⁶ Still others noted that the Library Awareness Program was a

80. FOERSTEL, *supra* note 66, at 55; see also *FBI Counterintelligence Visits to Libraries*, *supra* note 78, at 32 (statement of C. James Schmidt, Executive Vice President, Research Libraries Group, Inc.) (referring to government's argument that access to unclassified information should be limited because "we are threatened by an 'information mosaic,' composed of separate bits of unclassified data such that the whole is greater than the sum of its parts.").

81. FOERSTEL, *supra* note 66, at 56 (quoting the author's interview with Nancy Gubman, librarian at NYU's Courant Institute of Mathematical Sciences Library).

82. See *THE KGB AND LIBRARY TARGET*, *supra* note 75, at 32-33 (noting the FBI's need to piece together Soviet intelligence efforts by pursuing all contacts between possible Soviet agents and Americans, including librarians).

83. FOERSTEL, *supra* note 66, at 59.

84. *FBI Counterintelligence Visits to Libraries*, *supra* note 78, at 75-76 (testimony of Paula Kaufman); Ault, *supra* note 76, at 1535 n.15.

85. *FBI Counterintelligence Visits to Libraries*, *supra* note 78, at 13 (statement of Duane E. Webster, Executive Director of Association of Research Libraries).

86. *Id.* at 24 (testimony of C. James Schmidt of the American Library Association).

thinly veiled government effort to control the dissemination of non-classified information in much the same vein as NSDD 145.⁸⁷ Finally, some critics noted that the FBI's request potentially violated state confidentiality laws.⁸⁸

Not content to leave privacy issues in the hands of state laws, members of Congress proposed legislation to protect the confidentiality of library circulation records. The proposed law would have prevented librarians from disclosing to law enforcement officials records related to library use unless there existed a court order (obtained after an opportunity for a full hearing) based upon "clear and convincing evidence" finding that the subject of the order was involved in criminal activity and the information sought was "highly probative."⁸⁹ The FBI, however, sought to amend the law so that it could obtain patrons' library records simply by using a "national security letter" (NSL), a form of administrative subpoena that allows the government to access records on a much lower showing than court orders require.⁹⁰ As a result of the FBI's lobbying efforts, and to avoid the insertion of an NSL provision, proponents of the bill eventually abandoned it.⁹¹ The Library Awareness Program also fell into disuse as a result of the public controversy surrounding it, although the FBI refused to abandon it altogether.⁹²

87. Representative Don Edwards, who opposed the program, noted that the "library visits were tied to the troubling, though sometimes fitful, government effort to control unclassified information." Don Edwards, *Government Information Controls Threaten Academic Freedom*, THOUGHT & ACTION: THE NEA HIGHER EDUC. J., Spring 1989, at 89. See also *FBI Counterintelligence Visits to Libraries*, *supra* note 78, at 13-14 (statement of Duane E. Webster) (reporting that the FBI attempted to gain access to private databases, linking the FBI's library program and NSDD 145).

88. See Ault, *supra* note 76, at 1549 ("Librarians have reported attempts by the FBI to force disclosures expressly prohibited by state confidentiality laws.").

89. See *Video and Library Privacy Protection Act of 1988: J. Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Cts., Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary and the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary*, 100th Cong. 5-6, 14 (1989) (statement of Hon. Robert W. Kastenmeier, Chairman, Subcomm. on Cts., Civil Liberties, and the Admin. of Justice) (proposing also that the law enforcement officials must show that less intrusive attempts to gain the information have failed and that the "value of information" sought prevails over privacy interests).

90. See *id.* at 146-47 (letter from Reps. Don Edwards and Robert Kastenmeier to Rep. Louis Stokes) (discussing proposed national security letter (NSL) amendment and criticizing the FBI's lobbying efforts); see also *infra* notes 91, 133 and accompanying text.

91. See FOERSTEL, *supra* note 66, at 132-33 (describing withdrawal of library bill after the FBI's legislative liaison approached Congress attempting to gain an exemption).

92. See *id.* at 74-76 (relating the FBI's attempts to assure the public that the program was still in use, while privately "back[ing] off" from using it).

B. Post 9/11 Use of Mosaic Theory

1. Mosaic Theory in the Courts

Other than in the FOIA and state secrets contexts, use of mosaic theory receded after the Reagan and Bush I Administrations, a phenomenon consistent with the Clinton Administration's more generous attitude toward FOIA and government openness.⁹³ Since 9/11, however, the Bush II Administration has invoked mosaic theory to justify numerous actions. Some of its most aggressive invocations involve FOIA.⁹⁴ In *Center for National Security Studies v. Department of Justice*, the government relied on mosaic theory to justify withholding the identification of certain people detained in the initial aftermath of the 9/11 attacks, as well as other information relating to their arrests and detentions (such as date and location of arrest or release).⁹⁵ Thus, the government argued that release of detainee information might interfere with law enforcement proceedings by allowing terrorists to map the course of the investigation and develop the means to impede it.⁹⁶ Similarly, in *ACLU v. Department of Justice*, the government relied on mosaic theory to justify withholding summary statistics about the enforcement of certain provisions of the USA PATRIOT Act, such as the number of times that certain kinds of intelligence-related subpoenas were issued.⁹⁷ The government again argued that release of such statistics, when coupled with other information in the public domain, might allow terrorists to map the FBI's investigative efforts.⁹⁸

In both cases, courts ultimately allowed the government to withhold information based on mosaic theory, although not everyone agreed. The district court in *Center for National Security Studies* originally ruled mosaic theory inapplicable to some of the information.⁹⁹ The appellate

93. See Thomas S. Blanton, *National Security and Open Government in the United States: Beyond the Balancing Test*, in NATIONAL SECURITY AND OPEN GOVERNMENT: STRIKING THE RIGHT BALANCE 33, 52-54 (2003), available at www.maxwell.syr.edu/campbell/Past%20Events/Papers/NSOG.pdf. (examining President Clinton's directives mandating openness).

94. At least one critic has noted that "the withholdings validated in the recent [post 9/11 mosaic theory] cases have been more speculative, more categorical, and more controversial than the withholdings validated before the attacks." Pozen, *supra* note 9, at 653-54.

95. See 215 F. Supp. 2d 94, 103 (D.D.C. 2002), *aff'd in part and rev'd in part*, 331 F.3d 918 (D.C. Cir. 2003).

96. See *id.*

97. See 321 F. Supp. 2d 24, 35 (D.D.C. 2004).

98. See *id.* at 37 (arguing that disclosure would inform terrorist organizations of the FBI's investigative techniques).

99. See *Ctr. For Nat'l Sec. Studies*, 215 F. Supp. 2d at 103-04 (finding that the defendants improperly relied upon mosaic theory because "there is simply no existing precedent" and applying it would "turn 7A into an exemption dragnet").

court reversed that ruling over the objection of Judge David Tatel, who accused his colleagues of “drastically diminish[ing], if not eliminat[ing], the judiciary’s role in FOIA cases that implicate national-security interests” based upon conclusory government affidavits and their own speculation.¹⁰⁰ Even the *ACLU v. Department of Justice* court noted that the government’s reliance on mosaic theory “may cast too wide a net,” although it upheld the Exemption 1 claim after citing to *Sims*.¹⁰¹

The Bush Administration increasingly invokes mosaic theory in state secrets situations as well. In litigation involving the wrongful termination of an FBI whistleblower,¹⁰² secret renditions of potential terrorists to other countries,¹⁰³ and the NSA surveillance schemes,¹⁰⁴ the government has relied on mosaic theory in its assertion of the state secrets privilege. Already a controversial privilege because of courts’ extreme deference in such cases,¹⁰⁵ the government’s use of mosaic theory with that privilege evidences the Bush Administration’s aggressive stance with respect to secrecy regarding government information. The results are significant. As a recent article noted, “the impossibility and mosaic theories, coupled with the courts’ demonstrated reluctance to even conduct *in camera* inspections of material before affirming secrecy, mean that an administrator’s decision to withhold information by assertion of the state secrets privilege is virtually unreviewable.”¹⁰⁶

100. *ACLU v. Dep’t of Justice*, 331 F.3d 918, 951 (D.C. Cir. 2003) (Tatel, J., dissenting).

101. See *ACLU v. Dep’t of Justice*, 321 F. Supp. 2d at 37-38 (yielding to the court’s reliance on *Sims*, 471 U.S. at 178 in *Cir. for Nat’l Sec. Studies*, 331 F.3d at 928).

102. See *Edmonds v. Dep’t of Justice*, 323 F. Supp. 2d 65, 77-78 (D.D.C. 2004), *aff’d*, 161 Fed. Appx. 6 (D.C. Cir. 2005) (arguing that the Court must defer to the government’s expertise, especially when national security is at risk).

103. See Memorandum of Points and Authorities in Support of Motion to Dismiss at 9, *El-Masri v. Tenet*, No. 1:05-cv-01417-TSE-TRJ (E.D. Va. Mar. 13, 2006), available at www.aclu.org/pdfs/safefree/govt_mot_dismiss.pdf (employing a “deferential standard of review” to suggest that the evidence supported the Director’s claim of privilege).

104. See *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 985-86 (N.D. Cal. 2006) (setting forth the government’s assertions regarding the need to dismiss plaintiffs’ lawsuit); Defendants’ Motion to Dismiss, or In the Alternative, for Summary Judgment at 12, *ACLU v. NSA*, No. 2:06-CV-10204 (E.D. Mich. May 26, 2006), www.cryptome.quintessenz.at/mirror/aclu-34.pdf (arguing that “the privilege is absolute” and the court should not weigh the needs of the parties).

105. See William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85, 86-87 (2005) (noting that in most cases in which the state secrets privilege is employed against citizens’ constitutional claims, the privilege is upheld). Weaver and Pallitto note that courts denied executive assertions of state secrets privilege in only four of the fifty-six reported cases decided from *United States v. Reynolds* until 2001. *Id.* at 101-02. See also Note, *The Military and State Secrets Privilege: Protection for the National Security or Immunity for the Executive?*, 91 YALE L.J. 570, 571 (1982) (suggesting that the manner in which state secret privilege has been used “seriously burdens discovery rights”).

106. Weaver & Pallitto, *supra* note 105, at 108. The “impossibility” theory involves a government assertion that the evidence sought is so critical to a plaintiff’s case that it cannot proceed absent the evidence. Successful invocation of the privilege requires dismissal of the

Mosaic theory also appears in government litigation unrelated to FOIA or state secrets. In September 2001, the Bush Administration closed to the public all “special interest” deportation proceedings involving people potentially related to the 9/11 attacks.¹⁰⁷ In two separate cases, *Detroit Free Press v. Ashcroft*¹⁰⁸ and *North Jersey Media Group, Inc. v. Ashcroft*,¹⁰⁹ media groups challenged the blanket closure, claiming that it violated the First Amendment’s guarantee of press access to legal proceedings.¹¹⁰ In both cases, the Bush Administration justified the blanket closure by arguing that “the importance of protecting against disclosure of information is not limited to obviously sensitive information. Even bits and pieces of information that may appear innocuous in isolation can fit into a bigger picture by terrorist groups in order to thwart the Government’s efforts to investigate and prevent terrorism.”¹¹¹

Although the cases proceeded on nearly identical legal and evidentiary lines, the *Detroit Free Press* and *North Jersey Media Group* courts ultimately split on the closure issue. The evidence supporting the government’s assertion of mosaic theory involved conclusory affidavits from agency officials—also liberally sprinkled with mosaic theory rhetoric—alleging that open hearings would: (1) reveal sources and methods of investigation, (2) provide information allowing terrorists to exploit the immigration system, (3) provide terrorists with the state of the FBI’s investigations and knowledge about terrorists, (4) allow terrorists to interfere by causing misleading evidence to be used, and (5) stigmatize those who eventually turn out to be unrelated to terrorism.¹¹² According to

case. See, e.g., *Tilden v. Tenet*, 140 F. Supp. 2d 623, 627 (E.D. Va. 2000). Government officials increasingly assert the privilege to avoid lawsuits rather than immunize particular information from discovery. See Scott Shane, *Invoking Secrets Privilege Becomes a More Popular Legal Tactic By U.S.*, N.Y. TIMES, June 4, 2006, at 32 (describing recent cases where the privilege was used to dismiss cases rather than protect certain documents).

107. See *North Jersey Media Group, Inc. v. Ashcroft*, 205 F. Supp. 2d 288, 290 (D.N.J. 2002) (discussing memorandum closing hearings issued by Chief United States Immigration Judge Michael Creppy), *rev’d*, 308 F.3d 198, 218 (3d Cir. 2002).

108. 195 F. Supp. 2d 937 (E.D. Mich.), *aff’d*, 303 F.3d 681 (6th Cir. 2002).

109. 205 F. Supp. 2d 288 (D.N.J. 2002), *rev’d*, 308 F.3d 198 (3d Cir. 2002).

110. See *Detroit Free Press*, 195 F. Supp. 2d at 940; *North Jersey Media Group*, 205 F. Supp. 2d at 290. Plaintiffs relied on Supreme Court cases allowing press access to certain court hearings. See generally *Press-Enter. Co. v. Superior Court of Ca.*, 478 U.S. 1, 10 (1986) (holding that preliminary hearings are included in the First Amendment right of access); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580 (1980) (determining that “the right to attend criminal trials is implicit in the guarantees of the First Amendment”).

111. Brief for Appellants at 47, *Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002) (No. 02-1437) (internal quotation marks omitted); *North Jersey Media Group, Inc. v. Ashcroft*, 308 F. 3d 198, 218 (3d Cir. 2002).

112. See *North Jersey Media Group*, 308 F.3d at 218-19 (summarizing the Declaration of Dale L. Watson). The government relied on a similar affidavit in *Detroit Free Press*. See Declaration of Dale L. Watson, *Detroit Free Press v. Dep’t of Justice* at 4-5, 195 F. Supp. 2d 937 (E.D. Mich. 2002), No. 02-70339, available at <http://www.cnss.org/watsonaffidavit.pdf> (discussing the rationale underlying his belief that opening the detention hearings would

the *North Jersey Media Group* court, these arguments, though speculative, were credible and un rebutted. Moreover, the case involved national security, an area in which the court was loathe to second-guess the government, even with civil liberties at stake.¹¹³ In contrast, the *Detroit Free Press* court rejected the government's invocation of mosaic theory. Although the court acknowledged that "the risk of 'mosaic intelligence' may exist," it found that the government's belief that all detainees might potentially disclose information leading terrorists to impede government investigations was unsupported by evidence and speculative at best.¹¹⁴ The Court further feared that the mosaic theory argument was limitless, as the mere assertion of "national security" as a rationale allowed the government to "operate in virtual secrecy" by "clos[ing] any public hearing completely and categorically, including criminal proceedings."¹¹⁵

The Bush Administration also relied on mosaic theory to defend the indefinite detention of non-citizens rounded up in the aftermath of the 9/11 attacks. In Fall 2001 hearings seeking release of detainees—most of whom were later found to have no connection to terrorism—the FBI argued for their continued detention because "the business of counterterrorism intelligence gathering . . . is akin to the construction of a mosaic" which requires the "gathering and processing [of] thousands of bits and pieces of information that may seem innocuous at first glance."¹¹⁶ Essentially, the FBI argued that continued detention was necessary because the detainees might later be found to have information relevant to a terrorist investigation.¹¹⁷ The government made a similar mosaic theory argument in response to a more recent class action lawsuit challenging the indefinite detentions.¹¹⁸

compromise the investigation). In *North Jersey Media Group*, the government also provided an affidavit from James S. Reynolds, Chief of the Terrorism and Violent Crimes Section of the Justice Department's Criminal Division, making essentially the same statements. See *Detroit Free Press*, 303 F.3d at 705-06.

113. See *North Jersey Media Group*, 308 F.3d at 219 (refusing to "conduct a judicial inquiry . . . as national security is an area where courts have traditionally extended great deference to Executive expertise").

114. See *Detroit Free Press*, 303 F.3d at 707, 709.

115. *Id.* at 709-10.

116. See Amy Goldstein, *A Deliberate Strategy of Disruption; Massive, Secretive Detention Effort Aimed Mainly at Preventing More Terror*, WASH. POST, Nov. 4, 2001, at A01 (quoting affidavit of FBI official).

117. See Nancy V. Baker, *National Security Versus Civil Liberties*, 33 PRESIDENTIAL STUD. Q. 547, 554 (2003) (discussing an FBI affidavit arguing that even those with "minor violations" should be detained).

118. See Memorandum of Law in Support of Partial Motion to Dismiss on Behalf of the United States and Motion to Dismiss on Behalf of Defendants John Ashcroft, Robert Mueller, James W. Ziglar, Dennis Hasty, and Michael Zink, *Turkmen v. Ashcroft*, No. 02 CV 2307 (JG) (E.D.N.Y. Nov. 30, 2004), available at www.ccr-ny.org/v2/legal/september_11th/docs/Defs'_Brief_%20Omnibus_Motion_to_Dismiss1130041.pdf. The defendants' motion did not explicitly mention mosaic theory. See *id.* Rather, it argued for court deference to the government's detention of plaintiffs because national security was

2. Mosaic Theory Outside of the Courts

a. Sensitive but Unclassified Information

The Bush Administration also has revived Reagan-era initiatives based on mosaic theory, although in a somewhat different format. In a program reminiscent of NSDD 145, the Bush Administration encouraged administrative agencies to safeguard and withhold sensitive information, defined as government information “regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our Nation and the safety of our people.”¹¹⁹ The justification for such a move was partially grounded in mosaic theory, as Bush Administration officials feared that terrorists were culling public sources of information to piece together government activity.¹²⁰

These actions concern observers. No overarching legal framework currently governs “sensitive but unclassified” information (which consists of up to fifty-six separate designations and definitions by various agencies),¹²¹ and agency officials must find that it falls within existing FOIA exemptions to withhold such information. Even prior to the Bush Administration’s aggressive campaign, there was fear that this chaotic scheme, with so little oversight, would result in excessive secrecy by resulting in confusion and over-classification of material.¹²² Some critics

involved and because the “investigations were exceedingly complex, requiring a nationwide effort to obtain information regarding terrorist organizations, methodology, and personnel.” *Id.* at 41. To support its claim, the government cited to the portions of *CIA v. Sims* and *Halkin v. Helms* discussing mosaic theory. *Id.* The federal court recently dismissed the plaintiffs’ claims regarding the illegality of the indefinite detention, but it made no mention of mosaic theory. See Memorandum and Order, *Turkmen v. Ashcroft*, No. 02 CV 2307 (JG), at 69-77 (E.D.N.Y. June 14, 2006), available at www.nyed.uscourts.gov/pub/rulings/cv/2002/02cv2307mo-f.pdf (stating that the government’s subjective intention to keep the suspects in jail is immaterial since the “entire detention was authorized by the post-removal period detention statute”).

119. See Memorandum from Andrew H. Card, Jr., Assistant to the President and White House Chief of Staff, to the Heads of Executive Departments and Agencies (Mar. 19, 2002), <http://www.fas.org/sgp/bush/wh031902.html>; see also Memorandum from Laura L.S. Kimberly, Acting Director, Information Security Oversight Office to Departments and Agencies (Mar. 19, 2002), <http://www.fas.org/sgp/bush/wh031902.html> (providing guidelines on how to “safeguard information,” including “sensitive but unclassified information,” by using measures such as “giving full and careful consideration to all applicable FOIA exemptions”).

120. See, e.g., Donald F. Rumsfeld, Sec. of Def., Cable to “RUHH Subscribers” (Jan. 14, 2003), <http://www.fas.org/sgp/news/2003/01/dodweb.html> (describing an Al Qaeda manual which detailed tactics of culling public sources and websites for Department of Defense (DOD) information and cautioning personnel to “think[] about what may be helpful to an adversary” when deciding what unclassified information to post on websites).

121. See National Security Archive, *Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government’s Policies on Sensitive Unclassified Information* at 9 (Mar. 2006), www.nsarchive.org (reporting that twenty-four of the thirty-seven surveyed agencies follow their own “internally-generated policies”); Wells, *supra* note 51, at 1210-11 (discussing the variety of definitions of “sensitive but unclassified” used by agencies).

122. REPORT OF THE COMM’N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S.

note that “a great deal of non-sensitive information is being withheld [since the Bush Administration’s campaign] that should be or previously would have been released under FOIA.”¹²³ Others note that the existing haphazard framework inhibits sharing of information among government agencies that is necessary to protect national security,¹²⁴ a problem the Bush Administration’s campaign likely exacerbates.

In early 2006, the Department of Defense (DOD) also proposed legislation exempting from disclosure under FOIA “information in the possession of DOD concerning weapons of mass destruction.”¹²⁵ Specifically, such information would have included that which assisted in (1) “develop[ment], produc[tion], or us[e] of weapons of mass destruction,” (2) “evading the detection or monitoring of the development, production, use, or presence of [such] weapons,” or (3) “disclos[ing] a vulnerability to the effects of [such] weapon[s].”¹²⁶ The proposed legislation assumed that many entities, both inside and outside the government, “operate[d] research programs, chemical plants, nuclear power stations, medical treatment facilities, and other activities that generate[d] information that easily could assist a terrorist or other adversary to make or use a weapon of mass destruction.”¹²⁷ The DOD recognized that agencies often could withhold such information under FOIA Exemptions 1, 2, or 4, but nevertheless

DOC. NO. 105-2, at 29 (1997) (commenting that many officials reported classifying information to shelter it).

123. National Security Archive, *supra* note 121, at 26. See JOHN BAKER ET AL., MAPPING THE RISKS: ASSESSING THE HOMELAND SECURITY IMPLICATIONS OF PUBLICLY AVAILABLE GEOSPATIAL INFORMATION 123 (2004) (arguing that information was needlessly withheld from public view after the Card directive because “very few of the publicly accessible . . . sources appear useful to meeting a potential attacker’s information needs”).

124. See GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, at 6 (2006), available at <http://www.gao.gov/new.items/d06385> (suggesting that the lack of oversight leads to a greater chance that the sharing of material will be unnecessarily restricted).

125. See H.R. 5122, 109th Cong., §§ 923(a), (d)(2) (2006) (version introduced in the House, Apr. 6, 2006) (proposing that such information be exempt from FOIA until its “sensitivity . . . can be reasonably confirmed”). According to the House Report, the DOD originally proposed this provision, and the House agreed to incorporate it. See COMM. ON ARMED SERV., NAT’L DEF. AUTHORIZATION ACT FOR FISCAL YEAR 2007, H.R. REP. NO. 109-452 at 477-79 (2006) (printing the Department of Defense’s letters to the House requesting the bill’s enactment).

126. H.R. 5122 § 923(d)(2).

127. See Federation of American Scientists, “Proposed DOD FOIA Exemption for Unclassified WMD Information,” available at <http://www.fas.org/sgp/news/2006/04/dodfoia.html> (last visited Oct. 7, 2006) (providing a section by section analysis of the DOD’s proposed exemption to FOIA).

argued for a new exemption in cases where existing exemptions did not apply.¹²⁸ In other words, the proposed legislation created an exemption for sensitive but unclassified information.

Although the proposed law represented an improvement over the Reagan-era's vague and amorphous definition of sensitive but unclassified information, problems still existed. While the bill pertained only to "weapons of mass destruction," it allowed for the restriction of information that was only tangentially related to such weapons, but which had substantial scientific or public health implications. Similarly, while the bill provided that material could be withheld only as long as it was sensitive,¹²⁹ it provided no guidelines for making such determinations, thus granting a great deal of discretion to agency officials. Finally, the bill preempted all state and local disclosure laws,¹³⁰ an action which failed to recognize that "[p]ublic health officials and agencies in state and local governments and outside government often have different, sometimes competing, public health priorities."¹³¹

Later iterations of the proposed legislation deleted this provision.¹³² Nevertheless, the DOD's attempt to insert a limited sensitive but classified provision into FOIA reveals the continuing problems that arise with attempts to withhold information using such an amorphous concept.

b. USA PATRIOT Act

At the behest of the Bush Administration, Congress also enacted legislation with roots in the FBI's Library Awareness Program. Section 505 of the USA PATRIOT Act provided the FBI with greater leeway to use national security letters to gather library user information, among other things.¹³³ Prior to the USA PATRIOT Act, the FBI could issue NSLs to

128. See *id.* (reporting that Section 923 "would exempt from disclosure under the Freedom of Information Act (FOIA) certain information . . . which does not also meet the threshold for national security classification").

129. See H.R. 5122 § 923(a).

130. *Id.* § 923(c) (prohibiting state and local authorities from enacting laws dealing with information subject to the section).

131. SUNSHINE IN GOVERNMENT INITIATIVE, DEFENSE SPENDING PROPOSAL WOULD EXPAND SECRECY 2 (Apr. 24, 2006), http://www.sunshineingovernment.org/Defense_FOIA.pdf.

132. See H.R. 5122, 109th Cong. (2006) (version engrossed in the House (May 16, 2006)). A newer version of the bill instead contains a provision providing that "sensitive but unclassified homeland security information in the possession of the Department of the Defense" that is shared with state and local personnel in relation to terrorist activities as required under the Homeland Security Act "shall not be subject to disclosure" under FOIA simply because it was shared with other agencies. See John Warner National Defense Authorization Act for Fiscal Year 2007, H.R. 5122, 109th Cong. § 1405 (2006) (engrossed amendment as agreed by the Senate), available at <http://thomas.loc.gov/cgi-bin/query/C?c109:/temp/~c109Eoq4bv> (discussing provisions recently adopted by Congress).

133. The FBI has the authority to issue compulsory NSLs in situations defined by various statutes that do not require judicial or prosecutorial oversight. See Charles Doyle, *Administrative Subpoenas and National Security Letters in Criminal and Foreign*

obtain various telephone and electronic transactions records (for Internet usage), financial records, and other consumer credit records.¹³⁴ Section 505 of the USA PATRIOT Act expanded the FBI's power to issue NSLs, allowing access to records after the FBI certified that it sought information relevant to a "foreign counterintelligence investigation."¹³⁵ The previous standard required "specific and articulable facts giving reason to believe that the customer or entity whose records [were] sought [was] a foreign power or an agent of a foreign power."¹³⁶ The breadth of the government's power under Section 505 to issue NSLs based on generalized suspicion, combined with a provision prohibiting recipients from disclosing receipt of an NSL,¹³⁷ essentially allowed the FBI to access library records of individuals not suspected of terrorism in much the same way that the Library Awareness Program operated.¹³⁸

The government, however, justified the statute as a necessary counterintelligence measure.¹³⁹ It also specifically justified the nondisclosure portions of the statute with reference to mosaic theory. According to government officials, "disclosure of the NSL recipient's identity may . . . permit the subject of the NSL, or those involved [with] the NSL, to deduce that the government is aware of [their] identity, leading

Intelligence Investigations: Background and Proposed Adjustments at 22–23 (Apr. 15, 2005), www.fas.org/sgp/crs/natsec/RL32880.pdf (listing requirements FBI agents must meet before they may issue an NSL).

134. See 18 U.S.C. § 2709 (2000) (allowing FBI agents to gain subscriber information from an "electronic communications service provider" only if there are "specific and articulable facts . . . that the person . . . is a foreign power or agent of a foreign power"); 12 U.S.C. § 3414(a) (2000) (applying the same standard to financial institutions); 15 U.S.C. § 1681u(c) (2000) (requiring consumer reporting agencies to provide such information upon the same standard).

135. See, e.g., USA PATRIOT Act § 505(b), Pub. L. No. 107-56, 115 Stat. 272, 365–66 (2001) (amending 12 U.S.C. § 3414(a)(5)(A) (2000)) (amending the Financial Privacy Act of 1978 to allow the FBI greater access to records).

136. Intelligence Authorization Act for Fiscal Year 1987, § 404, Pub. L. No. 99-569, 100 Stat. 3190, 3197 (amending 12 U.S.C. § 3414(a)(5)).

137. See, e.g., 18 U.S.C. § 2709(c) (2000) (implementing a nondisclosure provision). The Act did not contain an obvious provision providing for judicial review of NSLs.

138. Critics of the USA PATRIOT Act amendments noted that the amendments could allow the FBI to access information regarding citizens' reading and Internet habits with very little prosecutorial or judicial oversight. See, e.g., AMERICAN CIVIL LIBERTIES UNION, UNPATRIOTIC ACTS: THE FBI'S POWER TO RIFLE THROUGH YOUR RECORDS AND PERSONAL BELONGINGS WITHOUT TELLING YOU 13 (2003), <http://www.aclu.org/safefree/resources/16813pub20030730.html> (warning that the FBI has used NSLs more freely since the 2001 law); Susan Nevelow Mart, *Protecting the Lady from Toledo: Post-USA PATRIOT Act Electronic Surveillance at the Library*, 96 LAW LIBR. J. 449, 468 (2004) (suggesting that "overcollection of information" frequently occurs); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1356 (2004) (discussing the expansion of the government's power under the § 505 standard).

139. See Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 41-54, 69 (2004) (discussing the legitimate counterintelligence function of NSLs).

them to flee or go deeper under cover.”¹⁴⁰ Furthermore, “while that piece of information may appear innocuous by itself, it could still be significant to a terrorist organization when combined with other information available to it.”¹⁴¹

Two district courts have rejected the government’s assertion of mosaic theory to support the non-disclosure provision, finding the theory either inapplicable to the First Amendment challenge asserted¹⁴² or conclusory and unsupported by actual facts related to the particular claim involved.¹⁴³ As one court succinctly put it, mosaic theory might be relevant when the government

[a]sserts that secrecy is necessary for national security purposes in a *particular situation* involving *particular persons* at a *particular time*. Here, however, the Government cites no authority supporting the open-ended proposition that it may universally apply these general principles to impose perpetual secrecy upon an entire category of future cases whose details are unknown and whose particular twists and turns may not justify, for all time and all places, demanding unremitting concealment and imposing a disproportionate burden on free speech.¹⁴⁴

As a result of the issues raised in these decisions and the public outcry over the NSL provisions, Congress recently amended them. The new provision allows recipients to petition for judicial review modifying or setting aside the NSL, requires FBI certification of a danger to national security prior to imposing a nondisclosure requirement, and makes clear that NSLs do not apply to libraries when they operate in their traditional role.¹⁴⁵ Although the 2006 amendments provide some safeguards for recipients of NSLs and library/Internet users, critics note that problems remain. Perhaps most significantly, some critics note that the judicial review and non-disclosure provisions are effectively meaningless because

140. See *Doe v. Gonzales*, 386 F. Supp. 2d 66, 76 (D. Conn. 2005) (citing the government’s reasons for wanting to keep Doe’s identity confidential).

141. *Id.* at 77.

142. See *id.* at 77-78. See also *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 524-25 (S.D.N.Y. 2004) (holding that the Government failed to cite relevant authority for its secrecy claim).

143. See *id.* at 78.

144. *Doe v. Ashcroft*, 334 F. Supp. 2d at 524-25.

145. For a thorough discussion of these amendments, see Brian T. Yeh & Charles Doyle, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis* at 10-16 (Mar. 24, 2006), www.fas.org/sgp/crs/intel/RL33332.pdf (discussing the recent restrictions placed on NSLs).

courts must treat as conclusive the government's certification that disclosure may endanger national security.¹⁴⁶ Proponents of the law defended this presumption using mosaic theory.¹⁴⁷

III. IMPLICATIONS AND SOLUTIONS

The instances of non-FOIA invocation of mosaic theory reflect the depths to which the theory has infiltrated the government's mindset. Mosaic theory is no longer limited to government attempts to block FOIA or discovery requests in the course of litigation.¹⁴⁸ Now, the government invokes mosaic theory to rationalize closing deportation hearings, indefinitely detaining non-citizens, restricting dissemination of non-classified information, and secretly searching certain kinds of records, including library and Internet records. In other words, the government uses mosaic theory to justify the very bases of certain programs or actions. Given the constitutional liberties at stake with such actions, this use of the theory represents a significant step beyond refusal to provide information in response to FOIA requests. No good can come from allowing the government to assert mosaic theory unchallenged.

As noted above, recent invocations of the theory block questions about these programs by arguing that revelation of information enables enemies to hurt the United States and by casting those who question the government as outsiders unable to assess the risk. Government officials support their claims with little more than conclusory statements that terrorists, who are smarter than judges or the public, will piece together the information, and

146. See *id.* at 14. In addition, although NSLs no longer apply to libraries in their traditional role, a library providing Internet services beyond a certain undefined level is still subject to NSL authority. *Id.* at 15. Moreover, the FBI also can obtain library records through Section 215 of the USA PATRIOT Act, which allows the government to apply for a court order accessing "any tangible things (including books, records, papers, documents, and other items)." See USA PATRIOT Act § 215, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (amending 50 U.S.C. § 1861(2000)). As with NSLs, observers criticize the breadth of the government's power to obtain secretly such orders without meaningful oversight. As with the NSL provisions, Congress curtailed some of the government's authority to access such records in early 2006. To compare the law before and after the 2006 amendments, see Mart, *supra* note 138, at 461-62 and Yeh & Doyle, *supra* note 145, at 4-10.

147. See 152 CONG. REC. S1395 (Feb. 16, 2006) (statement of Sen. Kyl) (expressing concern that the absence of the rule would allow each judge to make a separate determination regarding the harmful effects of the information to national security).

148. I do not mean to diminish FOIA's importance. Absent a judicially recognized constitutional right of access to government information, FOIA is the primary source of information about government operations. In this sense, FOIA is critical to democratic accountability. See Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 144-45 (2006) (suggesting that FOIA's purpose is to "make democratic participation and citizen oversight a reality"). My point is simply that since FOIA litigation involves only requests for information, these important democratic issues are less obviously at the forefront of litigation than in the non-FOIA cases.

use it to impede terrorism investigations.¹⁴⁹ Officials make no genuine attempt to identify the danger, or even possible alternative dangers, posed by the information.¹⁵⁰ Rather, the government's argument suggests in some sort of shadowy way that the very existence of the information poses the danger; thus, it cannot fall into the wrong, or any, hands. As in the FOIA context, invocation of mosaic theory is a non-response designed solely to obtain a result—secrecy.

Unfortunately, the government's current use of mosaic theory effectively reads constitutional liberties out of the balance. Government officials apparently have determined that there is no acceptable risk of danger from disclosure of information and that infringement of constitutional liberties is an unavoidable side-effect of attaining that level of risk (although they rarely say this out loud). This reasoning shows either a fundamental misunderstanding of risk assessment (that is, the far-fetched belief that suppressing information can reduce the risk of terrorism to zero),¹⁵¹ an underestimation of the value of constitutional liberties in our governmental hierarchy, or a pretext to hide governmental misbehavior or accretion of power.¹⁵²

Not surprisingly, courts hearing constitutional challenges to programs in which the government has asserted mosaic theory have most often questioned the government's arguments.¹⁵³ Faced with balancing important liberties against the government's national security rationale, those courts have rejected broad and unsupported assertions of mosaic theory. Unfortunately, not all courts are so willing to question the government. Instead, some defer to broad assertions of mosaic theory

149. See *supra* notes 93-118, 140-41 (discussing the government's frequent attempts to invoke the mosaic theory without providing any compelling evidence).

150. See Ristroph & Jaffer, *supra* note 9, at 7 (“[T]he government need not explain even the potential danger; it can simply assert that information might be ‘significant’ in some as-yet-undetermined way.”).

151. At least two issues arise here. First, can we reduce such risk to nothing? Second, should this be our goal, or would it be counterproductive (for example, by interfering with intelligence information sharing or intruding too much upon civil liberties)? See, e.g., MITRE Corp.—JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance 25-26* (2004), <http://www.fas.org/irp/agency/dod/jason/classpol.pdf> (reporting an independent scientific advisory group's findings discussing the need to switch from a paradigm minimizing risk to one maximizing information flow subject to acceptable risk levels).

152. See Ristroph & Jaffer, *supra* note 9, at 7 (suggesting that mosaic theory makes the government unaccountable because citizens cannot complain about abuses of which they are unaware).

153. See, e.g., *Doe v. Gonzales*, 386 F. Supp. 2d 66, 78 (D. Conn. 2005) (deciding that the government's assertion of the mosaic theory was insufficient to support gag order); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 524 (S.D.N.Y. 2004) (determining that the government provided no evidence to sustain its “open-ended proposition”); *Detroit Free Press, Inc. v. Ashcroft*, 195 F. Supp. 2d 937, 947 (E.D. Mich. 2002) (holding that the government failed to meet even the most deferential standard to justify closing the hearings), *aff'd*, 303 F.3d 681 (6th Cir. 2002).

regardless of the constitutional liberties at stake.¹⁵⁴ With increasing governmental assertion of the state secrets privilege—an area in which courts routinely defer¹⁵⁵—one can expect that some courts will continue to defer, even in cases that involve constitutional rights.¹⁵⁶ Moreover, courts resolving FOIA litigation almost always defer to mosaic theory arguments. Government actors appear unlikely to change their ways in the near future based upon the actions of a few courts.

What are we to do about this? The answer begins with the FOIA cases where mosaic theory originally took root. If we can convince judges to exercise actual review over cases like *Sims*, forcing government officials to justify their decisions with evidence or, at the very least, specifically tailored arguments, about the need for secrecy, perhaps other courts will take up the cause. Eventually, government actors may alter their behavior as well. Imagine, for example, how things would have progressed if the Supreme Court had decided *Sims* in a manner consistent with the lower court opinions.

The district court in *Sims* was hardly hostile to the CIA. Rather, it provided the CIA with numerous opportunities to offer evidence supporting its Exemption 3 claim.¹⁵⁷ The district court sought to obtain a specific explanation from the CIA so that the agency could not insulate its actions from review by hiding behind a porous definition of “intelligence source.”¹⁵⁸ Had the agency eventually been forced to provide such information or abandon its claim of exemption it, and others watching the case, would have realized the kind of justifications required to support a national security withholding. Instead, the Supreme Court accepted the CIA’s invocation of mosaic theory and the notion that courts are not in a position to see the “bigger picture” without asking any further questions. The government’s assertion of mosaic theory brought to a halt what had been legitimate and thoughtful questions by the lower courts.¹⁵⁹

154. See *North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198, 215-16 (3d Cir. 2002); see also *supra* notes 107-15.

155. But see *Heptig v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (refusing to dismiss a lawsuit alleging that an NSA surveillance scheme violated First and Fourth Amendment rights based upon the government’s assertion of state secrets privilege).

156. See *supra* notes 102-06 and accompanying text.

157. See *supra* note 27 and accompanying text.

158. See *supra* note 29 and accompanying text.

159. The lower courts never discussed mosaic theory. The theory appeared in the government’s Supreme Court brief and then in the Supreme Court opinion. See Brief for Respondents at 6-7, *Sims v. CIA*, 471 U.S. 159 (1985) (No. 83-1249) (suggesting that the Director of Central Intelligence is authorized to do more than protect information that is already easily distinguishable as sensitive, and must sometimes “withhold superficially innocuous information”).

As the lower court decisions in *Sims* reveal, courts need not treat mosaic theory with such deference. One can allow assertion of the theory without squelching questions. To do so, however, one must focus on a concrete danger and its relationship to the information sought. Thus, courts should require agency assertions of mosaic theory to specifically identify the threat to national security, explain the potential causal link between the innocuous information released and the harm to national security, and explain how information already in the public domain, if relevant, does not undercut the agency's assertion of mosaic theory.¹⁶⁰

Government officials must do more than blandly state, as they do in much recent litigation involving national security, that release of information will allow terrorists to impede terrorism investigations. In a world in which terrorist investigations have occurred (and likely will continue to occur for decades), an agency could endlessly use this excuse. Instead, government officials must identify how the specific information likely will play a role in impeding particular investigations by focusing on potential, specific threats to those investigations, discussing the causal links between the information and those threats, and determining the basis for making particular inferences from the information in their possession.¹⁶¹ Similarly, in many instances, information sought via FOIA requests is available or partially available through other sources, as in *Sims* and several of the post 9/11 cases. The courts' reasoning that agencies may nevertheless refuse to disclose such information for intelligence purposes,¹⁶² while perhaps sound in theory, fails to acknowledge that, in a particular instance, information already in the public domain may substantially undercut the agency's rationale regarding withholding. At the very least, a court should require an explanation before it agrees to allow withholding.

Recently, in *Heptig v. AT&T*,¹⁶³ the court took a slightly different approach to determine whether information already widely reported by the media nevertheless qualified as a state secret for litigation purposes.

160. I use the general term "national security" here for ease of discussion. One would need to alter the questions depending upon whether the exemption involved classified information or a specific withholding statute, such as the National Security Act's protection of "intelligence sources and methods." There also may be additional questions courts could ask. See sources cited *infra* note 167. These appear to be the three most important assertions, however.

161. Alice Ristroph and Jameel Jaffer make a similar argument regarding the need for specificity and additional justifications although they argue that such specificity would "mean the end of the mosaic argument." Ristroph & Jaffer, *supra* note 9, at 7-8. To the extent that they call for the abandonment of mosaic arguments altogether, I disagree that such a move is likely or necessary. Obviously, however, courts and government officials must abandon the current iteration of mosaic theory.

162. See *supra* note 40 and accompanying text.

163. 439 F. Supp. 2d 974 (N.D. Cal. 2006).

According to the court, a statement in the public domain may still remain secret if it “possesses substantial indicia of reliability [for instance, coming from a reliable source such as the government] and whose verification or substantiation possesses the potential to endanger national security.”¹⁶⁴ Questions such as this may provide a reasonable way to distinguish between legitimate and illegitimate government claims.

The above requirements are not unduly onerous. Intelligence agencies are thoroughly familiar with the application of mosaic theory—not simply the assertion of it in litigation. Thus, such agencies understand the need to be concrete when constructing mosaics or guarding against their construction. In fact, federal agencies practicing operational security (OPSEC), an applied version of mosaic theory, explicitly recognize the need for specificity in practicing counterintelligence—i.e., intelligence activities designed to identify and counter threats to security. Accordingly, such agencies list as part of their practices the need to (1) identify “core secrets”—those “few nuggets of information” critical to the organization’s mission; (2) identify specific adversaries, their objectives, and their capabilities; (3) analyze the organization’s vulnerabilities; and (4) assess particular risks by matching an organization’s vulnerabilities to particular threats.¹⁶⁵ Without specific identification of such issues, officials understand both the uselessness of counterintelligence measures, because they have nothing identifiable at which to aim, and that failure to adequately identify risks wastes resources.¹⁶⁶

Courts taking the above approach to mosaic theory merely take a page from the counterintelligence manuals of the agencies.¹⁶⁷ Requiring

164. *Id.* at 990.

165. DefendAmerica, An Operational Security (OPSEC) Primer, <http://www.defendamerica.mil/articles/a021202b.html> (last visited Aug. 16, 2006) (discussing that the OPSEC process must determine information that would harm an organization’s ability to operate).

166. *Id.* (“The decision of whether to implement countermeasures must be based on cost/benefit analysis and an evaluation of the overall program objectives. . . . If you don’t know what to protect, how do you know you are protecting it? The ‘what’ is the critical and sensitive . . . information that adversaries require to meet their objectives.”).

167. Given courts’ history of deference in FOIA cases involving national security—especially mosaic theory cases—one rightfully wonders whether courts will ever exercise more rigorous review. This may be an area in which Congress should involve itself, much as it did after *EPA v. Mink*, to send some sort of signal to courts that the deference associated with mosaic theory is not appropriate. Many avenues are available, including (1) amending FOIA to set forth a judicial standard requiring consideration of the factors discussed above (leaving some details to the courts depending on particular issues arising in litigation), (2) amending the statute to include consideration of the public interest in disclosure, along with the national security interest so courts have an incentive to consider both sides of the liberty/security issue, (3) amending FOIA to require *in camera* inspection and use of special masters to aid with sensitive, difficult and time-consuming document review, and (4) amending FOIA to set up special courts or administrative bodies to deal with FOIA issues initially, while still allowing resort to Article III courts. See Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation Over National Security Information*

agencies that want to withhold information to identify potential harm and draw causal links to the release of apparently innocuous information is consistent with how agencies perform OPSEC (if performed well). Accordingly, agencies should already have done much of this work; if not, or if they refuse to justify their invocation of mosaic theory, it suggests that an agency uses the theory for other purposes or that officials lazily invoke it as a talisman. A court faced with such a situation is entitled to request more detailed support or, if it finds that avenue pointless, order disclosure.

The advantage of more rigorous judicial review goes beyond the immediate effects of FOIA litigation. A more rigorous requirement forcing agencies to justify their use of mosaic theory ideally will avoid much litigation by resulting in better decisionmaking from the outset.¹⁶⁸ More rigorous review of mosaic theory in the FOIA context also may affect the government's current assertions of mosaic theory beyond FOIA. Once *Sims* unquestioningly accepted mosaic theory, it became a powerful weapon for the government in any national security context. If courts clarified, however, that mosaic theory required justification and causal connections, it would alter the entire backdrop for mosaic theory. Government officials could no longer wield this blunt weapon to justify such things as closure of immigration hearings, withholding non-classified

Under the Freedom of Information Act, 37 VILL. L. REV. 67, 93-102, 105-11 (1992) (discussing numerous ways to improve the litigation process for FOIA); Fuchs, *supra* note 148, at 173-75 (suggesting that *in camera* review will result in greater disclosure); Pozen, *supra* note 9, at 677-78 (proposing the use of special masters or assistants to help with fact-finding and evaluating the credibility of the government's claims); Wells, *supra* note 51, at 1218 n.118 (suggesting possible use of a statutory balancing test favoring disclosure of even properly classified information if the public interest in disclosure outweighs national security needs). These are merely suggestions, all of which need greater exploration—each has advantages and disadvantages. While occasional courts have undertaken some of these tasks, *see, e.g., Heptig*, 439 F. Supp. 2d at 1011 (issuing order to show cause regarding the possible appointment of a special master for assistance in assessing classified evidence claims), Congress is the most logical body to undertake such an exploration. The critical point is that its action should compliment the above suggestions, persuading courts that complete deference is inappropriate. Of course, Congress also could consider much broader issues, such as whether the exemptions themselves should be reconsidered or amended. *See, e.g., Wells, supra* note 51, at 1217-20. But that is beyond the scope of this Article.

168. This argument assumes, consistent with psychological research on accountability, that more rigorous judicial review could improve agency decisionmaking. *See* Jennifer S. Lerner & Philip E. Tetlock, *Accounting for the Effects of Accountability*, 125 PSYCHOL. BULL. 255, 255 (1999) (theorizing that accountability encourages people to give "compelling justifications" so that they may experience rewards). Such an assumption needs more detailed exploration than this Article allows, but current use of mosaic theory clearly does not make officials accountable in any sense of the word. Arguments exist that judicial review can improve government decisionmaking in certain contexts. *See* Mark Seidenfeld, *Cognitive Loafing, Social Conformity, and Judicial Review of Agency Rulemaking*, 87 CORNELL L. REV. 486, 508-09 (2002) (suggesting that "judicial review provides accountability . . . [when] courts examine the arguments pertaining to the validity and care of the agency reasoning"); Christina E. Wells, *Questioning Deference*, 69 MO. L. REV. 903, 939-49 (2004) (suggesting that judicial review might serve as a method of accountability when civil liberties are at stake).

information, or secret records searches. Instead, precedents would exist with far more specific requirements applicable only in specific circumstances. It would take determined interpretive efforts for government officials to find such specific requirements supportive of their broader initiatives.

To be sure, government officials might make such efforts; with sufficient motivation, one can justify almost anything.¹⁶⁹ However, officials seem far more likely to continue believing that “a little knowledge is a dangerous thing” under the existing regime of mosaic theory. Government actors might alter their attitudes if courts required greater justification of their actions. In an analogous situation involving free speech rights, evolution in the Court’s decisions appears to have changed the attitude of government officials. During World War I, courts indicted and convicted thousands of people because their speech had a “tendency” to cause interference with the war effort.¹⁷⁰ The Supreme Court originally reviewed such convictions using a version of the “clear and present danger” test that, like the current version of mosaic theory, deferred to the government’s allegations of harm.¹⁷¹ Over time, however, the Court realized that its test provided no protection against government overreaching and, as a result, imposed stringent intent and causal requirements.¹⁷² As the Court’s cases have evolved, so has the government’s attitude. Although the Court is most likely to defer to government officials’ suppression of speech during national security crises, government officials have not attempted to censor criticism of the government under the guise of national security in recent years, at least not as they attempted to do in 1917 or the Cold War.¹⁷³ One

169. See, e.g., RICHARD NISBETT & LEE ROSS, *HUMAN INFERENCE: STRATEGIES AND SHORTCOMINGS OF SOCIAL JUDGMENT* 169 (1980) (discussing the phenomenon of motivated reasoning, which occurs when individuals hold on to their beliefs even when presented with clear evidence to the contrary).

170. See *Shaffer v. United States*, 255 F. 886, 887 (9th Cir. 1919) (finding that statements violated the Espionage Act if their “natural and probable tendency and effect” was “such as are calculated to produce the result condemned by the statute”); see also *Frohwerk v. United States*, 249 U.S. 204, 209 (1919) (upholding a conviction for espionage because speech was a “little breath [that was] enough to kindle a flame”). For a discussion of the kinds of innocuous expression that resulted in criminal punishment during World War I, see Christina E. Wells, *Discussing the First Amendment*, 101 MICH. L. REV. 1566, 1582-84 (2003).

171. See *Schenck v. United States*, 249 U.S. 47, 52 (1919) (“The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent.”).

172. See, e.g., *Brandenburg v. Ohio*, 395 U.S. 444, 447-48 (1969) (holding that to convict a person of advocating illegal violence, the government must show that the expression is directed to and likely to incite or produce “imminent lawless action”); *Bridges v. California*, 314 U.S. 252, 263 (1941) (holding that “the substantive evil must be extremely serious and the degree of imminence extremely high before utterances can be punished”).

173. See, e.g., Geoffrey R. Stone, *War Fever*, 69 MO. L. REV. 1131, 1153 (2004) (“[T]he

can conclude that court decisions, in addition to resolving disputes, send broader signals to government actors who then internalize them. Ultimately, that internalized standard may spread to areas outside the immediate jurisprudence as well.

CONCLUSION

Whether one agrees with the ultimate outcome of *Sims*, the Court's unquestioning acceptance of mosaic theory had significant ramifications in and beyond the FOIA context. The decision reinforced a government attitude that views information as dangerous simply because of its possibilities. This effect, however, was not inherent in *Sims*. The Court could have accepted mosaic theory while requiring some justification for its assertion. Such an approach could have acknowledged the theory's potential validity without elevating it to the level of unquestioning deference. It might also have avoided expansion of that theory, and the concomitant emphasis on secrecy—apparently at all costs—well beyond the FOIA context.

efforts of government to suppress dissent have become both more subtle and less effective. . . . [W]e have indeed come a long way.”); Christina E. Wells, *Information Control In Times of Crisis: The Tools of Repression*, 30 OHIO N.U. L. REV. 451, 492-93 (2004) (noting that the current administration's censorship is still significantly more relaxed than that from World War I or the Cold War). Some of the government's decision to forego direct censorship simply may reflect an effort to find alternative, more subtle routes of suppression. Even this, however, suggests somewhat positive change as it shows that government officials have internalized court decisions and attempted to abide by the letter, if not the spirit, of them. For a thoughtful discussion, see Stone, *supra*, at 1152-53. We should, of course, remain vigilant regarding such alternate routes of suppression as any positive change that results from the evolution of doctrine easily erodes if more subtle routes of suppression go unchallenged.

* * *