

INFORMATION CONTROL: MAKING SECRETS AND KEEPING THEM SAFE

Alexander M. Taber*

The amount of classified information has increased to an astonishing point in recent years—having more than tripled during the Obama Administration alone. Concerns about overclassification are not new, but they are especially troubling given the amount of information now being classified and the amount of persons being prosecuted for leaking classified information. As it stands, the executive branch retains power to determine what information should be classified and who should be prosecuted for leaking classified information. In essence, the Executive holds both pen and sword and it may wield both in its full discretion. This Note addresses: how the current classification system came about and how it currently stands; the tools available to prosecute leaks; and possible solutions to the problems of overclassification and overprosecution.

TABLE OF CONTENTS

INTRODUCTION	582
I. OVERCLASSIFICATION	583
A. The Origins of “CLASSIFIED”	587
B. The Problems of Overclassification	594
II. PEN AND SWORD: THE EXECUTIVE’S ABILITY TO BOTH WRITE AND PROSECUTE THE LAW ON CLASSIFIED INFORMATION	596
A. The Espionage Acts	596
B. A Closer Look at Sections 793(d) and 793(e)	598
C. Current Prosecutions	602
III. RIGHTING THE SHIP	604
A. Legislative Solutions	605
B. Judicial Solutions	605

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2015. First, I would like to thank Professor Toni Massaro for her help and guidance with earlier drafts of a related paper. I would also like to thank the editorial staff at *Arizona Law Review* for their patience and diligence. Most importantly, I would like to thank my mother and father, Sue and Bill Taber, for their constant love and support. I would be but a shadow of who I am without them.

CONCLUSION	607
------------------	-----

INTRODUCTION

Gathering information about both foreign and domestic affairs is becoming harder and harder in the United States. More information is classified,¹ more people are being prosecuted for leaks,² and fewer people are speaking to reporters as a result.³ While part of the problem may be a result of choices made by the current Executive, it seems to primarily be a result of the system for classifying information, wherein discretion is the norm rather than the exception.

The current system of classification was created and has been maintained by executive order since the 1940s. But no statute controls the classification of documents, which leaves little to no oversight over what information becomes classified. Rather, executive agents classify information based largely on their subjective determinations about the potential harm that particular information might cause the nation.⁴ Additionally, there are few repercussions for wrongly classifying a document. Furthermore, each new president is not bound by prior presidential treatment of classified information—each may issue his own executive order as to classified information, and, in fact, many presidents have done so. The complete lack of uncertainty and subjectivity tends to result in a system of overclassification.

In addition to the classification system, the Espionage Acts provide the Executive with a means to enforce its orders by punishing individuals who disclose classified information without authorization. Under the Espionage Acts, an individual who willfully communicates any information “relating to the national defense” to someone “not entitled to receive it” commits a crime, regardless of that individual’s intent.⁵ There is no requirement that the leaker intend to disclose the information in order to harm the nation; all that is required is communication of some kind. Furthermore, the Acts do not define what information “relat[es] to national defense,” or who is “entitled to receive” such information, leaving the Executive with unfettered discretion to curtail whatever information it deems appropriate.

1. Since 2001, the number of classified decisions has increased nearly tenfold. INFO. SEC. OVERSIGHT OFFICE, 2013 REPORT TO THE PRESIDENT 6 (2013) [*hereinafter* ISOO REPORT], available at <http://www.archives.gov/isoo/reports/2013-annual-report.pdf>.

2. Since its enactment in 1917, the Espionage Act had only been used on three separate occasions against government officials prior to the Obama Administration. David Carr, *Blurred Line Between Espionage and Truth*, N.Y. TIMES, Feb. 26, 2012, at B1. To date, the Obama Administration has prosecuted eight federal employees for disclosing classified information to the media. Tim Bakken, *The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information: The Government’s Softening of the First Amendment*, 45 U. TOL. L. REV. 1, 7 (2013).

3. As one reporter stated, “There’s definitely a chilling effect. Government officials who might otherwise discuss sensitive topics will refer to these cases in rebuffing a request for background information.” Margaret Sullivan, Op-Ed., *The Danger of Suppressing the Leaks*, N.Y. TIMES, Mar. 9, 2013, at SR12.

4. See discussion *infra* Part II.

5. 18 U.S.C. §§ 793(d)–(e) (2012).

As it stands, the current classification system is entirely subject to executive discretion. Whatever information falls within the ambit of “national defense”, and any information that “relates” to it, is subject to executive control. The Executive can choose to let the information flow, or it can choose to plug it up, with little oversight from Congress or the courts.

The current classification system has grown out of control and needs to be reigned in. Several possible solutions are available. Some involve legislation, while others involve judicial construction. That said, regardless of which solution is chosen, some effort must be taken to curb the classification system or it will only continue to balloon.

This Note addresses the current classification system in three parts. Part I provides an overview of the classification system: how it came to be, its current legal foundations, and its ramifications. Part II examines the Espionage Act and the broad discretion it affords the Executive in prosecuting information it does not want disclosed. Finally, Part III considers possible solutions to the current classification regime.

I. OVERCLASSIFICATION

*Secrecy is a form of government regulation. Americans are familiar with the tendency to overregulate in other areas. What is different with secrecy is that the public cannot know the extent or the content of the regulation.*⁶

Concerns about rampant overclassification are not new.⁷ Nor is the problem unique to any one political party, president, or era.⁸ Over the past 50 years, critics from every generation have come forth to attack and decry the excesses of government secrecy.⁹ The 1956 Coolidge Committee concluded that “overclassification [had] reached serious proportions,”¹⁰ and attributed its overgrowth to the use of “general” criteria “for determining whether information should be classified at all” and the lack of criticism for “over-protecting” sensitive information.¹¹ The 1970 Defense Science Board Task Force on Secrecy concluded that the amount classified as scientific and technical information at the time “could profitably be decreased by as much as 90 percent by limiting the amount of

6. COMM’N ON PROTECTING & REDUCING GOV’T SECRECY, S. Doc. 105-2, REPORT OF THE COMM’N ON PROTECTING AND REDUCING GOV’T SECRECY xxi (1997) [hereinafter REPORT OF THE COMM’N], available at <http://www.gpo.gov/fdsys/pkg/GPO-CDOC-105sdoc2/pdf/GPO-CDOC-105sdoc2-3.pdf>.

7. Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 894.

8. *Id.* at 895.

9. Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL’Y REV. 399, 404 (2009).

10. DEF. DEP’T COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE BY THE COMMITTEE ON CLASSIFIED INFORMATION 6 (1956) [hereinafter REPORT TO THE SECRETARY], available at http://bkofsecrets.files.wordpress.com/2010/07/coolidge_committee.pdf.

11. *Id.* at 3

information classified and the duration of its classification.”¹² The 1997 Moynihan Commission stated that “[t]he classification system . . . is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters.”¹³

While successive generations have expressed concerns about the overclassification of information, the excessive classification of information that has occurred during the Bush and Obama Administrations is quite staggering. Since 2001, the number of classified decisions has increased nearly tenfold.¹⁴ In 2001 alone, the number of derivative classified decisions¹⁵ totaled around 8.39 million, whereas the annual figure for 2013 had increased to a startling 80.12 million.¹⁶ During the entirety of the Bush Administration, the number of annual classified decisions more than doubled, from 8.39 million decisions in 2001 to 23.22 million decisions in 2008.¹⁷ In 2009 alone, after President Obama took office, the number of classified decisions doubled again. The 2008 figure of 23.22 million decisions leapt to a staggering 54.65 million decisions, or an increase of 235%.¹⁸ In 2010, the number of decisions increased by 140% to 76.57 million decisions.¹⁹ The number of classification decisions again increased in 2011, totaling in at 92.06 million, a 120% increase.²⁰ Finally, in 2012, the number of classified decisions appears to have peaked at 95.18 million decisions.²¹ But even if the number of classification decisions seems to be in decline, the 2013 figure of 80.12 million decisions represents a 345% increase over little more than one term of President Obama’s presidency.

12. DEF. SCI. BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON SECRECY v (1970) [hereinafter DEFENSE SCIENCE BOARD TASK FORCE REPORT], *available at* <http://fas.org/sgp/othergov/dsbrep.pdf>.

13. REPORT OF THE COMM’N, *supra* note 6, at xxi.

14. ISOO REPORT, *supra* note 1.

15. Derivative classification involves “incorporating, paraphrasing, restating, or generating in new form information that is already classified.” *Id.* at 5. Original classification is a determination by an original classification authority (“OCA”) that “information owned by, produced by or for, or under the control of the U.S. Government requires protection because authorized disclosure of that information could reasonably be expected to cause damage to the national security.” *Id.* at 3. OCAs “classify information in the first instance” and must be able to “identify or describe the damage” that could result to national security if the information is not classified. *Id.* at 2. Derivative classifiers, on the other hand, may classify information in only two ways: “(1) through the use of a source document . . . ; or (2) through the use of a classification guide.” *Id.* at 5. “In theory, derivative classifiers lack policy discretion because they only classify items derivative of ‘that which has already been classified.’ In actuality, of course, determining what is derivative of already classified information—short of exact replicas of the latter—itself entails discretion.” Kitrosser, *supra* note 7, at 893.

16. ISOO REPORT, *supra* note 1.

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

It is unclear why the number of classified decisions has sharply increased. But, at a minimum, secrets logically breed more secrets.²² For example, executing a project in secret naturally requires a subset of secrets related to any activities in furtherance of that project's execution.²³ This unique nature of secrets arises primarily in the context of policy execution, including military plans.²⁴ To the extent that such execution is conducted in secret, new secrets necessarily accompany each layer of activity taken in furtherance of that execution.²⁵ Thus, if a President seeks to execute a policy in secret, any activity taken in furtherance of that policy must also remain secret, in addition to any communications about those activities. The initial secret snowballs into an avalanche of secrets advancing towards a particular goal.

Despite the nature of secrets, this does not explain the vast amount of classified activity in the United States. Part of the increase in classified decisions might be a result of agencies finding new ways to count new kinds of classified communications.²⁶ The 80 million "classification decisions" covered in a report produced by the Information Secrecy Oversight Office ("ISOO"), an agency created by executive order, "include[] classified emails, web pages, blogs, bulletin boards and instant-messaging systems that operate on classified computer networks."²⁷ Part of the increase might also be a result of increased agency information sharing.²⁸ If a secret document that was once distributed to only 20 people is now distributed to 200 people, those added distributions are counted as 180 extra derivative decisions.²⁹

Other explanations for the spike in classification decisions are less benign. Indiscriminately classifying documents is easier than giving each decision the necessary time and consideration.³⁰ Some officials do not have the time to make precise classification determinations a priority, while others fear the penalties they might incur for failing to make the proper classification and potentially disclosing sensitive information.³¹ "Because officials are rarely, if ever, penalized for improper classification [for classifying information at a higher level than necessary], there is

22. Kitrosser, *supra* note 7, at 887.

23. *Id.*

24. *Id.*

25. *Id.* at 888.

26. Shaun Waterman, *It's No Secret: There Are More Government Secrets Than Ever*, WASH. TIMES (May 29, 2012), <http://www.washingtontimes.com/news/2012/may/29/its-no-secret-there-are-more-government-secrets-th/?page=all>.

27. *Id.*

28. *Id.*

29. *Id.* (statement of William A. Cira, associate director in the Information Security Oversight Office) (internal quotation marks omitted).

30. Elizabeth Goitein & J. William Leonard, Op-Ed., *National Security and America's Unnecessary Secrets*, N.Y. TIMES (Nov. 7, 2011), <http://www.nytimes.com/2011/11/07/opinion/national-security-and-americas-unnecessary-secrets.html>.

31. Elizabeth Goitein, *Secrets and More (Government) Secrets*, HUFFINGTON POST (June 4, 2012, 5:12 AM), http://www.huffingtonpost.com/elizabeth-goitein/classified-documents_b_1568771.html.

no countervailing disincentive.”³² Some other explanations for the sharp increase include classifying information on the belief that it is easier to get things done when there are fewer people involved; hoarding information to increase an official’s sense of importance; or hiding involvement in government misconduct.³³

Another possible explanation for the dramatic increase in classified decisions from 2001 to the present relates to the dramatic increase in funding for U.S. spy agencies. For the fiscal year of 2014, the budget for U.S. spy agencies—the “black budget”—totaled \$52.6 billion.³⁴ That figure represents about twice the estimated size of the 2001 budget and a 25% increase since 2006, five years into what was then known as the “global war on terror.”³⁵ Over the past ten years the budget for the Central Intelligence Agency (“CIA”), National Security Agency (“NSA”), National Reconnaissance Office (“NRO”), National Geospatial-Intelligence Program (“NGIP”), and General Defense Intelligence Program (“GDIP”), have respectively increased by 56%, 53%, 12%, 108%, and 3%.³⁶ However, the public knows almost nothing about where this tax money went “because intelligence spending is considered top secret, and legislative oversight is done behind closed doors.”³⁷ Undoubtedly, some of that money funded the collection of classified information.

Regardless of the source of increased classification, the amount of classified decisions has reached an astonishing high since 2001. Before delving into the possible ramifications of overclassification, it is necessary to look at how the current regime of secrecy came to exist in the first place, and whether it actually has a legal basis.

32. *Id.*; see Scott Shane, *Complaint Seeks Punishment for Classification of Documents*, N.Y. TIMES, Aug. 2, 2011, at A16 (“While bureaucrats regularly get in trouble for failing to classify information their bosses think should be secret, Mr. [Steven] Aftergood . . . said he had never heard of anyone being punished for unjustified classification.”); REPORT OF THE COMM’N, *supra* note 6, at xxv (“Unfortunately, the secrecy system has developed into one in which accountability barely exists.”).

33. Goitein & Leonard, *supra* note 30.

34. Barton Gellman & Greg Miller, “Black Budget” Summary Details U.S. Spy Network’s Successes, Failures and Objectives, WASH. POST (Aug. 29, 2013), http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

35. *Id.*

36. Wilson Andrews & Todd Lindeman, *\$56.2 Billion: The Black Budget*, WASH. POST (Aug. 29, 2013), <http://www.washingtonpost.com/wp-srv/special/national/black-budget/>.

37. Cynthia Lummis & Peter Welch, *Intelligence Budget Should Not Be Secret*, CNN (April 21, 2014), <http://www.cnn.com/2014/04/21/opinion/lummis-welch-intelligence-budget/>; see also Gellman & Miller, *supra* note 34 (Director of National Intelligence James R. Clapper Jr., responding to inquiries, stated, “Our budgets are classified as they could provide insight for foreign intelligence services to discern our top national priorities, capabilities and sources and methods that allow us to obtain information to counter threats.”).

A. *The Origins of “CLASSIFIED”*

*The accretion of dangerous power does not come in a day. It does come, however slowly, from the generative force of unchecked disregard of the restrictions that fence in even the most disinterested assertion of authority.*³⁸

“From the earliest days of the Republic, American Presidents have asserted a right to conceal executive communications.”³⁹ One possible source of this power to make and keep secrets is the Constitution itself. But the Constitution only mentions the word “secrecy” once, in Article I:

Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those present, be entered on the Journal.⁴⁰

The clause does not mention any specifics as to what “Judgment require[s] Secrecy”; it does not say whether Congress can create a *system* of secrecy; there is no mention of any executive power to classify information; and there is certainly no description of any power to make the disclosure of secrets a crime. Significantly, the power described in the provision “is couched as an exception to a general norm of openness.”⁴¹ Thus, the provision suggests that, when government secrecy does occur, “it should be rare, difficult to engage in, and sufficiently exceptional as to be detectable”⁴² It by no means “evinces blanket constitutional approval of government secrecy.”⁴³ To the contrary, that the Constitution mentions the word “secrecy” in only one context is telling. The Framers could have explicitly provided for a power to create national secrets, either in the executive branch or in the legislative branch, but they did not do so.

Another possible source of secrecy power is executive privilege. It is possible that the executive power vested in Article II⁴⁴ encompasses a “right to conceal executive papers and communications.”⁴⁵ In other words, executive privilege might have been a commonly recognized attribute of the executive power, and proper understanding of the meaning of this phrase may have been lost in the passage of time.⁴⁶

38. *Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure)*, 343 U.S. 579, 594 (1952) (Frankfurter, J., concurring).

39. Saikrishna Bangalore Prakash, *A Critical Comment on the Constitutionality of Executive Privilege*, 83 MINN. L. REV. 1143, 1143 (1999).

40. U.S. CONST. art. I, § 5, cl. 3.

41. Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489, 523 (2007).

42. *Id.*

43. *Id.* at 524.

44. “The executive Power shall be vested in a President of the United States of America.” U.S. CONST. Art. II, § 1, cl. 1.

45. Prakash, *supra* note 39, at 1148.

46. *Id.* at 1149.

It is also possible that the Constitution contemplates that the executive privilege to conceal communications is essential and inherent to the execution of the President's constitutional duties.⁴⁷ While the privilege may not be explicitly safeguarded by the Constitution, the Constitution implicitly guarantees the means by which the President can discharge his duties.⁴⁸

A final possibility is that this executive privilege exists in the penumbra of Article II powers vested in the President.⁴⁹ While no textual authority specifically confers this privilege upon the President, the various powers guaranteed, when taken together, generate a shadow under which the President may operate in the execution of those powers.⁵⁰

In support of an executive privilege for secrecy, scholars have typically looked to two separate historical sources: statements made by delegates at the Constitutional Convention said to demonstrate an embrace of such privilege, and two passages from the Federalist Papers touting secrecy as one of the virtues entailed in having a unitary President.⁵¹ George Mason, speaking at the Constitutional Convention in 1787, stated, "[t]he chief advantages which have been urged in favor of unity in the Executive, are the secrecy, the dispatch, the vigor and energy which the government will derive from it, especially in time of war. That these are great advantages, I shall most readily allow."⁵² James Wilson averred the same: "[A]n executive ought to possess the powers of secrecy, vigour & Dispatch . . ."⁵³ Similarly, in the Federalist Papers, John Jay and Alexander Hamilton both extolled the qualities of secrecy and dispatch of a unitary Executive.⁵⁴ In The Federalist No. 64, Jay wrote:

It seldom happens in the negotiations of treaties, of whatever nature, but that perfect *secrecy* and immediate *despatch* [sic] are sometimes requisite . . . [T]here doubtless are many . . . who would rely on the

47. *Id.*

48. *Id.*

49. *Id.* at 1150.

50. *Id.*

51. Kitrosser, *supra* note 41, at 510.

52. 1 THE RECORDS OF THE FEDERAL CONVENTION OF 1787, at 112 (Max Farrand ed., 1911), available at http://f-oll.s3.amazonaws.com/titles/1057/0544-01_Bk.pdf.

53. *Id.* at 70. James Wilson later expanded upon the capacity of the President to keep secrets:

The executive power is better to be trusted when it has no screen. Sir, we have a responsibility in the person of our President; he cannot act improperly, and hide either his negligence or inattention; he cannot roll upon any other person the weight of his criminality; no appointment can take place without his nomination; and he is responsible for every nomination he makes . . . [He] is possessed of power far from being contemptible; yet not a *single privilege* is annexed to his character; far from being above the laws, he is amenable to them in his private character as a citizen, and in his public character by *impeachment*.

JAMES WILSON, *Remarks of James Wilson in the Pennsylvania Convention to Ratify the Constitution of the United States*, in 1 COLLECTED WORKS OF JAMES WILSON 236 (Kermit L. Hall & Mark David Hall eds., 2007), available at http://f-oll.s3.amazonaws.com/titles/2072/Wilson_4140.01_LFeBk.pdf (emphasis in original).

54. Kitrosser, *supra* note 7, at 887.

secrecy of the president, but who would not confide in that of the senate, and still less in that of a large popular assembly.⁵⁵

In The Federalist No. 70, Hamilton explained:

[A]ll men of sense will agree in the necessity of an energetic executive That unity is conducive to energy will not be disputed. Decision, activity, secrecy, and despatch [sic], will generally characterize the proceedings of one man, in a much more eminent degree than the proceedings of any greater number; and in proportion as the number is increased, these qualities will be diminished.⁵⁶

Critics of an executive privilege for secrecy have tried to put those statements in perspective. Professor Saikrishna Prakash has noted that there was never an explicit assertion made during the drafting or ratification of the Constitution to support the idea that a president “might enjoy a constitutional right to secret communications.”⁵⁷ While “several members of the founding generation [may have] commented favorably on the executive’s ability to act with secrecy,” those comments “hardly demonstrate that the proposed executive would enjoy a constitutional right to an executive privilege.”⁵⁸ Rather, the discussions about executive secrecy reflect but one of the many common attributes a single executive would enjoy over a plural legislature.⁵⁹

Textual and structural arguments also belie the notion that the President may have a superseding authority to keep and make secrets based on executive privilege alone. First and foremost, the Constitution is a document of enumerated powers—the federal government only enjoys those powers that the Constitution confers.⁶⁰ If the Constitution confers upon the President an executive privilege, there “must be some textual or structural basis for it.”⁶¹ Significantly, the Constitution lacks any explicit reference to anything resembling an executive privilege—the phrase “executive privilege” appears nowhere in its text. Additionally, the Constitution lacks any reference to a power to keep “secrets.”⁶² As noted above, the only text in the Constitution that mentions a variation of the word “secret” occurs in Article I as a power of the Legislature and as an exception to a general rule of openness.

Furthermore, the Framers understood that the President depends upon congressional legislation to help carry into execution his Article II powers.⁶³ As

55. THE FEDERALIST NO. 64, at 357 (John Jay) (Barnes & Noble Classics 2006).

56. THE FEDERALIST NO. 70, at 388 (Alexander Hamilton) (Barnes & Noble Classics 2006).

57. Prakash, *supra* note 39, at 1174.

58. *Id.* at 1175–76.

59. *Id.* at 1176.

60. *Id.* at 1151. See U.S. CONST. amend. X (“The powers *not delegated* to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.” (emphasis added)).

61. Prakash, *supra* note 39, at 1152.

62. *Id.*

63. *Id.* at 1153.

Prakash argues, “[T]he President lack[s] a constitutional right to any and all necessary or even helpful means of executing his powers. Congress . . . suppl[ies] the funds, raise[s] the armies and navies, and create[s] the officers and departments, notwithstanding the absolute centrality of these means to the executive branch’s operations.”⁶⁴

Even where the President may have a limited capacity to keep secrets, the text and structure of the Constitution do not equate this capacity with a vested secret-keeping right.⁶⁵ While the President may have a capacity to engage in secret activities in furtherance of his executive duties, Congress can curtail those activities by passing legislation or permitting itself or others to obtain information about those activities under certain conditions.⁶⁶ Because the executive branch is largely beholden to legislative directives in order to act, Congress can either mandate oversight of executive actions or otherwise restrain the secrecy within which the Executive may operate in service of those directives.⁶⁷

Notwithstanding the textual and structural arguments against an executive privilege to secrecy, the Supreme Court has moved in the opposite direction. In *United States v. Nixon*,⁶⁸ the Court recognized the existence of an “executive privilege”—an ability to withhold information—for the first time.⁶⁹ While the Court rejected President Nixon’s specific claim of executive privilege, it deemed the executive privilege doctrine, in itself, valid.⁷⁰ The Court confirmed that a “presumptive privilege for Presidential communications” exists.⁷¹ Specifically:

A President and those who assist him must be free to explore alternatives in the process of shaping policies and making decisions and to do so in a way many would be unwilling to express except privately. . . . The privilege is fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution.⁷²

The Court also acknowledged that courts should show “utmost deference” when a President invoked such a privilege on the grounds that his communications were “military or diplomatic secrets.”⁷³

Interestingly, and curiously, the Court went out of its way to make this pronouncement. The facts of the case before it did not require the Court to sanction any presumptive privilege for the President.⁷⁴ As some scholars maintain, “The Court simply could have said that, whatever the strength or weaknesses of a putative

64. *Id.*

65. Kitrosser, *supra* note 7, at 917.

66. *Id.*

67. *Id.* at 918.

68. 418 U.S. 683 (1974).

69. Eric Lane et al., *Too Big a Canon in the President’s Arsenal: Another Look at United States v. Nixon*, 17 GEO. MASON L. REV. 737, 743–44 (2010).

70. Kitrosser, *supra* note 41, at 501.

71. *Nixon*, 418 U.S. at 708.

72. *Id.*

73. *Id.* at 710.

74. Lane et al., *supra* note 69, at 744.

executive privilege, it would not prevail in the circumstances of the Nixon case.”⁷⁵ Whatever the reason for the Court’s recognition of this privilege, the Court’s opinion has served “to greatly enhance the power of future presidents and to hide facts from Congress and the American public.”⁷⁶

Accordingly, the fount of secrecy power appears, at least to the Court, to come from executive privilege. Presidents would be loath to disagree. For more than 70 years, the system of classification that we know today has existed by way of executive fiat.⁷⁷ With the exception of the Kennedy Administration, “a new executive order on classification [has been] issued each time one of the political parties regained control of the executive branch.”⁷⁸ These have often been at variance with one another, at times even outright reversing the policies of a previous order.⁷⁹

In 1940, President Franklin Roosevelt issued the first executive order on classification, which essentially conferred presidential recognition on the present military classification system.⁸⁰ Invoking § 795 of the Espionage Act,⁸¹ President Roosevelt’s order defined those military installations that he thought required “protection against the general dissemination of information.”⁸² Notably, the order required “the direction of the President” for something to be “classified, designated, or marked” as “‘secret’, ‘confidential’, or ‘restricted.’”⁸³

In 1951, President Harry Truman issued his own executive order on classification. Whereas President Roosevelt’s executive order invoked a specific statute, President Truman’s order invoked “the authority vested in [him] by the Constitution and statutes, and as President of the United States.”⁸⁴ The order created a system of regulations in order to “establish minimum standards . . . for identifying and protecting information the safeguarding of which is necessary in order to protect the security of the United States . . .”⁸⁵ “[C]lassified security information” was to be designated as either “Top Secret,” “Secret,” “Confidential,” or “Restricted.”⁸⁶ But only information requiring “protective safeguarding in the interest of the security of the United States” could be so classified.⁸⁷ Any head of an executive agency⁸⁸ wherein the “classified security information” originated, was considered

75. *Id.*

76. *Id.* at 745.

77. “[S]ecrets in the Federal Government are whatever anyone with a stamp decides to stamp secret. There is no statutory base and never has been; classification and declassification have been governed for nearly five decades by a series of executive orders . . .” REPORT OF THE COMM’N, *supra* note 6, at xxii.

78. *Id.* at 11.

79. *Id.*

80. Kitrosser, *supra* note 7, at 890.

81. 18 U.S.C. § 795 (2012).

82. *See generally* Exec. Order No. 8,381, 5 Fed Reg. 1,147 (Mar. 22, 1940).

83. *Id.*

84. *See generally* Exec. Order No. 10,290, 16 Fed. Reg. 9,795 (Sept. 24, 1951).

85. *Id.* § 1(a).

86. *Id.* § 2.

87. *Id.* § 3.

88. *Id.* § 9.

an “appropriate classifying authority.”⁸⁹ Importantly, the head of an executive agency could authorize “appropriate officials within his agency to assign information to the proper security classification”⁹⁰ President Truman’s order, in effect, granted nonmilitary agencies the ability to classify information whenever it seemed “necessary in the interest of national security.”⁹¹

Interestingly, President Richard Nixon’s 1972 executive order on classification specifically sought to avoid “[b]oth unnecessary classification and over-classification.”⁹² According to the order, classifications could only be made on the basis of “national security considerations.”⁹³ In no instance could information be classified “in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security.”⁹⁴ In addition, unlike past orders, President Nixon’s order provided concrete examples of the sort of potential damage that could justify a “Top Secret” classification.⁹⁵ The examples furnished in the order equipped officials better to assess the need for classification than the phrase “damage to the national security.”⁹⁶ Subsequent executive orders have lacked such specificity, thus granting classifiers a broad scope of classification.⁹⁷

President Bill Clinton’s executive order significantly contrasted with President George W. Bush’s executive order. For one, President Clinton’s order directed that information should not be classified “[i]f there is significant doubt about the need to classify that information.”⁹⁸ President Bush’s order omitted this directive.⁹⁹ Additionally, President Bush’s order omitted a directive by President Clinton’s order that “[i]f there is significant doubt about the appropriate level of

89. *Id.* § 19(a).

90. *Id.* § 24(c).

91. Kitrosser, *supra* note 7, at 890.

92. Exec. Order No. 11,652, §§ 4, 37, Fed. Reg. 5,209 (Mar. 8, 1972).

93. *Id.*

94. *Id.* While this is not specific proof that the classification system was being abused for such purposes, orders like this beg the question as to why such practices would be specifically mentioned if they were not a problem.

95. Steven Aftergood, *An Inquiry Into the Dynamics of Government Secrecy*, 48 HARV. C.R.-C.L. L. REV. 511, 513 (2013); *see also* Exec. Order No. 11,652, 37 Fed. Reg. 5,209, at § 1(A) (Mar. 8, 1972) (“‘Top Secret’ refers to that national security information or material which requires the highest degree of protection. The test for assigning ‘Top Secret’ classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of ‘exceptionally grave damage’ include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technologic developments vital of national security. This classification should be used with the utmost restraint.”).

96. Aftergood, *supra* note 95, at 514.

97. *Id.*

98. Exec. Order No. 12,958, § 1.2(b), 60 Fed. Reg. 19,825, 19,826 (Apr. 17, 1995).

99. *See generally* Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

classification, it shall be classified at the lower level.”¹⁰⁰ In contrast, President Bush’s order added a provision that declared “[t]he unauthorized disclosure of foreign government information is presumed to cause damage to the national security.”¹⁰¹

President Barack Obama’s Executive Order No. 13526 currently governs the classification of information. Notably, it reinstated the Clinton directive that information should not be classified if significant doubts exist about its need to be classified.¹⁰² It also re-installed the Clinton directive that information should be classified at a lower level if significant doubts exist about the appropriate level of classification.¹⁰³ President Obama’s order, however, kept the Bush directive that “unauthorized disclosure of foreign government information is presumed to cause damage to the national security.”¹⁰⁴

Tautologically, the order defines “national security” to mean “the national defense or foreign relations of the United States.”¹⁰⁵ Further, it defines “[d]amage to the national security” as “harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information”¹⁰⁶ The circularity of these definitions could encompass the activities and publications of anyone, individuals and newspapers, deterring the release or publication of all kinds of information about the government for fear of affecting national security or national defense.¹⁰⁷

Additionally, like previous orders, all levels of classification refer to the degree of “damage to the national security” that unauthorized disclosure could be expected to cause: “grave damage” gets “Top Secret” classification; “serious damage” gets “Secret” classification; and mere “damage” gets “Confidential” classification.¹⁰⁸ In effect, any information that is labeled “top secret,” “secret,” or

100. Exec. Order No. 12,958, § 1.3(c), 60 Fed. Reg. 19,825, 19,826 (Apr. 17, 1995).

101. Exec. Order No. 13,292, § 1.1(c), 68 Fed. Reg. 15,315, 15,315 (Mar. 25, 2003).

102. Exec. Order No. 13,526, § 1.1(b), 75 Fed. Reg. 707, 707 (Dec. 29, 2009).

103. *Id.* § 1.2(c).

104. *Id.* § 1.1(d). “Foreign government information” is defined as:

- (1) information provided to the United States Government by a foreign government or governments, or international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
- (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
- (3) information received and treated as “foreign government information” under the terms of a predecessor order.

Id. § 6.1(s).

105. *Id.* § 6.1(cc).

106. *Id.* § 6.1(l).

107. Bakken, *supra* note 2, at 5.

108. Exec. Order No. 13,526, § 1.2(a)(1)–(3), 75 Fed. Reg. 707, 707–08 (2009).

“confidential,” which is disclosed to an unauthorized person, *presumably* causes some sort of damage to national security, regardless of whether that assumption is right or wrong.

The lack of specificity as to what constitutes “damage to the national security” has been acknowledged by the Office of the Director of National Intelligence as problematic. In an unclassified report, the Director found:

There appears to be no common understanding of classification levels among the classifications guides reviewed by our team, nor any consistent guidance as to what constitutes ‘damage,’ ‘serious damage,’ or ‘exceptionally grave damage’ to national security—nor is it clear what simply needs to be protected from broad public dissemination (unclassified but for official use only). There is a wide variance in application of classification levels.¹⁰⁹

The problem is not so much that the terms are meaningless, but rather that they are highly subjective.¹¹⁰

This subjectivity is reflected in the amount of overclassification that has appeared recently. In a statement to the House Committee on the Judiciary, Thomas Blanton, director of the National Security Archive at George Washington University, said, “[E]xperts believe 50% to 90% of our national security secrets could be public with little or no damage to real security.”¹¹¹ Similarly, after the 9/11 Commission reviewed the government’s most sensitive records about Osama bin Laden and Al-Queda, the Commission’s co-chair Thomas Kean observed, “Most of what I read that was classified shouldn’t have been. Easily 60 percent of the classified documents have no reason to be classified—none.”¹¹²

B. The Problems of Overclassification

It is obvious that secrecy can serve executive branch agencies, as well as national security interests. But secrecy can also serve as an effective means of “evading controversy, gaining political advantage, concealing misconduct, excluding critical voices, and undermining accountability.”¹¹³

Secrecy and an overabundance of secrecy pose several problems. For one, secrecy eliminates a system of checks and balances over the executive branch. “[T]here can be no checks and balances against a program that is implemented in secret unless the very fact of the program, including the need for secret

109. DIR. OF NAT’L INTELLIGENCE ET AL., INTELLIGENCE COMMUNITY CLASSIFICATION GUIDANCE FINDINGS AND RECOMMENDATIONS REPORT 11 (2008), *available at* <http://www.fas.org/sgp/othergov/intel/class.pdf>.

110. Aftergood, *supra* note 95, at 515.

111. *Hearing on the Espionage Act and the Legal and Constitutional Implications of Wikileaks Before the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement of Thomas Blanton, Director, National Security Archive, George Washington University), *available at* <http://www2.gwu.edu/~nsarchiv/news/20101216/Blanton101216.pdf>.

112. Scot J. Paltrow, *Exclusive: National Archives Sits On 9/11 Commission Records*, REUTERS (Sept. 8, 2011, 8:18 AM), <http://www.reuters.com/article/2011/09/08/us-sept11-archive-idUSTRE7872QI20110908>.

113. Aftergood, *supra* note 95, at 523.

implementation, is disclosed and publicly debated.”¹¹⁴ This lack of checks and balances in the executive branch also “lends itself to a culture of ‘group think’ that secrecy fosters and exacerbates.”¹¹⁵ Many have argued that the reluctance of both the press and Congress to ask difficult questions prior to the invasion of Iraq, combined with the Bush Administration’s particular proclivity for secrecy, created an insular environment within the White House that stifled debate, and allowed for easy acceptance of questionable data on weapons of mass destruction and equally questionable predictions of a peaceful post-invasion Iraq.¹¹⁶

Another problem with overclassification is that it jeopardizes national security by inhibiting information sharing both within the various agencies of the federal government and with state and local agencies.¹¹⁷ By limiting the sharing of information between officials and agencies, overclassification inhibits the government’s ability to understand and link data about security threats.¹¹⁸ Kean said that the failure to prevent the 2001 attacks was not rooted in leaks of sensitive information, but in the barriers that obstructed the sharing of information between various agencies.¹¹⁹ This failure was again exemplified on December 25, 2009.¹²⁰ When a Nigerian named Umar Farouk Abdulmutallab boarded Northwest Airlines Flight 253 and tried to ignite explosives hidden in his underwear, it was not the very expensive and immense post-9/11 national security system that prevented the disaster.¹²¹ It was a passenger who saw what Abdulmutallab was doing and tackled him.¹²² There were numerous clues about a possible attack, but nobody put them

114. Kitrosser, *supra* note 41, at 543; *see also* 158 CONG. REC. S6793–94 (daily ed. Nov. 14, 2012) (statement of Sen. Ron Wyden) (“[M]embers [of Congress] often rely on the press to inform them about problems that congressional overseers have not discovered on their own. I have been on the Senate Intelligence Committee for 12 years now, and I can recall numerous specific instances where I found out about serious government wrongdoing—such as the NSA’s warrantless wiretapping program, or the CIA’s coercive interrogation program—only as a result of disclosures by the press.”).

115. Kitrosser, *supra* note 7, at 910. “Groupthink” involves making decisions as a group in a way that discourages creativity or individual responsibility. *Groupthink Definition*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/groupthink?q=group+think (last visited March 23, 2015).

116. Kitrosser, *supra* note 41, at 537.

117. Goitein & Leonard, *supra* note 30.

118. Goitein, *supra* note 31.

119. Scott Shane, *Since 2001, Sharp Increase in the Number of Documents Classified by the Government*, N.Y. TIMES (July 3, 2005), <http://query.nytimes.com/gst/fullpage.html?res=9907EFD9113AF930A35754C0A9639C8B63>; *see also* NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, at xvi (2004), *available at* <http://www.9-11commission.gov/report/911Report.pdf> (“We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers.”).

120. *US Says Explosion On Plane Was Terrorism Attempt*, REUTERS (Dec. 25, 2009), <http://www.reuters.com/article/2009/12/26/usa-flight-idUSN2513625920091226?type=marketsNews>.

121. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1.

122. *Id.*

together because, as officials would later testify, the system had gotten so large that “the lines of responsibility had become hopelessly blurred.”¹²³

Secrecy in its most dangerous form also poses the possibility of it being misused by those set on manipulating public debate towards their own ends.¹²⁴ Through classifications, designated federal employees have the authority to decide what government information should be censored.¹²⁵ The executive branch can then spin government information through selective declassification or leakage of otherwise classified information.¹²⁶ Additionally, because the disclosure of classified information is illegal, the executive branch maintains the ability to prosecute the unwanted disclosure of classified information.¹²⁷ Further, the executive branch can determine not only which information the public can see, but which disclosures it wants to punish as well.

II. PEN AND SWORD: THE EXECUTIVE’S ABILITY TO BOTH WRITE AND PROSECUTE THE LAW ON CLASSIFIED INFORMATION

The classification system has ballooned to a staggering size since 2001. While the excessive amount of classified documents is itself a problem, the Executive’s unfettered discretion to determine what should be classified is far more troubling. As this Part illustrates, this discretion to classify comes hand-in-hand with the Executive’s discretion to prosecute any leaks of classified information. As the law currently stands, the Executive holds both pen and sword: it can classify the very information that it later has the ability to prosecute for its improper disclosure.

A. *The Espionage Acts*

Congress has attempted to pass the equivalent of an “Official Secrets Act”—which would authorize the punishment of government insiders for the mere revelation of classified information—many times, but every time it has failed.¹²⁸ Despite congressional failures to adopt an official secrets act, the existing criminal statutes give the Department of Justice (“DOJ”) sufficient means for prosecuting unauthorized leaks.¹²⁹ While the name of the Espionage Act may suggest that it is limited only to espionage, the plain language of the statute suggests that is not so limited.¹³⁰

123. *Id.*

124. Kitrosser, *supra* note 41, at 540.

125. Bakken, *supra* note 2, at 3.

126. Kitrosser, *supra* note 41, at 540. See David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 529 (2013) (“Journalists and government insiders have consistently attested that leaking is far more common among those in leadership positions.”).

127. See *infra* Part II.

128. Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 507–08 (2014).

129. *Id.* at 509.

130. *Id.*

The basic provisions of the Espionage Act are codified in §§ 793–794 of Title 18 of the United States Code.¹³¹ Section 794 prohibits traditional espionage activities; § 794(a) punishes actual or attempted communication with a foreign agent of any document or information “relating to the national defense” if the communication is “with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation.”¹³² Punishment for a violation of § 794(a) is “death” or “a term of imprisonment for any term of years or for life.”¹³³ Both the language of and Congress’s intent behind § 794(a) lead to the conclusion that the provision does not include public speech.¹³⁴

Section 794(b) (applicable only “in time of war”) comprehends the transfer of information to “the enemy” (undefined), and prohibits “collect[ing], record[ing], publish[ing], or communicat[ing], or attempt[ing] to elicit any information with respect to” troop movements and military plans or “any other information relating to the public defense, which might be useful to the enemy” with the “intent that the same shall be communicated to the enemy.”¹³⁵ Violating § 794(b) carries a punishment equal to that of § 794(a).¹³⁶ Scholars have concluded that this statute is only violated if information is published about troop movements and ship sailings with the purpose of communicating it to an enemy; a newspaper that publishes such information simply to satisfy its own readers’ curiosity does not violate this law.¹³⁷

Sections 794(a) and 794(b) thus create offenses involving the intentional transmission of information to foreign governments, agents, and citizens,¹³⁸ and also “criminalize preparatory conduct intended to achieve the proscribed results.”¹³⁹ The government has not indicted any leakers under § 794.¹⁴⁰ The lack of prosecutions under § 794 leads to the conclusion that the statute is either under-used or unnecessary.

“Section 793 defines six offenses, each involving conduct [that] would be preliminary to foreigners’ acquisition of information.”¹⁴¹ Subsections (c), (d), and (e) are the more sweeping and more problematic provisions¹⁴² in that they

131. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 937 (1973).

132. *Id.* (quoting 18 U.S.C. § 794(a) (2012)).

133. 18 U.S.C. § 794(a).

134. Edgar & Schmidt, Jr., *supra* note 131, at 943.

135. 18 U.S.C. § 794(b).

136. *See id.*

137. Edgar & Schmidt, Jr., *supra* note 131, at 965.

138. *Id.* at 938.

139. *Id.*

140. Papandrea, *supra* note 128, at 509.

141. Edgar & Schmidt, Jr., *supra* note 131, at 938. Section 793(a) prohibits “enter[ing], fl[y]ing over, or otherwise obtain[ing] information concerning . . . place[s] connected with the national defense” for “the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States.” 18 U.S.C. § 793(a). Section 793(b) prohibits, “for the purpose aforesaid,” “copy[ing], tak[ing], mak[ing], or obtain[ing],” any document “connected with the national defense.” *Id.* § 793(b).

142. Edgar & Schmidt, Jr., *supra* note 131, at 938.

criminalize the following: the receipt of material knowing that it has been obtained in violation of other espionage provisions,¹⁴³ communication of defense-related material or information to any person not entitled to receive it,¹⁴⁴ and retention of such information.¹⁴⁵ Subsections (d) and (e) prohibit willful conduct, while subsection (c) appears to prohibit *any* receipt of defense information by a person who knows that it was obtained in violation of the espionage laws.¹⁴⁶ Subsections (c), (d), and (e) also do not, at least on their face, require an intent to harm the United States.¹⁴⁷ Thus, subsections (c), (d), and (e) may make criminal nearly all acquisitions of “national defense” information, be it by private individuals or by newspapers.¹⁴⁸ Leakers are commonly charged under § 793(d).¹⁴⁹

B. A Closer Look at Sections 793(d) and 793(e)

Sections 793(d) and 793(e) are the most troublesome of all the espionage statutes.¹⁵⁰ The subsections read:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, *willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted* or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same *to any person not entitled to receive it, or willfully retains the same* and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, *willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted*, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same *to any person not entitled to receive it, or willfully retains the*

143. 18 U.S.C. § 793(c).

144. *Id.* § 793(d).

145. *Id.* § 793(e).

146. Edgar & Schmidt, Jr., *supra* note 131, at 938.

147. *Id.*

148. *Id.*

149. Papandrea, *supra* note 128, at 509.

150. Edgar & Schmidt, Jr., *supra* note 131, at 966.

same and fails to deliver it to the officer or employee of the United States entitled to receive it¹⁵¹

No special culpability requirement explicitly restricts the reach of subsections (d) and (e); a person need only act “willfully.” Any person who communicates defense material or information to anyone “not entitled to receive it” commits a serious criminal offense, regardless of whether they intended harm to the nation or whether they communicated such information mistakenly.¹⁵² Even “willfully retain[ing]” possession of such material is unlawful for those who lack special authorization.¹⁵³ As Harold Edgar and Benno Schmidt, Jr. have pointed out:

If these statutes mean what they seem to say and are constitutional, public speech in this country since World War II has been rife with criminality. The source who leaks defense information to the press commits an offense; the reporter who holds onto defense material commits an offense; and the retired official who uses defense material in his memoirs commits an offense.¹⁵⁴

One of the major problems with subsection 793(d) and (e) is that they fail to define those “not entitled to receive it,” which determines to whom communication of defense information is barred.¹⁵⁵ An attempt to give the President power to say who was and was not “entitled” to receive defense information was struck from the Espionage Act in 1917.¹⁵⁶ In light of this deletion, it is questionable whether the term can be given meaning by reference to an executive order.¹⁵⁷ Even so, none of the executive orders since the adoption of this language has made any reference to the “not entitled to receive it” formulation of subsection 793(d) and (e).¹⁵⁸

Another problem that consumes subsection 793(d) and (e) is whether, and to what extent, a violation requires any culpable motivation.¹⁵⁹ The subsections only use the word “willfully,” suggesting merely the requirement that a person act with knowledge that his conduct was unlawful,¹⁶⁰ as opposed to the other sections of the statute that require some purposeful “intent or reason to believe that the information is to be used to the injury of the United States.”¹⁶¹

Further still, the subsections do not define the ambiguous phrase “relating to national defense,” nor does any other part of the statute. To that end, the Supreme Court has given the Executive wide latitude to define documents and information “relating to national defense.”¹⁶² In *Gorin v. United States*, the Court undertook a

-
151. 18 U.S.C. § 793(d)–(e) (2012) (emphasis added).
 152. Edgar & Schmidt, Jr., *supra* note 131, at 1000; 18 U.S.C. 793(d).
 153. Edgar & Schmidt, Jr., *supra* note 131, at 1000; 18 U.S.C. 793(3).
 154. Edgar & Schmidt, Jr., *supra* note 131, at 1000.
 155. *Id.* at 1001.
 156. *Id.*
 157. *Id.*
 158. *Id.*; see generally Exec. Order. No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).
 159. Edgar & Schmidt, Jr., *supra* note 131, at 1001.
 160. Papandrea, *supra* note 126, at 509.
 161. 18 U.S.C. §§ 793(a)–(c), 794(a) (2012).
 162. See *Gorin v. United States*, 312 U.S. 19, 27–28 (1941).

challenge to the espionage statutes on the grounds that the phrase “information connected with or relating to national defense” was unconstitutionally vague.¹⁶³ The Court concluded that that statute contained “no uncertainty” that would “deprive a person of the ability to predetermine whether a contemplated action is criminal under the provisions of this law.”¹⁶⁴ According to the Court, the words “national defense,” as they are used in the statute, carry “a well understood connotation.”¹⁶⁵ “National defense” under the Espionage Act, as the Government maintained and the Court agreed with, is “a generic concept of broad connotations, referring to the military and naval establishments and the related activities of *national preparedness*.”¹⁶⁶ What activities constitute “national preparedness” is unclear. The Court conclusively stated that, “[w]here there is no occasion for secrecy, as with reports relating to national defense, . . . there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.”¹⁶⁷

The broad standard provided in *Gorin* gives the executive branch wide latitude in determining what information constitutes “national defense,” and whether it will choose to prosecute based on that determination. The standard of national preparedness appears to comprehend the national capacity to produce military goods.¹⁶⁸ But it could also include information about the political and diplomatic establishments that set the boundaries of military actions.¹⁶⁹ National preparedness could include information about oil reserves, agricultural production, ports, and airports; additionally, it could include multifarious activities that would otherwise appear innocuous.

Gorin specifically addressed challenges to § 793(b) and § 794(a).¹⁷⁰ Both § 793(b) and § 794(a) require a specific “intent or reason to belief that the information is to be used to the injury of the United States, or to the advantage of any foreign nation.”¹⁷¹ With this in mind, it’s not entirely clear that the Court would similarly uphold a challenge to either § 793(d) or § 793(e), but it would not be a stretch to assume that it would. In *New York Times Co. v. United States*, Justice White’s concurrence construed the actions of the newspapers to fall under § 793(e).¹⁷² According to Justice White, by enacting the espionage statutes, Congress “ha[d] addressed itself to the problems of protecting the security of the country and the national defense from unauthorized disclosure of potentially damaging information.”¹⁷³

163. *Id.* at 23.

164. *Id.* at 27.

165. *Id.* at 28.

166. *Id.* (quoting Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217) (emphasis added) (internal quotations omitted).

167. *Id.* at 27–28.

168. Edgar & Schmidt, Jr., *supra* note 131, at 976.

169. *Id.*

170. *See Gorin*, 312 U.S. at 21.

171. 18 U.S.C. § 793(b) (2012).

172. 403 U.S. 713, 737 (1971) (White, J., concurring) (“I would have no difficulty in sustaining convictions under these sections on facts that would not justify the intervention of equity and the imposition of a prior restraint.”).

173. *Id.* at 740.

In *United States v. Morison*, the Fourth Circuit ruled that § 793(d) and § 793(e) were not only constitutional, but also that they were not limited to “classic spying” activities.¹⁷⁴ Samuel Morison was convicted under § 793(d) and § 793(e) for the unauthorized transmission of satellite secured photographs “to ‘one not entitled to receive them,’” for obtaining secret intelligence reports without authorization, and retaining them without delivering them “to ‘one entitled to receive’ them.”¹⁷⁵ Morison appealed his conviction on the ground that the prohibitions of § 793(d) and § 793(e) should be strictly confined to conduct representing “classic spying and espionage activity.”¹⁷⁶ Morison argued that because he merely leaked the information to the press and did not transmit it to a foreign government, he was not guilty of a violation under the Espionage Act.¹⁷⁷ The Fourth Circuit flat-out rejected Morison’s argument. The legislative record, the court said, showed unmistakably that § 793(d) was intended to apply to disclosures to *anyone* “not entitled to receive” national defense information.¹⁷⁸ According to the court, there was “no basis in the legislative record for finding that Congress intended to limit the applications of section 793(d) and (e) to ‘classic spying’ or to exempt transmittal by a government employee, who . . . had in violation of the rules of his intelligence unit, leaked to the press” secret defense material.¹⁷⁹

Morison also argued that the statutes were unconstitutionally vague. Morison first argued that the phrase “relating to the national defense” could not survive constitutional challenge.¹⁸⁰ The court rejected this contention because prior precedent had already decided that the very same language in § 793(f)(2) “was not ‘vague in the constitutional sense.’”¹⁸¹ Next, Morison argued that because the statutes did not define whom may “receive” defense material, the phrase “entitled to receive it” was vague.¹⁸² To this point, the court looked to the classification system set up by executive order.¹⁸³ According to the court, the words “entitled to receive” were “limited and clarified by the Classification Regulations and, as so limited and clarified, [were] not vague.”¹⁸⁴ The court in effect, gave free range to the Executive to control information. By executive order, the Executive can determine who is “entitled to receive” material “relating to the national defense,” which is also defined by the Executive.

By enacting the Espionage Acts, “Congress has delegated the authority to make possession or disclosure of public information a criminal act to the classifying and prosecuting federal employees.”¹⁸⁵ Not only does the Executive determine what material is contained by the Espionage Acts, it also determines when the law has

174. 844 F.2d 1057, 1070 (4th Cir. 1988).

175. *Id.* at 1060.

176. *Id.* at 1063.

177. *Id.*

178. *Id.* at 1065.

179. *Id.* at 1070.

180. *Id.* at 1071.

181. *Id.*

182. *Id.* at 1074.

183. *Id.*

184. *Id.* at 1075.

185. Bakken, *supra* note 2, at 3.

been violated and may prosecute to its discretion. In regard to classified information, the executive branch can both write and execute the law and there does not appear to be any limits upon these abilities.

C. Current Prosecutions

Since 2009, the Obama Administration has pursued an aggressive policy against whistleblowers and leakers through the Espionage Act.¹⁸⁶ To date, the Administration has used the act to prosecute eight federal employees for disclosing classified information to the media.¹⁸⁷ Prior to this and for almost a hundred years, the Act has only been used three times to convict government officials.¹⁸⁸

In pursuit of these prosecutions, the government has used a vast array of disquieting techniques. In May 2013, the *Associated Press* reported that the DOJ secretly obtained two-months worth of the publication's telephone records.¹⁸⁹ Those records listed outgoing calls and personal phone numbers of individual reporters and office personnel in New York City, Washington, D.C., and Hartford, Connecticut.¹⁹⁰ In all, the government seized the records for more than 20 separate telephone lines assigned to the *Associated Press*'s office personnel and journalists in April and May of 2012.¹⁹¹

Similarly, when the DOJ began investigating possible classified leaks in 2009, investigators did more than obtain the telephone records of a working journalist suspected of receiving the source material.¹⁹² The DOJ used security badge access records to track the reporter's comings and goings from the State Department; they traced the timing of his calls with the State Department security adviser suspected of sharing the classified information; and they obtained a search warrant for the reporter's personal emails.¹⁹³

In response to criticism over these tactics, in 2013 Eric Holder, U.S. Attorney General, announced new guidelines that would significantly narrow the circumstances under which journalists' records could be obtained.¹⁹⁴ The guidelines, made effective in early 2014, state that the practice of issuing subpoenas, court

186. Katrina vanden Huevel, Op-Ed., *Threats to a Free Press, From Ferguson to the White House*, WASH. POST (Aug. 26, 2014), http://www.washingtonpost.com/opinions/katrina-vanden-heuvel-the-white-houses-threat-to-a-free-press/2014/08/25/fa1b5e9c-2ca5-11e4-9b98-848790384093_story.html?tid=rssfeed.

187. Bakken, *supra* note 2, at 7.

188. Carr, *supra* note 2.

189. Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, ASSOC. PRESS (May 13, 2013, 10:53 PM), <http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe>.

190. *Id.*

191. *Id.*

192. Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, WASH. POST (May 20, 2013, 3:10 PM), http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html.

193. *Id.*

194. Charlie Savage, *Holder Tightens Rules on Getting Reporters' Data*, N.Y. TIMES, July 13, 2013, at A1.

orders, and search warrants “to seek information from, or records of, non-consenting members of the news media” were to be “extraordinary measures, not standard investigatory practices.”¹⁹⁵ Prosecutors may only implement such practices “when the information sought is essential to a successful investigation, prosecution, or litigation; after all reasonable alternative attempts have been made to obtain the information from alternative sources; and after negotiations with the affected member of the news media have been pursued”¹⁹⁶ DOJ employees “must [also] obtain the authorization of the Attorney General to issue a subpoena to a member of the news media”¹⁹⁷ Importantly, in investigations concerning the “unauthorized disclosure of national defense information” the Director of National Intelligence must certify to the Attorney General the significance of the harm caused by the unauthorized disclosure, and further affirm that the disclosed information was “properly classified” before the Attorney General authorizes the issuance of subpoenas to members of the news media.¹⁹⁸

Unfortunately, these policy guidelines are not binding on the government. As the guidelines themselves state, they are “not intended to, and [do] not, create any right or benefit, substantive or procedural, enforceable at law or equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.”¹⁹⁹ Indeed, failure to comply with the guidelines “*may* constitute grounds for an administrative reprimand or other appropriate disciplinary action.”²⁰⁰ There is no legal consequence for failing to follow the guidelines.²⁰¹ Subpoenas, search warrants, and court orders are not rescinded or suppressed, and no one who acts contrary to the guidelines faces any type of punishment, misdemeanor or felony. In essence, the guidelines are just that: guidelines.

Furthermore, the policy does not extend any special protection to members of the news media “who are the focus of criminal investigations for conduct based on, or within the scope of, ordinary newsgathering activities.”²⁰² The guidelines do not define what constitutes “ordinary newsgathering activities.” Thus, whether gathering classified information from anonymous sources constitutes an “ordinary newsgathering activity” is up to executive interpretation.

195. Policy Regarding Obtaining Information From, or Records of, Members of the News Media, 80 Fed. Reg. 2,819, 2,820–21 (Jan. 21, 2015) (to be codified as 28 C.F.R. § 50.10(a)(3)).

196. *Id.*

197. *Id.* (to be codified as 28 C.F.R. § 50.10(c)(1)).

198. *Id.* (to be codified as 28 C.F.R. § 50.10(c)(4)(v)).

199. *Id.* (to be codified as 28 C.F.R. § 50.10(i)).

200. *Id.* (to be codified as 28 C.F.R. § 50.10(h)) (emphasis added).

201. See Ellen S. Podgor, *Department of Justice Guidelines: Balancing “Discretionary Justice,”* 13 CORNELL J.L. & PUB. POL’Y 167, 169 (2004) (“The accused has no judicial recourse when prosecutors fail to abide by these guidelines, as courts routinely find these guidelines strictly internal and unenforceable at law.”).

202. Policy Regarding Obtaining Information From, or Records of, Members of the News Media, 80 Fed. Reg. at 2,820–21 (to be codified as 28 C.F.R. § 50.10(a)(1)).

Additionally, the guidelines do not apply to special prosecutors.²⁰³ Special Prosecutor Patrick Fitzgerald evidenced this very danger when he chose to subpoena reporters in his investigation of the Valerie Plame leak.²⁰⁴ In 2003 Valerie Plame's identity as a CIA officer "was leaked in an article . . . shortly after her husband Joseph Wilson, a former U.S. diplomat, had published an article in the *New York Times* criticiz[ing] the Bush administration's use of intelligence before the war in Iraq."²⁰⁵ Prior to Fitzgerald's investigation of the leak, government officials expected leak investigations to be pursued with little zeal, which would not involve questioning journalists.²⁰⁶ Journalists also believed themselves to be immune from being forced to testify about their confidential sources.²⁰⁷ But Fitzgerald surprised both sources and journalists when he not only subpoenaed reporters, but also prevailed in court on challenges to those subpoenas.²⁰⁸

One commentator congratulated the Executive by noting that "the existence and durability of these guidelines might seem quite remarkable. For in functional terms, they amount to codification of a qualified reporter's privilege."²⁰⁹ But without a statute codifying a reporter's privilege, or a judicial determination that the First Amendment guarantees such a privilege, the protection of sources and reporters becomes dependent on executive discretion alone. And as the actions of the current Administration have demonstrated, that discretion since 2009 has more than doubled the amount of people prosecuted under the Espionage Act.

III. RIGHTING THE SHIP

Parts I and II demonstrated the ills that correspond with the current classification system. Most troubling of all is the complete lack of checks on the Executive. The Executive both writes and executes the law of classification. It determines what information "relates to national defense" and who is "entitled to receive it." Where a leak occurs, the Executive can then choose whether to prosecute it or not. In effect, the current classification system sets up a system of information control that is entirely dependent upon nondemocratic discretion. Though it is quite possible that there is no going back, there are several possible solutions to the

203. *In re* Special Proceedings, 373 F.3d 37, 44 n.3 (1st Cir. 2004) ("The regulation states that 'the following shall be adhered to by all members of the Justice Department in all cases,' 28 C.F.R. § 50.10 (2003), but a special prosecutor is not a member of the Justice Department."). While the current regulation contains different wording, it does not stray from the intent of the previous regulation. See Policy Regarding Obtaining Information From, or Records of, Members of the News Media, 80 Fed. Reg. 2,819, 2,820–21 (Jan. 21, 2015) (to be codified as 28 C.F.R. § 50.10(c)(1)) ("[M]embers of the Department must obtain authorization of the Attorney General . . ." (emphasis added)).

204. William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1471 (2008).

205. Paul Reynolds, *Q & A: The CIA Leak Case*, BBC NEWS (Sept. 9, 2006), <http://news.bbc.co.uk/2/hi/americas/4298732.stm>.

206. Lee, *supra* note 204, at 1471–72.

207. *Id.* at 1472.

208. *Id.*; see also *In re* Grand Jury Subpoena, Judith Miller, 438 F.3d 1141, 1183 (D.C. Cir. 2005).

209. Pozen, *supra* note 126, at 539.

problems associated with the current information-control regime. This Part will examine the most realistic and feasible of those solutions.

A. Legislative Solutions

As it stands, there is no statute that regulates the classification of information. Instead, classification has rested entirely upon successive executive orders, which have, from time to time, reshaped the entire landscape of classification with one broad stroke.²¹⁰ With uncertainty over what system controls and what should be classified, agents and agencies tend to overclassify rather than underclassify.²¹¹

In order to combat overclassification, Congress should enact legislation to set up procedures for classification, and clear standards under which information is to be classified. As far as standards go, President Nixon's Executive Order No. 11652 would be a good place to start because it provided concrete examples for the various levels of classification.²¹² Such legislation should also create punishments for instances where the classification system is abused.

In addition to eliminating some of the uncertainty, legislation would also put the classification system on surer footing. It is not entirely clear that classification through executive order is legal,²¹³ and by enacting legislation Congress could inject some legitimacy into the system. Enacting legislation would also provide Congress with oversight capabilities.

Another piece of important legislation should involve amending § 793(d) and § 793(e) of the Espionage Act. The subsections as they currently read are far too broad in that they are not limited to traditional spying activities. Congress should enact legislation that not only provides an intent requirement similar to that of § 794, but also enact legislation that defines the terms "relating to national defense" and "entitled to receive it" more specifically. Tying these two terms with any possible classification statutes would be optimal because it would provide further clarification as to whom the statute covers and what actions are considered criminal. As is, the statute does not enunciate either.

B. Judicial Solutions

As Justice Stewart remarked in the *New York Times*:

In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry—in an

210. REPORT OF THE COMM'N, *supra* note 6, at 11.

211. *Cf. supra* text accompanying notes 30–32; REPORT OF THE COMM'N, *supra* note 6, at 12 ("Aware that classification orders are regularly replaced, some officials opposed to the specifics of a given order have resisted complying with and enforcing policies, essentially waiting out an administration in the hope that the order will be replaced.")

212. *See* Exec. Order No. 11,652, § 14, 37, Fed. Reg. 5,209 (Mar. 8, 1972).

213. *See supra* text accompanying notes 61–68.

informed and critical public opinion which alone can here protect the values of democratic government.²¹⁴

However, the public's ability to be informed is diminishing. Recent circuit court decisions have given the Executive greater power to prosecute those who leak classified information. Specifically, the government may now subpoena reporters to testify as to the source of their confidential information.

Recently in *United States v. Sterling*, the Fourth Circuit ruled:

There is no First Amendment testimonial privilege, absolute or qualified, that protects a reporter from being compelled to testify by the prosecution or the defense in criminal proceedings about criminal conduct that the reporter personally witnessed or participated in, absent of a showing of bad faith, harassment, or other such non-legitimate motive, even though the reporter promised confidentiality to his source.²¹⁵

The Fourth Circuit relied heavily on *Branzburg v. Hayes*²¹⁶ in ruling that a reporter's privilege did not apply in criminal proceedings.²¹⁷ The court insisted that, though a reporter's privilege to safeguard the confidentiality of their sources extended to civil proceedings, no such privilege existed in the criminal context due to a "compelling public interest in effective criminal investigation and prosecution . . ."²¹⁸ The Fourth Circuit arrived at its opinion with the help of *In re Grand Jury Subpoena, Judith Miller*,²¹⁹ which stated that, "[u]nquestionably, the Supreme Court decided in *Branzburg* that there is no First Amendment privilege protecting journalists from appearing before a grand jury or from testifying before a grand jury or otherwise providing evidence to a grand jury regardless of any confidence promised by the reporter to any source."²²⁰ The First and Seventh Circuits reached similar conclusions as well.²²¹

These rulings carry special significance with respect to the Espionage Act. Because § 793(d) and § 793(e) do not require any specific intent, but merely that a person "communicate" information to someone "not entitled to receive it",²²² any disclosure of classified information to reporters, even in confidence, is not protected by any means. The government may simply subpoena the reporter who wrote about the classified information to find the leaker and plug the hole in the leaking ship.

Recent crackdowns have sent a loud message; as one reporter stated: "There's definitely a chilling effect. Government officials who might otherwise

214. 403 U.S. 713, 728 (1971) (Stewart, J., concurring).

215. *United States v. Sterling*, 724 F.3d 482, 492 (4th Cir. 2013).

216. 408 U.S. 665 (1972).

217. *Sterling*, 724 F.3d at 492.

218. *Id.* at 498.

219. 438 F.3d 1141 (D.C. Cir. 2005).

220. *Id.* at 1147.

221. See *In re Special Proceedings*, 373 F.3d 37, 44 (1st Cir. 2004); *McKevitt v. Pallasch*, 339 F.3d 530, 531–33 (7th Cir. 2003).

222. 18 U.S.C. § 793(d)–(e) (2012).

discuss sensitive topics will refer to these cases in rebuffing a request for background information.²²³

In response to these crackdowns, the most important thing that the judiciary can do is read the First Amendment to provide a reporter's privilege against disclosure of their sources. Finding such a privilege would not be difficult or much of a stretch of the imagination. Today, Wyoming is the only state that has not enacted or adopted a reporters' privilege,²²⁴ while 39 states have enacted specific statutes guaranteeing either a qualified or absolute privilege.²²⁵ In ten states without such laws, the privilege has been recognized in some form or another by the courts.²²⁶ The privilege seems to only be absent in the federal system.

By finding that the First Amendment contains a reporter's privilege, the courts would be ensuring that leakers retain some modicum of protection from executive retaliation. Without a reporter's privilege, leakers face an incredible risk of going to trial for trying to inform the public about various government activities. "Open debate and discussion of public issues are vital to our national health. On public questions there should be uninhibited, robust, and wide-open debate."²²⁷ The judiciary should attempt to foster this debate by quelling the fears of leakers with a constitutionally recognized reporter's privilege.

CONCLUSION

The current classification system has grown out of control and needs to be reined in. For too long the Executive has annexed the power to classify information. And for too long the Executive has held unfettered discretion to both write and enforce the classification of information. Given the extraordinary amount of classified information, and the sharp increase in leak prosecutions, action must be taken to curb the Executive's power to control the flow of information. Congress should enact legislation to put greater restrictions on classifications that also provide better guidance. Congress should also enact legislation that limits the prosecution of leaks to those intended to cause harm to the nation. Furthermore, the judiciary should find a reporter's privilege within the First Amendment to provide leakers some protection from prosecutions. Without action, the problems of the classification system will only become worse. Action must be taken, and it must be taken now.

223. Margaret Sullivan, Op-Ed, *The Danger of Suppressing the Leaks*, N.Y. TIMES, Mar. 9, 2013, at SR12.

224. *United States v. Sterling*, 724 F.3d 482, 532 (4th Cir. 2013) (Gregory, J., dissenting).

225. *Id.* (citing statutes).

226. *Id.* (citing cases).

227. *N.Y. Times, Co. v. United States*, 403 U.S. 713, 724 (1971) (Douglas, J., concurring) (internal quotation marks omitted).