Article

Secrecy's End

Oona A. Hathaway†

† Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School. I served as Special Counsel to the General Counsel at the U.S. Department of Defense in 2014–2015, during which time I held a Top Secret/Sensitive Compartmented Information security clearance. The views expressed in this Article are my own and not those of the U.S. Department of Defense. My thanks to participants in the Yale Law School summer research workshop and the National Security Group workshop for early input on this project. My thanks to Josh Chafetz, Jacob Hacker, Alex Joel, Robert Litt, David Pozen, Scott Shapiro, Tom Tyler, Abraham Wagner, and participants in the Yale Law School Faculty Workshop for helpful input. My thanks, too, to Ty McCormick at *Foreign Affairs* for his input on an article that builds on this one, *The End of Secrecy*. I am grateful to Nicole Ng, Isa Qasim, Mary Ella Simmons, and Emily Wang for their research assistance. I am grateful, too, to Ben Heineman, Stephen Cutler, Michael Solender, and Brad Smith for helpful discussions about how corporations protect their secrets. As always, I am grateful to the Yale Law School librarians, especially Lucie Olejnikova, for their invaluable support. Copyright © 2021 by Oona A. Hathaway.

INTRODUCTION

In 2019, 4,243,937 Americans held security clearances, 1,384,060 of them at the Top Secret level.[1] Together, they produced tens of millions of newly classified documents.[2] For decades, prominent national leaders have lamented the problem of overclassification, and several high-profile efforts to reform the system have sought to tackle it.[3] Both Presidents Bill Clinton and Barack Obama issued executive orders and took other steps that aimed to encourage greater

1. *Fiscal Year 2019 Annual Report on Security Clearance Determinations*, NCSC (April 2020), https://sgp.fas.org/othergov/intel/clear-2019.pdf [https://perma.cc/VX5J-VFMT].

2. *2017 Report to the President*, INFO. SEC. OVERSIGHT OFF. 55 (2017), https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf [https://perma.cc/QJ6D-68KV] [hereinafter *2017 ISOO Report*].

3. *See Examining the Costs of Overclassification on Transparency and Security: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 2 (2016) [hereinafter *Hearings*] (statement of Rep. Jason Chaffetz, Chairman, H. Comm. on Oversight and Gov't Reform) ("Estimates range from 50 to 90 percent of classified material is not properly labeled.").

transparency, discourage overclassification, and encourage declassification.[4] And yet, America's system of keeping secrets is more sprawling, fast-growing, and entrenched today than ever before.

This Article examines this massive system of secrecy, asking what it aims to achieve, whether it serves those ends, and how it could serve them better. Previous accounts have noticed the huge and growing numbers of classified documents. But they have failed to appreciate the dynamics that have made the problem as systemic and difficult to fix as it is. First, existing accounts fail to acknowledge the deeply dysfunctional relationship between the three branches of government in the creation and enforcement of the classification system, nor have they highlighted the xenophobic fears that generated such sweeping prohibitions. Second, many fail to appreciate that addressing the problem of overclassification means shaping the decisions of millions of people who have to make split-second decisions about how to classify a document as part of their daily jobs. Third, most imagine that tackling the problem is about protecting democracy at the cost of national security—and their proposals are accordingly tentative. Fourth and finally, few consider what government might learn from the private sector and the ways in which it keeps secrets without access to a classification system. This Article aims to offer a corrective on all four counts. And it aims to offer new and ambitious proposals for improving the system of government secrecy.

Secrecy has always been part of American governance. Yet this Article traces the history of official secrecy in the United States to show that the now-ubiquitous U.S. national security classification system is a relatively new invention: the interdepartmental system of defense-information markings only began to take shape in 1936—and the modern version emerged in the shadow of World War II. Strikingly, the criminal laws that are used to enforce these classification rules *preceded* those rules. The Espionage Act[5]—which even today is the key statute used to enforce the classification system—was first enacted in 1917, nearly two decades before the classification system

4. Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995); Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009). In 2015, the Office of the Director of National Intelligence issued the *Principles of Intelligence Transparency for the IC* and the *Transparency Implementation Plan*. *Principles of Intelligence Transparency for the Intelligence Community*, OFF. DIR. NAT'L INTEL., https://www.dni.gov/index.php/how-we-work/transparency [https://perma.cc/2S47-XYAW]; *Principles of Intelligence Transparency Implementation Plan*, OFF. DIR. NAT'L INTEL. (Oct. 27, 2015), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf [https://perma.cc/HNH2-XCNY].

5. Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217.

emerged. Support for the Espionage Act was fueled, moreover, by xenophobic wartime fear. From the outset, presidents exercised almost complete control over the classification system, issuing executive orders that set the rules that bind not only those working in the executive branch but anyone who might come into contact with classified information. Indeed, Congress itself has been caught in the vise, unable, for example, to release a report on torture committed by the Central Intelligence Agency (CIA) for years, because the Administration refused to declassify the information it contained.

The system that this classification by executive order has created is not just one in which Congress has played little role. It is also one that leads to ever more secrecy. The system creates incentives that almost always run in the direction of classifying rather than not classifying and classifying at higher levels rather than lower. Data show that new derivative classification decisions (creation of documents that use information that has previously been classified) have skyrocketed since the 1990s. Almost everyone who has examined the system has concluded that the result has been mass overclassification. Former Information Security Oversight Office Director J. William Leonard once opined that, "there's over 50 percent of the information that, while it may meet the criteria for classification, really should not be classified . . . ."[6] Others would put that number much higher.[7] Even Michael Hayden, the former director of the CIA and NSA under President George W. Bush, once complained, "I mean, I got an email saying, 'Merry Christmas.' It carried a Top Secret NSA classification marking."[8]

Though sometimes absurd, those classification markings are nonetheless backed by a mix of potentially harsh criminal, administrative, and civil sanctions. Indeed, unless it had since been declassified at the time he spoke, Hayden's disclosure of the contents of an email marked Top Secret is arguably a prima facie violation of the Espionage Act.[9] In prosecutions for violations of the Act, no court has looked behind a classification marking to determine whether it is justified or not. That is true even though the Act does not criminalize the release

6. *See Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats and Int'l Rel. of the Comm. on Gov't Reform of the U.S. H. of Rep.*, 108th Cong. 83 (2004) (statement of J. William Leonard, Director, Info. Sec. Oversight Off.).

7. *See id.*

8. Mike Giglio, *The U.S. Government Keeps Too Many Secrets*, ATLANTIC (Oct. 3, 2019), https://www.theatlantic.com/politics/archive/2019/10/us-government-has-secrecy-problem/599380 [https://perma.cc/7BAE-FWAS].

9. *See* 18 U.S.C. § 793(d).

of classified information as such—it prohibits the disclosure of "information relating to the national defense."[10] Nonetheless the courts have deferred to classification markings (which, again, did not exist at the time the statute was first written), treating the fact that a document is classified as sufficient to show that a person who had disclosed it "has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation."[11] Hence, in theory, a federal prosecutor could charge Hayden with a violation of the Espionage Act for disclosing the contents of his Top Secret Christmas message. And, indeed, my repetition of his disclosure in this Article is also an unauthorized disclosure and thus potentially a violation itself.[12] Obviously this is an absurd example—no federal prosecutor would ever bring such a case. Nonetheless, that it falls within the formal scope of the Espionage Act, thanks to the courts' deference to the classification system, illustrates the dangers of the current system—and the significant discretion and power that it grants to federal prosecutors.

This system has a deeply damaging effect on our democratic discourse, leaving the public ill-informed, silencing the press, allowing for selective prosecution, and silencing current and former government officials. In 2017, for example, the Department of Defense classified overseas troop counts that it had once routinely made public. When levels were finally disclosed pursuant to a Freedom of Information Act (FOIA) lawsuit, they showed that the Trump administration had not reduced troop levels in Iraq until the very end of his presidency and had not completed a full withdrawal from Syria, despite promises to do so.[13] When the government overclassifies, as it did in this case, the effect is to manipulate the information available to the public in ways many are not even aware of. As the late Senator Daniel Patrick Moynihan once observed, "secrecy is a mode of regulation. In truth, it is the ultimate mode for the citizen does not even know that he or she is being regulated."[14]

---

10. *See* 18 U.S.C. § 793(a).

11. *See* 18 U.S.C. § 793(d)–(e).

12. In my case, it would be a violation of 18 U.S.C. § 793(e), because my access is "unauthorized."

13. *See* Sam Aber, Nicole Ng, Phil Spector & Brandon Willmore, *Just Security Obtains Overseas Troop Counts that the Pentagon Concealed from the Public*, JUST SEC. (Mar. 21, 2021), https://www.justsecurity.org/75124/just-security-obtains-overseas-troop-counts-that-the-pentagon-concealed-from-the-public [https://perma.cc/R27Y-GB9F].

14. *Hearings*, *supra* note 3 (statement of Rep. Jason Chaffetz, Chairman, H. Comm. on Oversight and Gov't Reform) (quoting REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. DOC. NO. 105-2, at xxxvi (1997)).

This threat to democratic values is often treated as an unavoidable trade-off—to enhance democracy we must endanger national security; to enhance national security we must endanger democracy. A key argument of this Article is that this trade-off is mostly illusory. Mass overclassification harms core democratic values *and* hurts national security. Overclassification means we focus less on protecting the secrets that truly require defense; it hinders coordination not just between government and outside actors but also within government; and it puts millions of dedicated public servants in untenable and unrealistic positions. Benjamin Franklin is said to have quipped, "Three may keep a secret, if two of them are dead."[15] That is surely an exaggeration. Nonetheless, it is true that expecting more than *four million* people to effectively keep government secrets may be expecting too much, particularly when a significant number of them work for private contractors, some of whose job is simply to help manage the immense amount of classified information. Perhaps the greatest cost of the system, however, is the way in which it harms the ability of the government to make good decisions. Inventor Charles Franklin Kettering once observed, "When you lock the laboratory door, you lock out more than you lock in."[16] The same is true of government.

If I am right about the corrosive effects of the modern classification system, what should be done about it? To answer that question, this Article poses a thought experiment: What if we declared an end to the costly system of national security information classification? If it has so many pathologies and doesn't effectively achieve the goal it is meant to achieve—protecting national security—then perhaps we should seriously entertain the possibility of dispensing with it altogether. Past efforts at reform have simply sought to tinker with the existing system and have proven largely ineffective. Maybe what we need is a bold idea that will fundamentally reshape the landscape. After all, private business seems to manage to keep secrets—the formula for Coke, for example, remains a famously well-kept secret—so maybe there are other ways to keep our nation's secrets that may not have the same costs.

Although ending the system of government secrecy may seem absurd, considering the possibility forces us to contemplate the real purposes of the classification system. In this way, it serves a function

15. BENJAMIN FRANKLIN, POOR RICHARD'S ALMANACK 51 (Skyhorse Publ'g 2007).

16. JAMES R. NEWMAN & BYRON S. MILLER, THE CONTROL OF ATOMIC ENERGY: A STUDY OF ITS SOCIAL, ECONOMIC, AND POLITICAL IMPLICATIONS 15 (1948).

much like the idea of prison abolition in the work of philosopher Tommie Shelby.[17] Taking the idea of ending the system of secrecy seriously is a way to think about not just what is wrong about the existing system but what is right and valuable about it as well. Indeed, it helps us see that even if we were to end the system of classification, government secrecy would undoubtedly persist. After all, at its core, the system of classification is simply a way to identify who is permitted to access certain information. Likely the main effect of abolishing the system of classification altogether would be to make government secrecy *less* transparent and *less* effective. At the same time, contemplating ending the system of government secrecy allows us to look with new eyes at proposals that may not go all the way to abolition but that are significantly more ambitious than the modest—one might even say meek—reforms of the past.

This Article begins in Part I by examining how we got here—how did the United States go from having no unified system for classifying information at the start of World War II to classifying close to 50 million documents a year? Part II examines the modern system of secrecy. It shows that the system is shaped and governed almost entirely by executive orders from the president backed by criminal statutes mostly enacted by Congress *before* the classification system they enforce even existed. Part III considers the pathologies of the system. The claimed benefits of the system of classification are obvious—it is intended to protect national security. But at what cost? What dangers does the system pose to our democracy—and to national security itself? Part IV considers solutions to the problems outlined in Part III. It begins by asking what would happen if we stopped relying on the

17. *See* TOMMIE SHELBY, THE IDEA OF PRISON ABOLITION (forthcoming 2022). One may say something similar about some of the writing on police abolition. For some, "abolish the police" literally means an end to policing as we know it. For others, it means questioning the overuse of police for a wide range of activities better carried out in other ways. *See, e.g.*, ALEX S. VITALE, THE END OF POLICING (2017); *How Much Do We Need the Police?*, NPR (June 3, 2020), https://www.npr.org/sections/codeswitch/2020/06/03/457251670/how-much-do-we-need-the-police [https://perma.cc/866J-AQLG] ("Well, I'm certainly not talking about any kind of scenario where tomorrow someone just flips a switch and there are no police. What I'm talking about is the systematic questioning of the specific roles that police currently undertake, and attempting to develop evidence-based alternatives so that we can dial back our reliance on them."); Tracey Meres & Gwen Prowse, *Policing as Public Good: Reflecting on the Term "To Protect and Serve" as Dialogues of Abolition*, 73 FLA. L. REV. 1 (2021); Mariame Kaba, Opinion, *Yes, We Mean Literally Abolish the Police: Because Reform Won't Happen*, N.Y. TIMES (June 12, 2020), https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html [https://perma.cc/44ES-QXKE]; MARIAME KABA, WE DO THIS 'TIL WE FREE US: ABOLITIONIST ORGANIZING AND TRANSFORMING JUSTICE (2021).

modern system of classification to protect government secrets. The lessons learned from entertaining this possibility form the foundation for concrete reform proposals that are more ambitious than reforms of the past, including vastly increasing automatic declassification, significantly reducing criminalization for release of national security information (including by creating express protections for journalists), and changing the incentives that face the millions of people who have to make classification decisions as part of their daily work lives.

I. HISTORY OF CLASSIFICATION IN THE UNITED STATES

The current system for classifying government information in order to protect it from disclosure is relatively new. Indeed, as recently as just over a hundred years ago, it was not even a crime to disclose U.S. national security secrets. This Part traces the emergence of our system of classification—showing that it has its origins in xenophobic fears—and that concerns about the emerging system's effects on democratic discourse were raised, and ignored, from the start. It begins by describing the adoption of the first U.S. law to criminalize disclosure of national defense secrets—the 1911 Defense Secrets Act[18]—enacted in no small part because of anxiety over the rise of Japan as a global power and the growing presence of persons of Japanese descent in the United States. On the cusp of U.S. entry into World War I, that law was expanded by adoption of the 1917 Espionage Act, which took aim at the enemy within—those who, in the words of President Woodrow Wilson, were "born under other flags but welcomed under our generous naturalization laws to the full freedom and opportunity of America, who have poured the poison of disloyalty into the very arteries of our national life."[19] This law, which remains in force today, gained new reach and significance with the adoption during World War II of the first uniform and universal U.S. system for classification of information through a presidential executive order. Since then, a series of executive orders has continued the practice of president-directed classification, with the sole exception of Congress's decision to protect secrets relating to the destructive technology of the atomic weapon from the moment it comes into existence. This history provides an essential foundation for understanding the modern system of classification and the many pathologies that it produces.

18. Defense Secrets Act of 1911, Pub. L. No. 61-470, 36 Stat. 1084.

19. Woodrow Wilson, U.S. President, State of the Union Address (Dec. 7, 1915), *in* H.R. DOC. NO. 64-1, at 10–11.

A. AMERICA BEGINS KEEPING OFFICIAL SECRETS

Americans were initially reluctant to sanction secret activities by their government. In 1908, President Teddy Roosevelt's Attorney General, Charles Bonapart, sought to establish a small covert investigative entity in the Department of Justice (DOJ). Kentucky congressman J. Swagar Sherly responded, "If Anglo-Saxon civilization stands for anything, it is for a government where the humblest citizen is safeguarded against the secret activities of the executive of the government."[20]

While the U.S. government had kept secrets since its founding,[21] it did not have any rules protecting "Confidential" communications until the Civil War, and even then the rules were rarely enforced. There was no formal system for marking documents, and there were no official penalties for the release of secret information. It wasn't until the eve of World War I that the United States even had a system for classifying secret documents and punishing their release. In creating the new system for classifying information, the Americans did what they often did when it came to national security: they copied the British, who had invented the idea of government classification of information during the 1850s Crimean War and refined it over the course of the next half century.[22]

Starting in 1853, the British War Office began using three separate markings for documents it wanted to keep secret: "Confidential," "Private Confidential," and "Secret and Confidential."[23] But what these markings meant, exactly, is far from clear—it does not appear that they were understood to signify who could view the documents, how the documents were to be handled, or the penalties that would come from failing to keep the documents secret. It wasn't until the end of

---

20. *See* MONTE REEL, A BROTHERHOOD OF SPIES: THE U-2 AND THE CIA'S SECRET WAR 23 (2018).

21. George Washington is said to have declared in 1777 "There are some secrets, on the keeping of which so depends, oftentimes, the salvation of an army: secrets which cannot, at least ought not to, be entrusted to paper; nay, which none but the Commander-in-Chief at the time should be acquainted with." LYNNE CHENEY, THE VIRGINIA DYNASTY: FOUR PRESIDENTS AND THE CREATION OF THE AMERICAN NATION 69 (2021). But while that was his view, he had no way to enforce it other than keeping information on close hold. *See id.*

22. *See* ARVIN S. QUIST, *Classification in the United States Prior to World War II*, *in* SECURITY CLASSIFICATION OF INFORMATION: INTRODUCTION, HISTORY, AND ADVERSE IMPACTS 9 (2002).

23. *See generally* ADJUTANT-GENERAL'S OFF., THE QUEEN'S REGULATIONS AND ORDERS FOR THE ARMY (1868), https://rnzaoc.files.wordpress.com/2018/08/the-queens-regulations-1868.pdf [https://perma.cc/DLY8-JJK6].

the nineteenth century, with the 1889 British Official Secrets Act,[24] that British law made clear the penalties that would come from improperly disclosing secrets. In the 1890s, British Army regulations established something closer to a modern classification system.[25] Among other requirements, the new rules specified that classified documents were to be marked "Secret" or "Confidential" and enclosed in two envelopes, with the inner envelope containing the classification marking and the outer containing the address to which the document was to be delivered.[26] Not long before World War I, the British added a third classification marking to the other two: "For Official Use Only."[27]

In 1911, the United States adopted the Defense Secrets Act,[28] patterned on the 1889 British Official Secrets Act. This marked the start of a transformation toward a new, more formal system of secret-keeping by the United States government.[29] It also marked a transformation toward greater peacetime militarization. As a Senate report on the law explained, "The necessity for such protection has increased with the growing importance of national preparation-for-war in time of peace."[30] The Russo-Japanese war of a few years earlier had highlighted the new military capacities of nations outside the West, and that clearly had members of Congress worried. "The imperative need of action without further delay," the report explained, "is shown in the great activity of foreign spies in the last few years, particularly on our Pacific coast and insular possessions."[31]

---

24. Official Secrets Act of 1889, 52 & 53 Vic. c. 52 (Eng.).

25. QUIST, *supra* note 22, at 16, 40 n.61 (citing THE QUEEN'S REGULATIONS AND ORDERS OF THE ARMY § XXI, para. 11 (1894)). A draft of the Queen's Regulations and Orders for the Army published in 1889 contains no mention of marking or other classification requirements. *See* WAR OFF., THE QUEEN'S REGULATIONS AND ORDERS FOR THE ARMY: PART I (1889). The Queen's Regulations and Orders for the Army published in 1899 *does* include references to "Secret, Confidential, and other Documents." *See* WAR OFF., THE QUEEN'S REGULATIONS AND ORDERS FOR THE ARMY 356–57 (1899) [hereinafter THE QUEEN'S REGULATIONS AND ORDERS FOR THE ARMY 1899]. This supports the claim that the change took place in the interim.

26. THE QUEEN'S REGULATIONS AND ORDERS FOR THE ARMY 1899, *supra* note 25, at 356.

27. *See* QUIST, *supra* note 22, at 17, 40 n.66 (citing *Army Orders*, London, HMSO, 1910, AO 133/1909, dated May 1, 1909).

28. Act of Mar. 3, 1911, Pub. L. No. 61-470, 36 Stat. 1084 (preventing the disclosure of national defense secrets).

29. Before the passage of the act, there were some limited laws dealing with treason, unlawful entry into military bases, and the theft of governmental property.

30. S. REP. NO. 61-1250, at 1–2 (1911).

31. *Id.* (quoting H.R. REP. NO. 61-1942, at 2 (1911)).

Those fears were intimately tied to race, particularly to anxiety over the rise of Japan as a global power and the growing presence of persons of Japanese descent in the United States. News accounts at the time reflect an intense unease about the security of the U.S. colonial occupying force in the Philippines, where for years there had been reports of Japanese spies.[32] Reflecting racist anxieties of the time, a story in the *Detroit Free Press* with the headline "Jap Spies in Every Nation" claimed that "American army officers assert that the system of espionage in the Philippines has been so extensive that the officials in Tokyo know more about the islands than the war department in Washington."[33]

The fears reflected growing anti-Japanese sentiment in the early 1900s. In 1880, the total Japanese population in the United States was only 148.[34] The Chinese Exclusion Act of 1882[35] and subsequent renewals and extensions meant that Chinese immigration was effectively prohibited until 1943.[36] Japan was not included in the Exclusion Act, probably because Japan prohibited emigration when the Exclusion Act was passed in 1882, and few Japanese had arrived in the U.S. as a result. In 1886, Japan lifted its emigration restrictions, and by 1908, more than 150,000 Japanese immigrants had entered the United States.[37] Beginning in 1908, a host of U.S. laws aimed to restrict and eventually prohibit Japanese immigration and bar Japanese immigrants already present in the country from American citizenship.[38] A 1982 government study of the conditions that led to Japanese internment camps during World War II reported that hostility during this period was fed by economic competition and "racial stereotypes and

32. *See, e.g.*, *Hobson's "Spy" Measure Is Passed by Senate*, WASH. TIMES, Feb. 27, 1911, at 1 ("The bill is made to apply to the Philippines . . . . It is aimed among other things at the efforts of Japanese spies to obtain plans of the Philippine defenses.").

33. Frederic J. Haskin, *Jap Spies in Every Nation: In Guise of Menials They Gain Valuable Information for Mikado*, DETROIT FREE PRESS, Apr. 6, 1908, at 1.

34. COMM'N ON WARTIME RELOCATION AND INTERNMENT OF CIVILIANS, PERSONAL JUSTICE DENIED: REPORT OF THE COMMISSION ON THE WARTIME RELOCATION AND INTERNMENT OF CIVILIANS 30 (1983) [hereinafter COMMISSION ON WARTIME RELOCATION] ("[R]eview[ing] the facts and circumstances surrounding Executive Order Numbered 9066, issued February 19, 1942, and the impact of such Executive Order on American citizens and permanent resident aliens.").

35. Chinese Exclusion Act of 1882, Pub. L. No. 47-126, 22 Stat. 58 (1943).

36. Act of Dec. 17, 1943, Pub. L. No. 78-199, 57 Stat. 600 ("repealing the Chinese Exclusion Acts, establishing quotas, and for other purposes").

37. *See* COMMISSION ON WARTIME RELOCATION, *supra* note 34.

38. *See id.*

fears: the 'yellow peril' of an unknown Asian culture achieving substantial influence on the Pacific Coast or of a Japanese population alleged to be growing far faster than the white population."[39]

It is precisely such fears that led to the very first law in the United States to criminalize spying. It was an incident right out of a spy novel (and might have had just about as much foundation in truth) that finally spurred Congress to act. In April 1910, two officers of a foreign government (unspecified in the account, but almost certainly Japan) offered $25,000 (worth about $650,000 in today's dollars) to an enlisted member of the U.S. Engineer Corps to provide photographs and drawings of U.S. defense installations in the Philippines, which was at the time under the colonial rule of the United States. The enlisted man was the official photographer for the Corps, so no one was concerned when he took photographs of the interior works of the installation on Corregidor Island. After he began taking photographs, he apparently had second thoughts and told his superiors. They ordered him to proceed with negotiations so that the two men who had offered to pay for the photographs could be captured.[40]

The enlisted man met with the foreigners as planned, and, according to a later newspaper account, in "broken English," they said, "You have brought just what we want."[41] Because they had not brought the promised payment with them, they instructed the enlisted man to meet them at 9:00 that evening to deliver the photographs. No sooner had these words been uttered than "the door of the room flew open, and four soldiers rushed in and arrested all three."[42] But the foreign agents did not remain in jail for long. The Attorney General of the Philippines concluded that they could not be prosecuted because there was no U.S. or Philippine law criminalizing their conduct.

It was not just the Philippines. Newspapers reported "Japanese spies roaming about the Philippines, Hawaii, and continental United States, busily making drawings of the location of guns, mines, and other weapons of defense"—all with impunity.[43] Reports of spying came from up and down the Pacific coastline—including Los Angeles,

39. *Id.* at 4.

40. *Bill to Punish Spies Goes Before House*, N.Y. TIMES, Jan. 19, 1911, at 1. The story was recounted along with several similar stories less than two weeks later in a Committee of the Judiciary Report. S. REP. NO. 61-1250, at 3 (1911).

41. *Bill to Punish Spies Goes Before House*, *supra* note 40.

42. *Id.*

43. John Corrigan, *Seeking to Guard Military Secrets*, ATLANTA CONST., Jan. 29, 1911, at A4.

Portland, Oregon, harbors around Puget Sound, and Seattle.[44] Newspapers also detailed the sophisticated Japanese spying operation, including rumors that "agents of the Japanese War Office, in the guise of railroad section laborers or servants in families residing in the locality are stationed at every large railroad bridge on the Pacifica coast."[45]

The stories were fantastic—and few were likely true. The *Detroit Free Press* reported, for example, that a local Hawaiian family hired a Japanese man as a cook, but soon learned that he had little experience in the kitchen. One day while the woman of the house was running errands, she entered a large Japanese bank only to see her "cook," who had come in from another entrance, "instantly surrounded by the bank officials, who treated him with such fulsome respect and deference" that she finally understood why her cook could not cook: "She was harboring a high-class spy under her roof."[46] To this there were added tales of candy store operators who were really map-makers, fishermen who were really taking harbor soundings, and Japanese barbers at a military club in Berlin who reported that the "real opinion of many prominent German officials in regard to Japanese matters was quite the contrary to what had been expressed through diplomatic channels."[47]

To give the government tools to crack down on these supposed legions of spies, the new Act would impose criminal penalties on those who attempted to obtain information to which they were not "entitled" and for communicating such information to unauthorized individuals.[48] As one of the committee reports put it, "To prevent the acquisition of this information, nearly all of the nations of the world with any developed system of national defense, except the United States, have upon their statute books stringent laws under which they can restrain and to a degree prevent spying by inflicting punishment upon persons found guilty. America alone has no such law and our national defense secrets as a consequence have no protection against spies."[49]

The 1911 Act did not define "national defense secrets"; it simply provided that "whoever . . . without proper authority, obtains, takes,

---

44. S. REP. NO. 61-1250, at 2 (1911) (detailing reports received by members of Congress and the War Department of "spying" around the world, including in the Philippines and West Coast of the United States).

45. Frederic J. Haskin, *Japanese Secret Service*, COURIER J. (Louisville), Apr. 6, 1908, at 5.

46. *Id.*

47. *Id.*

48. H.R. REP. NO. 61-1942, at 1 (1911) (preventing the disclosure of national defense secrets).

49. *Id.* at 2.

or makes, or attempts to obtain, take, or make, any document, sketch, photograph, photographic negative, plan, model, or knowledge of anything connected with the national defense to which he is not entitled" as well as anyone receiving or possessing the same could be fined or imprisoned.[50] The law inspired little debate, but one congressman, William Stiles Bennet, asked, "Suppose a tourist going down through the harbor, having a camera, which is not an uncommon thing for tourists to have, should take a photograph of Fort Hamilton or Fort Wadsworth or Fort Lafayette, would that be a violation of this statute?"[51] He was (not entirely convincingly) assured that it probably would not, but "[a]t any rate, there would be a very small penalty."[52] The bill nonetheless passed with unanimous consent.[53]

B. "[W]E COULD NO MORE REPEAL THE CONSTITUTION THAN WE COULD THE LAW OF GRAVITY"

In his 1915 State of the Union address, President Woodrow Wilson appeared before Congress and asked it to strengthen the laws against sedition and disclosure of information:

> I am sorry to say that the gravest threats against our national peace and safety have been uttered within our own borders. There are citizens of the United States, I blush to admit, born under other flags but welcomed under our generous naturalization laws to the full freedom and opportunity of America, who have poured the poison of disloyalty into the very arteries of our national life; who have sought to bring the authority and good name of our Government into contempt, to destroy our industries wherever they thought it effective for their vindictive purposes to strike at them, and to debase our politics to the uses of foreign intrigue . . . . A little while ago such a thing would have seemed incredible. Because it was incredible we made no preparation for it. We would have been almost ashamed to prepare for it, as if we were suspicious of ourselves, our own comrades and neighbors! But the ugly and incredible thing has actually come about, and we are without adequate federal laws to deal with it. I urge you to enact such laws at the earliest possible moment and feel that in doing so I am urging you to do nothing less than save the honor and self-respect of the nation. Such creatures of passion, disloyalty, and anarchy must be crushed out . . . . They have formed plots to destroy property, they have entered into conspiracies against the neutrality of the Government, they have sought to pry into every confidential transaction of the Government in order to serve interests alien to our own.[54]

In 1917, Congress replaced the 1911 Defense Secrets Act with the 1917 Espionage Act—a law that, with a few revisions, still forms the

---

50. Act of Mar. 3, 1911, Pub. L. No. 61-470, 36 Stat. 1084 (preventing the disclosure of national defense secrets).

51. 46 CONG. REC. 2,030 (1911) (statement of Rep. William Bennet).

52. *Id.* (statement of Rep. Richard Parker).

53. *Id.*

54. Wilson, *supra* note 19.

key legal basis for criminal enforcement of unauthorized disclosure of national security information in the United States today.[55] The Act incorporated and expanded the provisions of the earlier law, including the places and items protected. Whereas the earlier law had applied to a person who obtained information "to which he was not lawfully entitled," the 1917 Act applied not only to those who had unlawful access but also to those who lawfully possessed or who had been "entrusted with or having lawful possession or control of" the relevant material or information.[56] The Act also criminalized the making of "false statements with intent to interfere with the operation or success of military or naval forces of the United States or to promote the success of its enemies" when the United States is at war.[57] In short, while the 1911 Act was aimed at foreign spies at home and abroad, the 1917 Act was aimed at the enemy within. Some of the senators debating the bill raised concerns that it was vague and overbroad. They worried in particular that a journalist might easily be swept within the language when engaging in ordinary reporting.[58] Senator John Works, remarked, "If the Czar of Russia should ever see this legislation, if it becomes a law, he would turn green with envy at the extent to which the Government of the United States has gone to close the eye and stop the ears of its citizens against any information as to what the Government is doing."[59]

As the bill was being debated, President Wilson appeared before a joint session of Congress and requested a declaration of war against Germany.[60] Congress approved a Declaration of War with Germany four days later.[61] Three days after that—on Monday, April 9—the House Committee of the Judiciary held a hearing on the espionage bill at which it heard from members of various organizations, including suffragists, labor representatives, and leaders of the peace movement,

55. Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217.

56. *Compare* Act of Mar. 3, 1911, Pub. L. No. 61-470, 36 Stat. 1084 (banning the gathering of information in and around military bases and other property, as well as the dissemination of defense information to those without proper clearance), *with* Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217 (omitting provisions requiring intent to injure the United States or advantage a foreign nation, and publishing improperly gathered or disseminated information).

57. Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217.

58. *See Revision and Strengthening of Espionage, Neutrality, Passport and Shipping Regulations: Hearings Before the H. Comm. on the Judiciary*, 64th Cong. 6 (1917).

59. 55 CONG. REC. 3,586 (1917).

60. President Woodrow Wilson, Joint Address to Congress Leading to a Declaration of War Against Germany (1917).

61. Declaration of War with Germany, S.J. Res. 1, 65th Cong. (1917) (enacted).

worried that the bill would infringe the right of free speech.[62] Mrs. Gertrude Eaton, a professor of English literature, worried that the law was so vague that it might encompass "the person who may write a letter to the New York Times, if the New York Times would publish it, saying that possibly we had fought long enough and that it was about time for peace."[63] She and others testifying that day suggested the senators "insert some clause, whatever you thought best, providing that this be understood as not in any way abridging the right under the Constitution of free speech and assembly."[64]

The senators not only dismissed the concerns; they ridiculed the idea that any statement protecting free speech was necessary. Representative Thaddeus Caraway asked one speaker, "Do you not think it would be looked upon as a joke to pass a law saying that we are not repealing the Constitution? . . . Do you not think people would laugh at us from ocean to ocean?"[65] Louis Lochner, speaking on behalf of the Emergency Peace Federation answered, "I think that while we are living in times of peculiar stress and a singularly excited time that the possibility of making yourselves laughable, gentleman, would be far offset by the greater comfort and aid that you would promote throughout the Nation."[66] Representative Caraway answered, "You know that we could no more repeal the Constitution than we could the law of gravity, and that if we were to insert in the law the fact that we are not going to repeal the law of gravity it would be silly and absurd, if you will pardon me."[67] Shortly thereafter, Congress voted the bill into law with little change.[68]

Far from silly and absurd, the worries would prove prophetic. Two years after the law went into effect, the Supreme Court considered the criminal conviction of Charles Schenck and Elizabeth Baer, members of the Executive Committee of the Socialist Party in Philadelphia, for printing and distributing more than 15,000 fliers to men slated for conscription, urging them not to submit to the draft.[69] In a unanimous opinion written by Justice Oliver Wendell Holmes Jr., the Court concluded that Schenck and Baer were, indeed, guilty of violating Section 3 of the Espionage Act and could be criminally prosecuted

62. *Espionage and Interference with Neutrality: Hearings Before the H. Comm. on the Judiciary on H.R. 291*, 65th Cong. (1917).

63. *Id.* at 11.

64. *Id.* at 9–10.

65. *Id.* at 15.

66. *Id.*

67. *Id.*

68. Espionage Act of 1917, Pub. L. No. 65-24, 40 Stat. 217.

69. Schenck v. United States, 249 U.S. 47, 48–50 (1919).

for it. The restriction did not violate the First Amendment, Holmes held, in circumstances where the expressions were intended to result in a crime and posed a "clear and present danger" of succeeding.[70]

Schenck and Baer were not alone. Presidential candidate Eugene V. Debs gave a speech in 1918 denouncing the Espionage Act. He was prosecuted for violating the Act he criticized and was sentenced to ten years in jail. Debs challenged his conviction on First Amendment grounds, but the U.S. Supreme Court upheld the decision, citing its earlier decision in *Schenck*.[71] He was only released from jail in 1921, after President Warren G. Harding commuted his sentence to time served.[72]

The section of the Act under which Schenck, Baer, and Debs were convicted was separate from the portions of the Act dealing with disclosure of national security information.[73] But the Supreme Court's decisions made clear that the Act authorized restrictions on dissemination of information that might otherwise run afoul of the First Amendment. The Court's embrace of the "clear and present danger" standard opened the door to restrictions based on national security concerns.[74]

With criminal penalties in place for disclosure of information relating to national security, and the Supreme Court prepared to accept restrictions on dissemination of information for national security purposes, the last piece of the puzzle that would set the stage for the modern national security state's regulation of information fell into place.

---

70. *Id.* at 52.

71. Debs v. United States, 249 U.S. 211, 211 (1919) (holding that Debs's First Amendment defense was disposed of for the same reasoning expressed in *Schenck*).

72. *Harding Frees Debs and 23 Others Held for War Violations*, N.Y. TIMES, Dec. 24, 1921, at 1, 4.

73. They were convicted under Section 3 of the Act. *See Debs*, 249 U.S. at 211; *Schenck*, 249 U.S. at 48. That Section was further strengthened by the Sedition Act of 1918, which was then repealed after the war. *See* Sedition Act of 1918, Pub. L. No. 65-150, 40 Stat. 553, 553–54 (expanding Section 3 to cover a broader range of activities, including expression of negative opinions about the government or the war effort, and interfering with the sale of government bonds).

74. The "clear and present danger" standard was later displaced by the more-speech-protective incitement doctrine. *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) ("[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.").

C. WHAT IS A SECRET?

Now there were rules allowing criminal prosecution of those who disclosed national security secrets (or, as the Espionage Act put it, "information respecting the national defense" that could be "used to the injury of the United States").[75] But what was such a secret? The answer would be provided by the executive branch, first working through the military branches in a disorganized and decentralized manner but eventually moving toward the massive, centralized classification machine that we have today.

After its entry into World War I, the U.S. military adopted rules for classifying information that once again mirrored the British system. American Expeditionary Force General Order No. 64, issued November 21, 1917, is reportedly the first attempt by the United States government to adopt a formal classification system.[76] It specified rules for the use of "Confidential" and "Secret" designations, making clear that "secret matter will be kept under lock and key subject to use only by the officers to whom it has been transmitted."[77] Confidential matter would be "similarly cared for unless it be part of office records."[78] Even then the order directed that "the file shall be locked except during office hours."[79] The order further provided rules for marking such documents, for their circulation, and for maintaining their security. The War Department regulations that followed shortly thereafter largely followed the template set by the General Order. They specified, moreover, that those who failed to follow the regulations would be subject to punishment under the Articles of War or under the 1917

75. Espionage Act of 1917, Pub. L. No. 65-21, § 1, 40 Stat. 217, 217.

76. *See* QUIST, *supra* note 22, at 24. An earlier War Department General Order issued in 1912 provided that records determined to be "confidential" were to be kept under lock, "accessible only to the officer to whom intrusted." *Safe-Keeping of Military Records Concerning Seacoast Defenses*, *in* COMPILATION OF GENERAL ORDERS CIRCULARS AND BULLETINS OF THE WAR DEPARTMENT 216 (1916) (originally published in WAR DEPARTMENT GENERAL ORDERS NO. 3 (Feb. 1912)). All confidential materials were issued serial numbers, which were marked on the documents. Lists of these serial numbers were kept at the offices from which they emanated. *Id.* This filing system was not, however, widely used. *See* Harold C. Relyea, *Government Secrecy: Policy Depths and Dimensions*, 20 GOV'T INFO. Q. 395, 397 (2003) (stating that very few soldiers had duties subjecting them to General Order No. 3); HAROLD C. RELYEA, CONG. RSCH. SERV., RL33494, SECURITY CLASSIFIED AND CONTROLLED INFORMATION: HISTORY, STATUS, AND EMERGING MANAGEMENT ISSUES (Mar. 8, 2007).

77. James G. Harbord, General Orders No. 64, *in* HEADQUARTERS AMERICAN EXPEDITIONARY FORCES, EXTRACTS FROM GENERAL ORDERS 13, 13 (1918).

78. *Id.*

79. *Id.*

Espionage Act—the first effort to expressly leverage the criminal penalties in that Act to enforce later-issued executive branch classification orders.[80]

In the period between World War I and World War II, the Navy and Army adopted their own regulations on classified information, producing a mish-mash of classification rules across the branches. That changed on the eve of World War II. In 1938, Congress enacted a revision to the Espionage Act making it unlawful "to make any photograph, sketch, picture, drawing, map, or graphical representation" of certain "vital military or naval installations or equipment" the president found to be in the interests of national defense, without obtaining proper permission.[81] To give effect to the statute's protections, President Franklin D. Roosevelt signed the very first executive order regulating classified information in the United States in March 1940, a mere six months after Adolf Hitler invaded Poland.[82] The order was not limited to the bounds of the 1938 statute. It went beyond it to encompass:

> [A]ll official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications which are now marked under the authority or at the direction of the Secretary of War or the Secretary of the Navy as 'secret,' 'confidential,' or 'restricted' and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.[83]

The structure of modern government information security thus came into being during the period between the start of World War I and the end of World War II: Congress enacted laws providing criminal penalties for the release of information relating to the national defense. But it left it to the president to determine what information met that standard. The president, in turn, initially left the determination to the various military services. But with the unification of the services under a single umbrella of the new post-Second World War Department of Defense, it shifted to a centralized, top-down classification scheme. That scheme would be outlined in a series of executive orders. In the course of the last several decades, Congress has almost entirely ceded authority over classification to the president.[84] As we shall see,

---

80. *See* QUIST, *supra* note 22, at 25.

81. Act of January 12, 1938, ch. 2, §§ 1–5, 52 Stat. 3, 3–4 (codified at 18 U.S.C. §§ 795–97).

82. Exec. Order No. 8,381, 5 Fed. Reg. 1,147, 1,147–48 (Mar. 22, 1940) ("Defining Certain Vital Military and Naval Installations and Equipment").

83. *Id.* § 3.

84. Presidents have increasingly claimed plenary authority to regulate classified information. *See* Statement on Signing the Foreign Relations Authorization Act, Fiscal

Congress has occasionally come to rue its decision to effectively grant the president a blank check to criminalize national security information.

There was, and remains, only one significant exception to the blank-check approach: the terrible new destructive technology of the nuclear bomb.

D. CLASSIFIED AT BIRTH

In June 1942, President Roosevelt authorized the initiation of a project that aimed to produce an atomic bomb before the end of the war. The project, run by the Army Corps of Engineers and headquartered in New York City, would come to be known as the Manhattan Project. Colonel (soon Brigadier General) Leslie Groves was charged with running the project, and he quickly assembled the scientific and construction teams needed to launch the program.[85]

The importance of secrecy was obvious from the start. Restriction of information about atomic energy began with the scientists themselves, who voluntarily restricted publication of their scientific work once they realized the implications of the weapon their research might make possible.[86] A number of the scientists doing research in the area were émigrés or refugees from Europe and were concerned that Nazi Germany, where the initial discovery of nuclear fission had been made, would use the results of their work.[87] The Manhattan Project, as it would come to be known, was kept secret, even from many

---

Years 1992 and 1993, 2 PUB. PAPERS 1344 (Oct. 28, 1991) ("The mandatory public disclosure of some of these [diplomatic] activities would be inimical to the success of U.S. foreign policy, and I shall therefore interpret this provision consistent with my constitutional authority to protect such information."); Statement on the Intelligence Reform and Terrorism Prevention Act, 3 PUB. PAPERS 3118 (Dec. 17, 2004) (objecting to certain sections of the 2004 Intelligence Reform and Terrorism Prevention Act, on the grounds that they impeded on presidential authority); Statement on Signing the Consolidated Appropriations Act, 2017, DAILY COMP. PRES. DOC. 2 (May 5, 2017) ("The President's authority to classify and control access to information bearing on the national security flows from the Constitution and does not depend upon a legislative grant of authority.").

85. Cynthia C. Kelly, *An Unprecedented Alliance*, *in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS 69 (Cynthia C. Kelly ed., 2007).

86. ENRICO FERMI, THE CHICAGO PILE-1: THE FIRST CHAIN REACTION, *reprinted in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 82.

87. Cynthia C. Kelly, *Explosive Discoveries and Bureaucratic Inertia*, *in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 17–18.

of those working on it: only a small number of the 150,000 people employed on the Manhattan Project knew that they were working on the production of an atomic bomb.[88] Many only learned the purpose of their work after the United States dropped the first atomic bomb on Hiroshima, Japan, on August 6, 1945.[89]

Scientific discovery is by nature a collaborative enterprise. Those who engage in it, particularly those who engage in the basic science of the kind that gave rise to this new form of nuclear technology, tend to reside largely in universities, where those who do the work are also there to share what they know—with their students and colleagues. Academic scientists are accustomed to moving quickly to publish information about new discoveries. Indeed, there are significant professional benefits to be gained from being the first to get a new discovery into print.

Launching a secret government program that aimed to explore a new frontier of science meant transforming—or at least altering—the process of scientific inquiry itself. The head of the Manhattan Project, J. Robert Oppenheimer, was a theoretical physicist and professor of physics at the University of California, Berkeley. He traveled from university to university—Princeton, Berkeley, Chicago, MIT, and Cornell—to recruit promising scientists, particularly those already working on nuclear research.[90] This group of brilliant scientists agreed not to publish any of their discoveries until after the war. But more than that, the government "erected invisible walls round every branch of research, so that no department ever knew what any other was doing."[91]

For many scientists involved in the project, the level of secrecy imposed on their work was alien. The security procedures were anathema to Edward Condon, a leading professor of physics at Princeton recruited by Oppenheimer to serve as associate director. Shortly after Condon joined the project, Oppenheimer and Condon traveled to Chicago, where they discussed the production schedule for plutonium with the director of the Project's Metallurgical Lab. After learning of

88. ROBERT JUNGK, SWIMMING IN SYRUP, *reprinted in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 93.

89. Cynthia C. Kelly, *Secret Cities*, *in* The MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 156.

90. STEPHANE GROUEFF, A NEW AND UNCERTAIN ADVENTURE IN THE WILDERNESS, *reprinted* in THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 157.

91. JUNGK, *supra* note 88, at 93.

the trip, General Groves reprimanded Oppenheimer and Condon for what he considered a dangerous security breach. Oppenheimer didn't flinch, but Condon was so outraged that he promptly resigned his position—a mere six weeks after starting. In his resignation letter to Oppenheimer, he stated, "I feel so strongly that this policy puts you in the position of trying to do an extremely difficult job with three hands tied behind your back."[92] If they could not meet with collaborators without violating security, he argued, "I would say the scientific position of the project is hopeless."[93]

Condon was not the only scientist who worried that science and secrecy were a poor mix. Many worried that imposing secrecy on science could be futile—since most "secrets" could be replicated in other places with scientific expertise. Secrecy could be harmful because restricting the free flow of ideas could slow the rate of scientific discovery. After all, scientists are accustomed to learning through exchange. Yes, there are often cases in which they keep parts of their research secret for a time, but the ultimate goal is generally publication within a relatively short timeframe. The program of scientific exploration at the Project ran directly counter to this standard scientific approach. Oppenheimer aimed to overcome this problem by draining much of the intellectual firepower out of the universities and pouring them into the Project.[94] Scientists could not share information with those outside the project, but collaboration was encouraged internally—at least within each piece of the project. Indeed, for many of those involved, it was the opportunity to work closely with so many of their fellow scientists that attracted them to the project in the first place.

After the successful detonation of the nuclear bomb, many concluded that the information was just too dangerous to be made public. Indeed, there were a number of Soviet spies active in Los Alamos.[95] Their work was likely made easier by Oppenheimer's rejection of Groves' effort to compartmentalize all of the work of the scientists working on the project—preventing any one scientist on the project from understanding enough to compromise the project as a whole. Oppenheimer believed that scientific progress would proceed more

92. KAI BIRD & MARTIN SHERWIN, APPEASING GENERAL GROVES, *reprinted in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 137.

93. *Id.*

94. GROUEFF, *supra* note 90, at 157.

95. *Interview with Lilli Hornig on "The Story with Dick Gordon," reprinted in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 250 (discussing Los Alamos scientists and Soviet spies Klaus Fuchs and David Greenglass).

quickly if the scientists on the project had a sense of the overall project, and he arranged weekly seminars at which the scientists shared their findings with one another. Oppenheimer was proven right: the group produced a weapon in record time.[96] But Groves would prove prescient, as well.[97]

In 1946, stunned and terrified by the destructive power of atomic energy, Congress enacted the Atomic Energy Act.[98] It was the first—and, aside from its successor statute in 1954, the only—U.S. statute to establish a program for restricting the dissemination of an entire category of information. As one contemporary commentator put it, "The Act creates a government monopoly of the sources of atomic energy and buttresses this position with a variety of broad governmental powers and prohibitions on private activity."[99] Under the Act, information relating to atomic energy is restricted from birth, no matter its source. No decision need be made to render relevant information classified; "all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power" is "Restricted Data" from the moment it comes into existence.[100] That provision, with some modifications,[101] remains in force today.

On 29 August, 1949, the Soviet Union secretly conducted its first successful nuclear weapon test at the Semipalatinsk Test Site in Kazakhstan.[102] The design of the bomb was based directly on the American "Fat Man" design for a plutonium bomb—the detailed plans for

96. JOSEPH ALBRIGHT & MARCIA KUNSTEL, HOLES IN THE SECURITY FENCE, *reprinted in* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 265.

97. *See id.* at 264–65 (stating that, as Groves suspected, lack of compartmentalization made penetration of Los Alamos by spies easier).

98. *See* Atomic Energy Act of 1946, Pub. L. 79–585, § 10, 60 Stat. 755, 766–68 (1946).

99. NEWMAN & MILLER, *supra* note 16, at 4.

100. ARVIN S. QUIST, *Classification Under the Atomic Energy Act*, *in* SECURITY CLASSIFICATION OF INFORMATION: INTRODUCTION, HISTORY, AND ADVERSE IMPACTS 87 (2002).

101. Specifically, "Restricted Data" is defined as: "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142." Atomic Energy Act of 1954, Pub. L. 83-703, ch. 2 § 11(r), 68 Stat. 919, 924 (codified at 42 U.S.C. § 2014(y)).

102. *Detection of the First Soviet Nuclear Test, September 1949*, NAT'L SEC. ARCHIVES (Sept. 9, 2019), https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2019-09-09/detection-first-soviet-nuclear-test-september-1949 [https://perma.cc/SK8G-GAJX] (discussing the United States' detection of the first Soviet test of a nuclear device at Semipalatinsk).

which Soviet spies had obviously stolen.[103] The efforts to keep the information about the bomb out of Soviet hands had proven ineffective; the United States no longer had unilateral control over nuclear weapons technology.[104] Whether that was inevitable given the size and geographic dispersion of the Manhattan Project—and the nature of scientific inquiry—is far from clear. The detonation of the two nuclear bombs in Japan in 1945 proved to the Soviets that such a weapon was possible. The stolen information accelerated the development of a nuclear weapon by the Soviets, but they were arguably on track to develop a bomb even in the absence of insights gained by espionage. What is clear is that the system of classification developed for the Manhattan project was just the beginning.

II. THE MODERN SYSTEM OF SECRECY

In the years after World War II and the embarrassing and devastating nuclear espionage by the Soviets, the United States developed the system of classification that continues to this day. This Part describes how that system, which relies almost entirely on executive orders from the president, backed by criminal statutes enacted by Congress (the most important of them the previously discussed 1917 Espionage Act), emerged and grew. It explains the rapid expansion of classified information—which in recent years has led to around 50 million new classified documents every year. Finally, it describes how this system is enforced.

A. CLASSIFICATION BY EXECUTIVE ORDER

In the post-World War II era, the classification rules have been made almost exclusively by presidents through unilateral executive orders. The Atomic Energy Act is the only significant congressional statute to address classification of information. For the most part, Congress has chosen to defer to the president when it comes to the regulation of information security. Presidents set the rules governing

103. It would later become clear that the spy was Klaus Fuchs, a German theoretical physicist who had worked on the Manhattan Project. *See* THOMAS C. REED & DANNY B. STILLMAN, THE NUCLEAR EXPRESS: A POLITICAL HISTORY OF THE BOMB AND ITS PROLIFERATION 30–33 (2009); *cf.* Robert S. Norris, Jeremy Bernstein & Peter D. Zimmerman, *An Uncertain Train of Nuclear Events*, 16 NONPROLIFERATION REV. 293, 294 (2009) (book review) ("Espionage by Klaus Fuchs . . . helped the Soviet Union produce a bomb more quickly.").

104. *See generally* THE MANHATTAN PROJECT: THE BIRTH OF THE ATOMIC BOMB IN THE WORDS OF ITS CREATORS, EYEWITNESSES, AND HISTORIANS, *supra* note 85, at 247–66 (collecting excerpts discussing the advancements made by the Soviet nuclear program because of spies within the Manhattan Project).

the designation of individuals permitted to receive restricted information and the handling of classified security information, including marking, transmission, storage, and destruction—backed by congressional statutes giving them the force of law with criminal penalties.

As noted in Part I, President Franklin D. Roosevelt initiated the practice of regulating classification rules through executive order when he issued Executive Order 8,381 in March 1940, to give effect to authority granted by Congress to define "certain vital military and naval installations or equipment as requiring protection against the general dissemination of information."[105] After the war, in February 1950, President Harry Truman, drawing on the same specific statutory authority, issued Executive Order 10,104, which added a fourth security classification—Top Secret—to the then-existing three (Restricted, Confidential, and Secret).[106] In 1951, Truman issued Executive Order 10290,[107] replacing the diverse regulations the services had adopted with new rules on classification that were to be applied throughout the executive branch. This time, the Order dropped any reference to any particular statute, referencing instead "the authority vested in me by the Constitution and statutes, and as President of the United States."[108]

Presidents have periodically updated and revised these rules over the years by issuing new executive orders, but the essential structure has remained consistent.[109] It is worth pausing here to notice that this is a breathtaking fact: nearly *all* of the modern rules regarding classification of information are contained in an executive order, *not* in legislation. Congress has played no role in generating or shaping these orders—as a rule, executive orders become effective upon signature of the president alone.[110] Executive orders do not ap-

105. Exec. Order No. 8,381, 5 Fed. Reg. 1,147 (Mar. 22, 1940) ("Defining Certain Vital Military and Naval Installations and Equipment").

106. Exec. Order No. 10,104, 3 C.F.R. 82 (1950).

107. Exec. Order No. 10,290, 3 C.F.R. 471 (1951).

108. *Id.*

109. Since Truman issued Executive Order 10,290 in 1951, Presidents have issued the following orders: Exec. Order No. 10,501, 3 C.F.R. 115 (1953) (Dwight D. Eisenhower); Exec. Order No. 11,652, 3 C.F.R. 375 (1972) (Richard Nixon); Exec. Order No. 12,065, 3 C.F.R. 190 (1978) (Jimmy Carter); Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (Apr. 2, 1982) (Ronald Reagan); Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995) (Bill Clinton); Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 5, 2003) (George W. Bush); Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009) (Barack Obama).

110. Congress's creation of FOIA in 1966 is critiqued by some as acknowledging, if

pear anywhere in the Constitution, nor does any provision in any statute authorize them. Indeed, there is no formal definition of an executive order.[111] The Federal Register Act requires that executive orders and proclamations be published in the Federal Register.[112] An executive order issued in 1962 established some rules regarding the form, routing, and publication of executive orders—an executive order on executive orders![113]

Executive orders cannot exceed the president's own constitutional authority or usurp Congress's.[114] The president may use executive orders to do what the president is already able to do—such as regulate the activities of the executive branch—but not to increase the power of the office. This also means that there's nothing stopping the president from revising or even revoking an order on a moment's notice (and even in secret).[115] The practice of governing the classification of information through executive order has been accepted in significant part because the executive orders have generally been regarded as restricted to matters within the president's exclusive and independent constitutional authority. After all, classification rules formally only directly govern the behavior of those in the executive

not blessing, the system of classification by executive order, giving up on the opportunity of engaging in real reform. *See* David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1121–22 (2017) ("In [opting for the indirect FOIA model] Congress effectively blessed the modern classification regime for the first time."); SAM LEBOVIC, FREE SPEECH AND UNFREE NEWS 188 (2016) ("In 1966, in its Freedom of Information Act, Congress did not challenge the legitimacy of the classification system, but acknowledged it.").

111. *See* VIVIAN S. CHU & TODD GARVEY, CONG. RSCH. SERV., RS20846, EXECUTIVE ORDERS: ISSUANCE, MODIFICATION, AND REVOCATION 2 (2014) ("[T]here is no definition of executive orders . . . .").

112. 44 U.S.C. § 1505(a)(1).

113. *See* Exec. Order No. 11,030, 3 C.F.R. 610 (June 19, 1962) ("Preparation, Presentation, Filing, and Publication of Executive Orders and Proclamations").

114. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638 (1952) (Jackson, J., concurring) (stating that where a president "takes measures incompatible with the expressed or implied will of Congress" the "[c]ourts can sustain exclusive presidential control in such case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution").

115. The Brennan Center for Justice explains the basis for believing that there are secret modifications to executive orders not disclosed to the public. As its report on "secret law" puts it, "The tacit modification or waiver of published orders is one of the most pernicious forms of secret law. Not only are members of the public unaware of the true state of the law; they are actively misled, as the law that has been modified or waived remains, unaltered, on the books." *See* Elizabeth Goitein, *The New Era of Secret Law*, BRENNAN CTR. FOR JUST. 35–36 (2016), https://www.brennancenter.org/sites/default/files/2019-08/Report_The_New_Era_of_Secret_Law_0.pdf [https://perma.cc/R3QC-RT6H].

branch. But, as we shall see, despite this formal limit, the rules have had an impact far beyond the executive branch itself.

Today, the classification of government documents containing national security information is governed by Executive Order 13,526.[116] It is the last in a very long line of executive orders that have, since the 1950s, regulated the executive branch's treatment of national security information, each modestly tweaking the standards for classification up or down.[117] Issued by President Obama in 2009, the current Order lays out three levels of classification: Top Secret, Secret, and Confidential. Officials classify information as Top Secret when its unauthorized disclosure "reasonably could be expected to cause exceptionally grave damage" to an area of national security "that the original classification authority is able to identify or describe."[118] The second-highest classification level, Secret, is applied to information when its unauthorized disclosure "reasonably could be expected to cause serious damage" to national security.[119] The lowest level, Confidential, is applied to information when its unauthorized disclosure "reasonably could be expected to cause damage" to national security.[120] In addition, there are Special Access Programs, including "Sensitive Compartmented Information" (SCI).[121] SCI clearance is sometimes referred to as "above Top Secret," but that is not quite right:

116. Exec. Order No. 13, 526, §§ 2.1–2.2, 75 Fed. Reg. 707, 712 (Dec. 29, 2009) (setting forth rules for use of derivative classification and classification guides). There are a number of other orders and memoranda that help guide information policy. *See*, *Policy Documents*, INFO. SEC. OVERSIGHT OFF. https://www.archives.gov/isoo/policy-documents [https://perma.cc/S573-C56K].

117. Eisenhower, Nixon, and Carter each revised the system—changing definitions, developing standards for declassification, and outlining security measures for storage and communication of sensitive information. For the most part, these orders restricted the scope of classified information. That trend reversed with President Ronald Reagan's executive order, issued in 1982, which struck some of the earlier limitations added by his predecessors, removed classification time limits, and provided for reclassification of previously declassified material. Exec. Order No. 12, 356, 47 Fed. Reg. 14,874 (Apr. 2, 1982). In 1995, Clinton, in turn, reintroduced time limits on classification and provided higher standards for classifying documents. Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995). In 2003, the Bush administration yet again reversed some of these changes, among other things giving the vice president original classification authority and eliminating language favoring declassification. Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 5, 2003); *see* ARVIN S. QUIST, *Classification Under Executive Orders*, *in* SECURITY CLASSIFICATION OF INFORMATION: INTRODUCTION, HISTORY, AND ADVERSE IMPACTS 58–69 (2002).

118. Exec. Order No. 13,526, § 1.2(a)(1), 75 Fed. Reg. 707 (Dec. 29, 2009).

119. *Id.* § 1.2(a)(2).

120. *Id.* § 1.2(a)(3).

121. Special Access Programs, 32 C.F.R. § 154.17(b) (2012).

information at any classification level may be SCI if it falls within a designated compartment.

The background investigation for SCI access is the same as for Top Secret access, so they are often written together as "TS/SCI." But Top Secret access does not automatically qualify a person for SCI access. For that, a person must be granted specific access to the compartment (which requires a specific "need to know") and "SCI indoctrination," often referred to as being "read in" to the program.[122] Programs, in turn, are generally known by their designated codeword, which is itself classified.

Under the order, there are two ways that a document can become classified. One is that a person designated as an "original classification authority" (OCA) decides that information should be classified and gives it a classification designation.[123] This authority belongs in the first instance to a relatively elite group of twenty-eight leading government officials, including the vice president, chief of staff to the president, secretary of state, secretary of the treasury, secretary of defense, attorney general, and director of the CIA.[124] Each of these twenty-eight may, in turn, delegate their classification authority to subordinates that "have a demonstrable and continuing need to exercise this authority."[125] The latest figure of the number of people with original classification authority is 1,867.[126] OCAs are empowered to classify information that they determine "requires protection because unauthorized disclosure of that information could reasonably be expected to damage the national security."[127] They classify such information as Top Secret, Secret, or Confidential, mark the document to indicate its classification level, and choose the date at which the information will be declassified.[128]

---

122. For more on the "need to know," "SCI indoctrination," and other requirements for SCI access, see U.S. DEP'T OF DEF., NO. 5105.21, SENSITIVE COMPARTMENTED INFORMATION (SCI) ADMINISTRATIVE SECURITY MANUAL, 11–14 (2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m_vol3.pdf?ver=2020-09-15-132603-533 [https://perma.cc/YBY8-5MPR].

123. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

124. *Id.* at 708.

125. *Id.*

126. *2017 ISOO Report*, *supra* note 2, at 1.

127. *2016 Report to the President*, INFO. SEC. OVERSIGHT OFF. 3 (2016), https://www.archives.gov/files/isoo/reports/2016-annual-report.pdf [https://perma.cc/Y6PH-GD3J] [hereinafter *2016 ISOO Report*].

128. *Id.*

These OCAs classified around 58,501 documents in 2017.[129] That may sound like a lot, but it is dwarfed by the other form of classification: derivative classification. Derivative classification happens when a new document is created that uses information that has already been classified.[130] In 2017, the last year for which data is available (the office in the National Archives tasked with collecting the data stopped publishing it shortly after Donald Trump became president), some 4,030,625 individuals were cleared to access classified information and could potentially be derivative classifiers.[131] That year, more than forty-nine million documents were derivatively classified.[132]

Obama's executive order contains some restrictions meant to discourage overclassification. It states, "If there is significant doubt about the appropriate level of classification, [the information] shall be classified at the lower level,"[133] and, "If there is significant doubt about the need to classify information, it shall not be classified."[134] The order also places some limits on the types of information that may be classified.[135] Moreover, before designating information as classified, an OCA must be "able to identify or describe the damage" to national security

129. These figures are from the Information Security Oversight Office's 2017 annual report to the president. *See 2017 ISOO Report*, *supra* note 2, at 8. I use "2017" to refer in shorthand to "FY 2017." FY 2017 was not actually calendar year 2017, but was instead October 1, 2016, through September 30, 2017.

130. This happens when individuals with security clearances—who need not be OCAs—"reproduce, extract, or summarize" information that is already considered classified. Exec. Order No. 13,526, 75 Fed. Reg. 707, 712 (Dec. 29, 2009).

131. To be exact, 2,831,941 were designated "eligible (in access)," meaning that they "were briefed into access to classified information," and 1,198,684 were declared "eligible (not in access)," meaning that they were "determined eligible due to the sensitivity of their positions and the potential need for immediate access to classified information, but may not have actual access to classified information until the need arises." Nat'l Counterintelligence & Sec. Ctr., *Fiscal Year 2017 Annual Report on Security Clearance Determinations*, OFF. OF THE DIR. OF NAT'L INTEL 4–5 (2018), https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf [https://perma.cc/HG5J-W4YN].

132. *2017 ISOO Report*, *supra* note 2, at 9.

133. Exec. Order No. 13,526, 75 Fed. Reg. at 707–08. This provision was in the earlier executive order issued by President Bill Clinton but was stripped in the executive order issued by President George W. Bush. *See* Exec. Order No. 12,958, 60 Fed. Reg. 19,825, 19,826 (Apr. 17, 1995); Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 28, 2003).

134. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

135. *Id.* at 709.

that unauthorized disclosure could inflict.[136] The executive order forbids classification in order to "conceal violations of law, inefficiency, or administrative error" or to "prevent embarrassment" to a person or agency.[137] Yet, as one former government official put it, "the evidence is that it just has had little impact. The people buried in the system continue to do just what they want and are seldom held accountable."[138]

A final word about Congress's access to classified information under this executive order regime: together with the president and vice president, and Article III judges, members of Congress are not required to hold a security clearance to have access to classified information. They have access instead by virtue of the constitutional offices they hold.[139] Their staff, however, must obtain security clearances and sign nondisclosure agreements just like executive branch officials in order to be eligible for access to classified national security information, and they are not eligible for interim clearances—meaning delays in obtaining access can be lengthy.[140] Moreover, SCI is organized, as the term suggests, into "compartments," with access available only to those who need to know that information; TS/SCI clearance is not sufficient—and this applies to members of Congress as well as their staff. Who determines "need-to-know" is a source of ongoing tension between Congress and the executive branch. Congress maintains that it makes this determination, but the executive branch maintains that "need-to-know" is determined by the agency where the information

136. *Id.* at 707; *see* Elizabeth Goitein & David M. Shapiro, *Reducing Overclassification Through Accountability*, BRENNAN CTR. FOR JUST. 13 (2011), https://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf [https://perma.cc/3X7Y-4U8J].

137. Exec. Order No. 13,526, 75 Fed. Reg. at 710 (Dec. 29, 2009); *see* Goitein & Shapiro, *supra* note 136, at 13.

138. E-mail from Abraham Wagner, former official at Nat'l Sec. Council, Off. of the Dir. of Cent. Intel. & Dep't of Def., to author (June 8, 2021) (on file with Minnesota Law Review).

139. Mandy Smithberger & Daniel Schuman, *A Primer on Congressional Staff Clearances*, PROJECT ON GOV'T OVERSIGHT (Feb. 7, 2020), https://www.pogo.org/report/2020/02/a-primer-on-congressional-staff-clearances [https://perma.cc/53UU-X9A6]; FREDERICK M. KAISER, CONG. RSCH. SERV., RS20748, PROTECTION OF CLASSIFIED INFORMATION BY CONGRESS: PRACTICES AND PROPOSALS 8 (2011).

140. Off. of S. Sec., 110th Cong., UNITED STATES SENATE SECURITY MANUAL, at 8 (Apr. 2007); H.R., 117th Cong., RULES OF THE HOUSE OF REPRESENTATIVES, R. XXIII, cl. 13 (2021); KAISER, *supra* note 139; MICHELLE D. CHRISTENSEN, CONG. RSCH. SERV., R43216, SECURITY CLEARANCE PROCESS: ANSWERS TO FREQUENTLY ASKED QUESTIONS 9 (2016).

originated.[141] Since executive branch agencies are the ones in possession of the information, that effectively means the executive branch controls access to all compartmented information—even when members of Congress wish to disclose the information to other members or to their staff.

B. MASS OVERCLASSIFICATION: SECRECY BEGETS MORE SECRECY

Nearly everyone agrees that there is too much information classified by the government. So why hasn't the problem been fixed before now—and why do things appear to have become worse, not better, in recent decades? One reason is that the incentives for everyone involved in the process almost always run in the direction of classifying up, rather than down (that is, to move from unclassified to classified and from lower levels of classification to higher ones). The personal and professional penalties for getting it wrong by overclassifying are dwarfed by the professional penalties for getting it wrong by underclassifying.

Max Weber noted that every bureaucracy seeks to increase its power and influence by keeping its work secret.[142] The philosopher Sissela Bok agrees: "Concealment insulates administrators from criticism and interference; it allows them to correct mistakes and to reverse direction without costly, often embarrassing explanations; and it permits them to cut corners with no questions being asked."[143] Because it has these advantages, she points out, it has a tendency to spread within agencies and executive departments. This spread, moreover, increases the chances of abuse.

I saw these dynamics firsthand while working briefly at the Pentagon in a job with Top Secret clearance. I quickly learned that secrecy is the easiest course, and secrecy begets more secrecy. When I sat down at my desk to write a memo or even just an email, I had to decide at the outset whether it would be unclassified, classified Secret, or classified Top Secret. Depending on which I chose, the memo or email

---

141. Smithberger & Schuman, *supra* note 139; *Classified Information Nondisclosure Agreement: Briefing Booklet 5*, INFO. SEC. OVERSIGHT OFF. 5 (2001), https://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf [https://perma.cc/W5JH-BXEC] ("The holder of classified information to which you seek access is responsible for confirming your identity, your clearance, and your 'need-to-know.'").

142. MAX WEBER, FROM MAX WEBER: ESSAYS IN SOCIOLOGY 233 (H.H. Gerth & C. Wright Mills eds. & trans., 1946); *see also* HAROLD L. WILENSKY, ORGANIZATIONAL INTELLIGENCE: KNOWLEDGE AND POLICY IN GOVERNMENT AND INDUSTRY (1967) (discussing secrecy in bureaucracies).

143. SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 177 (1989).

had to be written on a different computer system—because the three systems are entirely separate. I could not, for example, email a document from my unclassified account to my secret account or vice versa. Moving a document to a higher level of classification was slow and cumbersome; moving it down was near to impossible.

Most important, if I got it wrong by classifying the document too highly, there would likely be no penalty. No one in the offices I worked with was, to my knowledge, ever disciplined for classifying a document at too high a level.[144] Classifying a document or email too low, however, could bring serious professional consequences—not to mention potentially threaten U.S. national security. The last thing anyone working in national security wants to do is inadvertently reveal information that may damage national security. This alone creates significant pressure toward higher levels of classification. And all of the work in these offices is conducted under significant time constraints, so I, like everyone I worked with, had to make a decision about how to classify a document or email in a split second. There was no time to carefully weigh the pros and cons. So, when I sat down at the desk, the incentives all ran in the direction of erring by choosing the higher level of classification for everything I wrote.

Time constraints also operate to push toward higher classification in another way: when it comes to email, there is much less "junk" to wade through on the classified systems. When sending a message that one wants very busy people to notice, sending it on a classified system increases the chance that it will get attention—or at least not get lost among the seemingly endless notifications of parking lot closures and lunchtime events that clutter the unclassified system. As one former government official put it to me, some officials "tend to mark things with the highest level of classification possible, on the assumption that more attention will be paid to them."[145] This same official also noted that "officials, military and others with authorized access to classified materials tend to believe what they are reading is true or correct. The corollary to this is that the higher the level of classification, and the more special markings on a document, the even better the information must be."[146] But, he cautioned, "This is often wrong and can be disastrous." The classification generally indicates how the

144. This is not true in every job with classified access. Where there is need for interoperability with persons who do not have classified access, for instance, that creates a significant pressure to classify downward.

145. E-mail from Abraham Wagner to Oona Hathaway, *supra* note 138.

146. *Id.*

information was obtained—but there is no guarantee that "people intercepted were correct or even telling the truth."[147]

The pressures pushing toward higher classification also stem from the requirement that a document must be classified at the highest level of classification of any information that it contains. So, if a ten-page memo contains a single sentence at the Top Secret level, then the entire document must be classified at the Top Secret level. Put concretely, if I read a Top Secret document containing information about the latest activities of a terrorist group, for instance, and I wanted to incorporate a single relevant fact into a memo I was writing about the legal authority to use force against that group, the legal memo had to be classified as Top Secret. That is true even if *all* of the rest of the memo contained no classified information at all (unless the document is "portion marked").[148] This is the essence of the derivative classification spillover problem—and it is at least part of the reason for massive, and accelerating, overclassification.

My experience is not unusual. As the chart below shows, the number of newly classified derivative classification decisions rose from around 23 million in 2008 to a high of 95 million in 2012, before falling back to around 50 million in 2015, where it remained through 2017.[149] (The Information Security Oversight Office (ISOO) ceased publishing the relevant data after issuing the 2017 report.) It is worth noting that each of these data points reflects the aggregate number of "decisions" in a given year, without identifying which agencies made

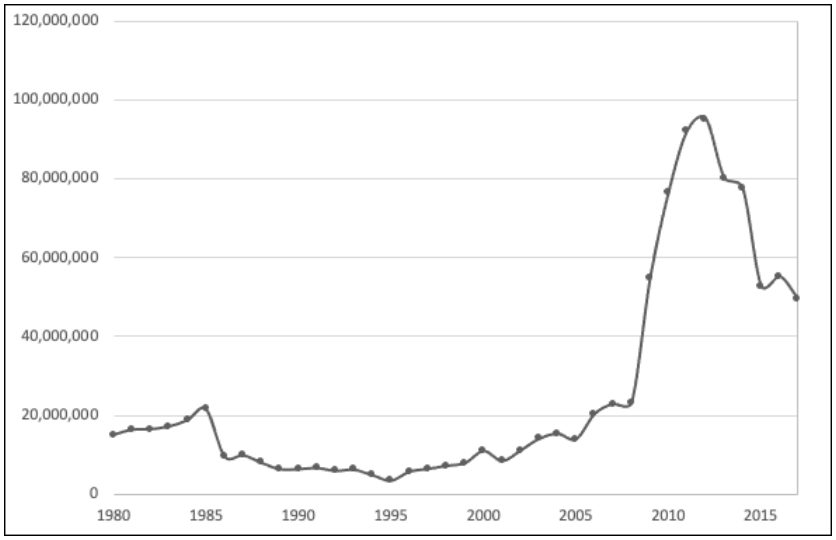
147. *Id.*

148. Each portion in a classified document is supposed to be portion marked, meaning that each portion is marked with the proper level of classification. 32 C.F.R. § 2001.21(c) (2001); *see* Exec. Order 13,526, 70 Fed. Reg. 707, 710 (Jan. 5, 2010). If this is done, then if the borrowed sentence is from an unclassified portion of the original document, then the new document would not need to be classified. However, the 2016 ISOO report found that the most frequent marking discrepancy in the 752 classified documents it reviewed was "the absence of some or all portion markings." *2016 ISOO Report*, *supra* note 127, at 19.

149. *ISOO Annual Report Archive*, INFO. SEC. OVERSIGHT OFF. (June 28, 2021), https://www.archives.gov/isoo/reports/annual-report-archive.html [https://perma.cc/UK6B-KQ7P]. A good portion of the spike from 2008–2009 reflects a change in methodology for counting derivative classification actions. The 2009 ISOO report explains that before the change, only finished products were counted, but the new guidance focuses on "classification decisions wherever they might occur." The report notes that "Agencies reported a total of 54.7 million derivative classification actions in FY 2009, a 135 percent increase from the 23.2 million derivative actions reported in FY 2008. As noted above, "the increase is largely attributed to more accurate data provided by agencies using the revised guidance that better captured existing activity." *2009 Report to the President*, INFO. SEC. OVERSIGHT OFF. 7–8 (2009), https://www.archives.gov/files/isoo/reports/2009-annual-report.pdf [https://perma.cc/N4RF-7JZM].

the decisions or the length or importance of the documents involved. As imperfect as this data is, it is the best that is currently publicly available.

FIGURE 1: NEW DERIVATIVE CLASSIFICATION DECISIONS, 1980–2017[150]



One might think that this problem can be combated with better training, and perhaps it could be ameliorated that way. But a mathematical model suggests that the gravitational pull not only to classification, but to the highest level of classification, is unavoidable given the basic structural features of the classification system. The Bell–La Padula Model is a mathematical model developed by David Elliott Bell

150. All data is from the ISOO's archive of annual reports, 1979–2017. *ISOO Annual Report Archive*, *supra* note 149. The 2018 report is brief and contains no relevant classification or declassification data; the same is true of the 2019 and 2020 reports. As a result, there is no public information on what happened regarding classified documents under President Trump. It is worth noting that we do not know the total number of documents generated by the government during these time periods and thus whether the increase in the absolute number of classified documents reflects a percentage increase or not. It is also worth noting that the number of *original* classification decisions and the number of original classification authorities have both seen much less growth—and even declines—over this same period. One would expect that to drive declines in derivative classification decisions, but that does not seem to have occurred.

and Leonard J. La Padula in the mid-1970s to formalize multilevel security policy.[151] Their aim was to figure out how to set up a computer system with different levels of security. Though it was funded by the U.S. Department of Defense, the goal was not limited to national security applications—it was meant to apply to any computer system with different levels of access. As Bell would later put it in an interview,

> [W]e viewed it that what we needed to do was to be able to address any computer system so we had to hit that balance that would be not too specific and not too general because we figured you needed a tool. We'd seen what we thought they needed was a way of analyzing, addressing, assessing a real computer system. So we went off to try to figure that out.[152]

The model followed two basic axioms: first, the simple security rule, "which states that a subject cannot read information for which it is not cleared," and second, the *-property, "which states that a subject cannot move information from an object with a higher security classification to an object with a lower classification ("no write down")."[153] These features describe the modern U.S. national classification system. And what Bell and La Padula found might not be a surprise to anyone who has studied the U.S. system: everything drifted to the highest level ("System High" in their model).[154]

The process of declassification can't possibly keep up with the speed at which new classified documents are generated. When a document is classified, the classifier must designate the date on which the document will automatically become declassified.[155] President

---

151. David Elliott Bell, *Bell-La Padula Model*, *in* ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (Henk C.A. van Tilborg & Sushil Jajodia eds., 2011).

152. Charles Babbage Inst., *Interview with David Elliott Bell Conducted by Jeffrey R. Yost*, CTR. FOR HIST. INFO. TECH. 15–16 (Sept. 24, 2012), https://conservancy.umn.edu/bitstream/handle/11299/144024/oh411deb.pdf [https://perma.cc/R92N-82MP].

153. Carl E. Landwehr, Constance L. Heitmeyer & John McLean, *A Security Model for Military Message Systems*, 2 ACM TRANS. ON COMPUT. SYS. 198, 201 (1984).

154. Bell, *supra* note 151, at 22.

155. Exec. Order No. 13,526, 75 Fed. Reg. 707, 709 (Dec. 29, 2009). Declassification has been something of a political football over the last seventy years. In Presidents Truman's and Eisenhower's executive orders, declassification was an afterthought. Exec. Order No. 10,290, 3 C.F.R. 471, 475 (1951); Exec. Order No. 10,501, 3 C.F.R. 115, 116–17 (1953). President John F. Kennedy's executive order stated that a goal of the order was to "preserve the effectiveness and integrity of the classification system and to eliminate classifications of information or material which no longer require classification protection." Exec. Order No. 10,964, 26 Fed. Reg. 8,932 (Sept. 22, 1961). But even that order applied automatic declassification to only a small fraction of classified documents. Nixon's order added a provision requiring that any document exempted from automatic declassification be subject to mandatory review after ten years, if there was a request for declassification. In the absence of a request, information would be

Obama's Executive Order states that this date should be ten years or less from the date of classification, unless "the sensitivity of the information requires" that it be classified for up to twenty-five years.[156] Under the Order, "[n]o information may remain classified indefinitely,"[157] but in practice, declassification can be a time-consuming process. Often, agencies insist on reviews to ensure that the information does not fall under an exception to automatic declassification, a process that may take years.[158]

To hurry that process along, President Obama's Order created a National Declassification Center, which adopted the motto: "Releasing All We Can, Protecting What We Must."[159] All it can is unfortunately not all that much. Its declassification work, while important, has paled

---

declassified after thirty years, unless the head of the originating Department personally determined in writing that continued protection of the document was "essential to the national security." Exec. Order No. 11,652, 3 C.F.R. 375, 380, 382 (1972). President Jimmy Carter's order kept Nixon's presumption toward declassification but stated that information that still met the classification requirements despite the passage of time should remain classified. Exec. Order No. 12,065, 3 C.F.R. 190, 196 (1978). President Reagan then rolled back many of the earlier orders' transparency measures, including eliminating automatic declassification. Exec. Order No. 12,356, 47 Fed. Reg. 14,874, 14,876 (Apr. 6, 1982). That approach remained until President Bill Clinton issued an order that mirrored Carter's earlier policy on declassification. Exec. Order No. 12,958, 60 Fed. Reg. 19,825, 19,827–29 (Apr. 17, 1995). Congress then intervened to require page-by-page review of all classified documents in case those documents might have information about nuclear or atomic material; only if the documents "have been determined to be highly unlikely to contain" such information could they be declassified. 50 U.S.C. § 2672(b)(1). Congress acted soon after Dr. Wen Ho Lee was convicted only of one (improper handling of restricted data) out of the original 59 counts against him for stealing secrets about the U.S. nuclear arsenal for the People's Republic of China. *See Report on the Government's Handling of the Investigation and Prosecution of Dr. Wen Ho Lee*, SUBCOMM. ON DEP'T OF JUST. OVERSIGHT, SENATE COMM. ON THE JUDICIARY (Dec. 20, 2001), https://irp.fas.org/congress/2001_rpt/whl.html [https://perma.cc/JL6Y-PD84]. George W. Bush's approach to declassification largely reflected Clinton's but it changed the 10-year default for declassification to a 25-year default. Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 28, 2003).

156. Exec. Order No. 13,526, 75 Fed. Reg. 707, 709 (Dec. 29, 2009).

157. *Id*. at 709.

158. *See* Elizabeth Goitein, *The Government Is Classifying Too Many Documents*, NATION (July 7, 2016), https://www.thenation.com/article/the-government-is-classifying-too-many-documents [https://perma.cc/VDW2-PELB]; Rosa Brooks, *Automatic for the People: How to End Obama's Culture of Secrecy in Just a Few Lines of Code*, FOREIGN POL'Y (May 20, 2013), https://foreignpolicy.com/2013/05/30/automatic-for-the-people [https://perma.cc/9SD8-JMKJ]; Matthew Connelly & Richard H. Immerman, *What Hillary Clinton's Emails Really Reveal*, N.Y. TIMES (Mar. 4, 2015), https://www.nytimes.com/2015/03/04/opinion/what-hillary-clintons-emails-really-reveal.html [https://perma.cc/8FG6-JMRL].

159. David Ferriero, *Releasing All We Can, Protecting What We Must*, NAT'L ARCHIVES: AOTUS BLOG (Jan. 7, 2016), https://aotus.blogs.archives.gov/2016/01/07/releasing-all-we-can-protecting-what-we-must-3 [https://perma.cc/B5HC-FTHS].

in comparison to the number of new classified documents created on a daily basis. In the first quarter of 2020, for instance, it released a list of 206 entries that completed declassification processing between October 1 and December 31, 2019.[160] The total of all declassified textual materials adds up to 1,754.394 cubic feet of material. Assuming 2,000 pages to 1 cubic foot of declassified material, that means roughly 3.5 million declassified pages. Even so, that pales in comparison to the number of documents undoubtedly classified during that same period—given recent historical rates, that's likely at least 12.5 million new *documents* (not pages). The Center's project is a bit like trying to empty a tub with a thimble while the faucet is still on full blast.

This recent experience is not an aberration. The 2017 ISOO report found that the process of declassification, which generally requires individual page-by-page review of documents, "cannot meet the demands imposed by large volumes of paper records needing timely review, let alone the deluge of electronic records already well underway."[161] There is, moreover, a massive backlog in Mandatory Declassification Review—the process by which an individual or entity can request a federal agency to review classified information for declassification—due largely to inadequate funding and technology.[162] The process is further slowed by the fact that those conducting the review are extremely risk-averse, resulting in what ISOO rightly calls an "unacceptably low" declassification rate.[163] This, once again, reflects the incentive structure for those making classification (or, in this case, declassification) decisions: there is little penalty for keeping information classified and lots of peril in improperly declassifying information that should have been kept secret.

Congress is in no small part responsible for the current state of affairs. In 1998, Congress adopted an amendment that terminated all automatic declassification authority activity for several months while

160. *List of Records Released During Fiscal Year 2020 Quarter 1*, NAT'L DECLASSIFICATION CTR., U.S. NAT'L ARCHIVES & RECS. ADMIN., https://declassification.blogs.archives.gov/wp-content/uploads/sites/16/2020/01/FY2020-Q1-Release-List-PDF-Format.pdf [https://perma.cc/B32H-E3EX].

161. *2017 ISOO Report*, *supra* note 2, at 15; *see also* Goitein & Shapiro, *supra* note 136, at 17–18 (describing how, after the process's 1995 creation by President Clinton, Congress added a page-by-page review process for many documents).

162. *2017 ISOO Report*, *supra* note 2, at 16–18*; see also* S. DOC. NO. 105-2, at 61 (1997) (discussing why some agencies conduct successful declassification programs while others do not).

163. *2017 ISOO Report*, *supra* note 2, at 15.

a "plan to prevent the inadvertent release of records containing Restricted Data" was developed.[164] That amendment was followed by an amendment a year later that required review of previously declassified documents.[165] The National Archives objected, arguing that it would "serve to bring cost-effective declassification to a halt,"[166] a warning that Congress largely ignored. Why the sudden lockdown? The Department of Energy had accidentally declassified and released information relating to the U.S. nuclear program. It led to finger pointing and backlash against declassification efforts, the effects of which are still felt today.[167] As John Powers, Associate Director for Classification Management, Information Security Oversight Office, explained, "Agencies got a lot more conservative after that. It slowed things down a lot and led them to be a lot more conservative overall. And that applied not just to nuclear secrets. There had been a presumption of openness, but that has not carried forward."[168] Agencies, moreover, became even more risk averse after the 9/11 attacks—no one wanted to be responsible for releasing information that might be seen as aiding the enemy. Combine this risk averse impulse with the requirement of resource-intensive page-by-page review, and ever-increasing numbers of newly classified materials coming into the system every year, and the predictable result is a huge—indeed insurmountable—declassification backlog.[169]

The situation is further slowed by the growth of FOIA requests over the same period. The subject matter experts in the agencies that review FOIA requests are often the very same people that are tasked to review documents for declassification purposes. The total number of FOIA requests received by the federal government grew from 644,165 in 2011 to 858,952 in 2019—a thirty-three percent increase

164. Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261, § 3161(a), 112 Stat. 1920, 2259–61 (1998).

165. National Defense Authorization Act for Fiscal Year 2000, Pub. L. No. 106-65, § 3149, 113 Stat. 512, 938 (1999).

166. Letter from John W. Carlin, Archivist of the U.S., to James C. Murr, Assistant Dir. for Legis. Reference, Off. of Mgmt. & Budget (July 14, 1998) https://fas.org/sgp/clinton/carlin0798.html [https://perma.cc/KUY7-UKDB].

167. *See* Letter from Kenneth E. Baker, Principal Deputy Dir., Off. of Nonproliferation and Nat'l Sec., to James C. Murr, Assistant Dir. for Legis. Reference, Off. of Mgmt. & Budget (July 24, 1998) https://fas.org/sgp/clinton/baker0798.html [https://perma.cc/7DJC-8HAG].

168. Telephone Interview with John Powers, Assoc. Dir. for Classification Mgmt., Info. Sec. Oversight Off. (Sept. 24, 2018).

169. *Id.*

over eight years.[170] That means that two spigots are running at once, not just one.

This, at least, is not a secret. After an extensive study of the classification system and discussions with stakeholders, the Public Interest Declassification Board—a committee established by Congress to advise the president on classification and declassification policy—concluded in 2012 that "the current classification system is fraught with problems. . . . [I]t keeps too many secrets, and keeps them too long; it is overly complex; it obstructs desirable information sharing inside of government and with the public."[171] Former Secretary of State John Kerry stated in 2015 that "there's a massive amount of overclassification" in the current system.[172] He continued: "People just stamp [a classification marking] on quickly because it's a way to sort of be correct if anybody had a judgement that somehow they had been wrong about whether it should be classified or not . . . the easy thing is to classify it and put it away."[173] Former Secretary of Defense Donald Rumsfeld, too, once stated, "I have long believed that too much material is classified across the federal government as a general rule."[174] And at a hearing in late 2016, Jason Chaffetz, the Chairman of the House of Representatives Committee on Oversight and Government Reform, noted that fifty to ninety percent of classified material is not properly labeled.[175] These problems are far from new. Indeed, in 1997, a commission led by Senator Moynihan concluded that it was time "for a new way of thinking about secrecy."[176] Secrecy, the commission concluded, "is a form of government regulation," but what is different from other forms of government regulation is that "the public cannot know the extent or content of the regulation."[177]

---

170. *Summary of Annual FOIA Reports for Fiscal Year 2019*, U.S. DEP'T OF JUST. 2 (2020), https://www.justice.gov/oip/page/file/1282001/download [https://perma.cc/XH63-B5C8].

171. Pub. Int. Declassification Bd., *Transforming the Security Classification System*, U.S. NAT'L ARCHIVES & RECS. ADMIN 2 (2012), https://www.archives.gov/files/declassification/pidb/recommendations/transforming-classification.pdf [https://perma.cc/M2VV-AYA3].

172. Mark Hensch, *Kerry: State Has 'Massive Amount of Overclassification,'* HILL (Sept. 4, 2015), https://thehill.com/blogs/ballot-box/presidential-races/252769-kerry-state-has-massive-amount-of-overclassification [https://perma.cc/YH5N-D6BV].

173. *Id.*

174. Goitein & Shapiro, *supra* note 136, at 1.

175. *Hearings*, *supra* note 3, at 2 (statement of Rep. Jason Chaffetz, Chairman, H. Comm. on Oversight and Gov't Reform).

176. S. DOC. NO. 105-2, at xxi (1997).

177. *Id.*

The excessive secrecy, the Commission found, not only undermined public understanding of the policymaking process; it also undermined trust in government and made it harder, not easier, to keep secrets. "Secrets," it concluded, "can be protected more effectively if secrecy is reduced overall."[178]

The Commission's first recommendation—one of several not implemented—was that Congress enact "a statute that sets forth the principles for what may be declared secret."[179] As the report noted, a system built exclusively on executive orders "inevitably degrades."[180] Among other things, the new statute would provide that all information would be declassified after thirty years, "unless it is shown that demonstrable harm to an individual or to ongoing government activities will result from release."[181] The problem, Moynihan himself noted, "is that organizations within a culture of secrecy will opt for classifying as much as possible, and for as long as possible."[182]

He was, of course, correct. After the Commission issued its report, the essential outlines of the system of government secrecy remained largely unchanged and the number of classified documents continued to grow.

C. ENFORCEMENT

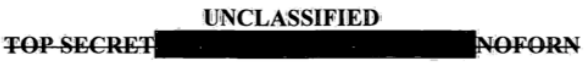
How is it that the executive orders issued by the president have force? After all, they are not laws in the traditional sense. So how is it that these elaborate rules of classification have bite? Most important, how do they have any effect outside the executive branch itself? It makes sense that those working in the executive branch would follow the rules. But why does anyone else?

The puzzle is perhaps best illustrated by the standoff between the Senate Intelligence Committee and the CIA over the Committee's intent to release a report it had prepared about the CIA's extensive program of detaining terrorism suspects in black sites located around the world and subjecting many of those held to cruel, inhumane, and degrading treatment and torture. The 6,300-page report was completed in 2012, but it was not released until December 2014—with redactions.[183] Why the holdup? The report, as journalist Jane Mayer de-

178. *Id.*
179. *Id.* at xxii.
180. *Id.*
181. *Id.* at xxiii.
182. *Id.* at xxxix.
183. S. REP. NO. 113-288 (2014).

scribed it in 2013, "threatens to definitively refute former C.I.A. personnel who have defended the program's integrity."[184] The CIA didn't like the report, but that alone shouldn't have prevented its release. Yet the CIA managed to assert control over the decision to declassify the report—even after the Senate Committee voted 11-3 to release significant portions.[185] It was only after the CIA was deeply embarrassed by news that it had penetrated a computer network used by the Senate Committee in preparing its report that the agency finally relented and—several months later—cleared the several-hundred-page executive summary for release, along with the CIA's own 112-page response.[186]

It appears likely that the report was not only Top Secret, but it contained compartmented information and therefore was classified to be accessed only by those with access to the appropriate compartment. The now-unclassified version of the report contains this header:



The blacked-out portion of the header between "TOP SECRET" and "NOFORN" (meaning "no foreign nationals") almost certainly contains still-classified compartment identification information. As noted above, members of the Senate do not need security clearance to view classified information themselves, but they do need to be granted access to view compartmented information. Moreover, if they were to release classified information to the public, they could be criminally prosecuted under the Espionage Act or one of the many other criminal sanctions that exist to enforce the rules (more on that below). An exception is that members of Congress almost certainly are protected from criminal prosecution for disclosures made on the floor of the

184. Jane Mayer, *Top C.I.A. Lawyer Sides with Senate Torture Report*, NEW YORKER (Sept. 26, 2013), https://www.newyorker.com/news/news-desk/top-c-i-a-lawyer-sides-with-senate-torture-report [https://perma.cc/7U23-3ZWK].

185. Spencer Ackerman, *Senate Committee Votes to Declassify Parts of CIA Torture Report*, GUARDIAN (U.K.) (Apr. 3, 2014), https://www.theguardian.com/world/2014/apr/03/senate-votes-declassify-cia-torture-report [https://perma.cc/RMR2-SFXC].

186. Mark Mazzetti & Carl Hulse, *Inquiry by C.I.A. Affirms It Spied on Senate Panel*, N.Y. TIMES (July 31, 2014), https://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html [https://perma.cc/33BG-4Z8V]; Greg Miller, Adam Goldman & Julie Tate, *Senate Report on CIA Program Details Brutality, Dishonesty*, WASH. POST (Dec. 9, 2014), https://www.washingtonpost.com/world/national-security/senate-report-on-cia-program-details-brutality-dishonesty/2014/12/09/1075c726-7f0e-11e4-9f38-95a187e4c1f7_story.html [https://perma.cc/T8P5-SJXY].

House or Senate by the Speech or Debate Clause of the Constitution.[187] Senator Dianne Feinstein took advantage of that protection when in 2014 she called out the CIA for impeding and interfering with the Senate Intelligence Committee's investigation of CIA torture program, to counter suggestions that Committee staff had mishandled classified materials in its investigation,[188] and to call for declassification of the Senate's report.[189]

This episode illustrates how the classification rules that formally apply through executive order only to the executive branch nonetheless have far-reaching effects even on Congress—and, we shall see, journalists, scholars, former government employees, and even the public at large. To explain why and how, this Section explores the various tools deployed to enforce the classification rules: criminal sanctions, administrative sanctions, and civil sanctions.

1. Criminal Sanctions

There is no single criminal law statute that governs classified information. There is, instead, a patchwork of statutes, as summarized in Table 1—the modern iteration of the Espionage Act chief among them. The problem is that these statutes were never really meant to govern improper storage or transmission of classified information of the kind, for example, Secretary of State Hillary Clinton was accused of during the 2016 campaign—or the intentional leaks of classified information of the kind carried out by Edward Snowden (more on that

187. "[F]or any Speech or Debate in either House, [the Senators and Representatives] shall not be questioned in any other Place." U.S. CONST. art. I, § 6, cl. 1; *see* Eastland v. U.S. Servicemen's Fund, 421 U.S. 491, 502–03 (1975) ("Thus we have long held that, when it applies, the Clause provides protection against civil as well as criminal actions, and against actions brought by private individuals as well as those initiated by the Executive Branch."). As Josh Chafetz has shown, members of Congress have failed to take much advantage of their immunity under the Speech or Debate Clause. JOSH CHAFETZ, CONGRESS'S CONSTITUTION 201–31 (2017).

188. It later became clear that the lead investigator for SSCI, Daniel Jones, had, in fact, improperly and intentionally removed classified materials from a secured room. He later explained he was concerned the documents would be destroyed and took "full responsibility." Spencer Ackerman, *Inside the Fight to Reveal the CIA's Torture Secrets*, GUARDIAN (U.K.) (Sept. 9, 2016), https://www.theguardian.com/us-news/2016/sep/09/cia-insider-daniel-jones-senate-torture-investigation [https://perma.cc/3XXF-PQ3G]. Jones was never prosecuted. *Id.*

189. *Transcript: Sen. Dianne Feinstein Says CIA Searched Intelligence Committee Computers*, WASH. POST (March 11, 2014), https://www.washingtonpost.com/world/national-security/transcript-sen-dianne-feinstein-says-cia-searched-intelligence-committee-computers/2014/03/11/200dc9ac-a928-11e3-8599-ce7295b6851c_story.html [https://perma.cc/5USF-6B3H].

later).[190] As explained earlier, they were really focused on preventing spying or theft of government property by foreign adversaries—first Japan and later the Soviet Union.

TABLE 1: KEY CRIMINAL STATUTES FOR DISCLOSURE OF CLASSIFIED INFORMATION[191]

Statute	Topic	Penalty	Famous Example, if any
18 U.S.C. § 641	Prohibits the theft or conversion of government property or records for one's own use or the use of another	"Shall be fined under this title or imprisoned not more than ten years, or both"	Daniel Ellsberg was charged with violating this statute and 18 U.S.C. § 793
18 U.S.C. § 793-98 (Espionage Act)	§ 793. Gathering, transmitting or losing defense information § 794. Gathering or delivering defense information to aid foreign government § 795. Photographing and sketching defense installations § 796. Use of aircraft for photographing defense installations § 797. Publication and sale of photographs of defense installations § 798. Disclosure of classified information	§ 793 & § 798: "Shall be fined under this title or imprisoned not more than ten years, or both." § 794: "shall be punished by death or by imprisonment for any term of years or for life." §§795-97: "shall be fined under this title or imprisoned not more than one year, or both"	Reality Winner was convicted under § 793; Julian Assange has been charged under § 793
18 U.S.C. § 952	Prohibits the willful publication or distribution of diplomatic codes by government employees	"shall be fined under this title or imprisoned not more than ten years, or both"	

190. *See infra* text accompanying note 238.

191. Other potentially relevant statutes include 18 U.S.C. § 371 ("Conspiracy to commit offense or to defraud United States") and 18 U.S.C. § 1905 ("Disclosure of confidential information generally").

18 U.S.C. § 1030(a)(1)	Punishes the willful retention and communication of classified information retrieved by means of a computer in excess of authorization, with reason to believe that such information "could be used to the injury of the United States, or to the advantage of any foreign nation."	"a fine under this title or imprisonment for not more than ten years, or both"	Nathan Van Buren (Supreme Court Case argued Nov. 30, 2020, still undecided)
18 U.S.C. § 1924	Prohibits unauthorized removal and retention of classified documents or material	"shall be fined under this title or imprisoned for not more than five years, or both"	General Petraeus, Director of the CIA
18 U.S.C. § 2071	Prohibits unauthorized concealment, removal, or mutilation of "any record, proceeding, map, book, paper, document, or other thing"	"shall be fined under this title or imprisoned not more than three years, or both"	
Atomic Energy Act of 1954, 42 U.S.C. §§ 2274	Prohibits disclosure of information relating to nuclear energy and weapons	shall be "punished by a fine of not more than $50,000 or imprisonment for not more than ten years, or both"	

Atomic Energy Act of 1954, 42 U.S.C. § 2277	Prohibits disclosure of Restricted Data	"shall, upon conviction thereof, be punishable by a fine of not more than $12,500"	
50 U.S.C. §§ 421	Prohibits disclosure of identities of undercover intelligence officers, agents, informants, and sources	"shall, upon conviction thereof, be punishable by a fine of not more than $12,500"	
50 U.S.C. § 783	Penalizes government officers or employees who, without proper authority, communicate classified information to a person who the employee has reason to suspect is an agent or representative of a foreign government."	"a fine of not more than $10,000, or imprisonment for not more than ten years," or both and ineligible for future position of trust	Irvin C. Scarbeck[192]
Intelligence Identities Protection Act (IIPA), 50 U.S.C. § 3121	Prohibits intentional disclosure of identifying information of cover intelligence operatives	Fine and/or 3-15 years of imprisonment, depending on particular violation.	

Two provisions of the Espionage Act have proven especially problematic. As originally written, the Espionage Act applied the same provisions to anyone who lawfully or unlawfully had information relating to the national defense.[193] Subsequent revisions separated the rules that applied to those who lawfully possess information from those who unlawfully obtained that information. The revised statute provides that anyone with *lawful access* to 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

192. Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1963).
193. Pub. L. No. 65-24 § 1(d), 40 Stat. 217, 218 (1917).

receive it" can be held criminally responsible.[194] The same is true if they "through gross negligence" permit such information to be removed.[195]

Now there are a few things to notice here. This statute applies only to someone who has *lawful* access to the classified information. Moreover, there are a lot of required mental elements to the crime. It is not enough to simply take some information out of the office. The possessor must "[have] reason to believe" that the information could be used to the injury of the United States or advantage of any foreign nation.[196] How would a prosecutor or a court know if the person had reason to believe that the document could be used in this way? This is where the classification rules often come into play: *Courts almost always assume that if the information was classified, then the accused must have had "reason to believe could be used to the injury of the United States or to the advantage of any foreign nation*."[197] If it has been classified, the reasoning goes, the government has determined that its release poses a threat to national security. And anyone who has a security clearance has been briefed on the importance of not disclosing the information to which they have access, because doing so can harm national security. Courts have thus almost entirely deferred to the executive branch's decision to classify a piece of information in determining whether its intentional release might be a criminal act. Courts have been entirely unreceptive to arguments that the information was improperly classified.[198] If it was classified, the courts generally don't inquire further. Indeed, thus far, no defendant has successfully challenged a prosecution on the grounds that the disclosed information was improperly classified.[199]

194. 18 U.S.C. § 793(d).

195. *Id.* § 793(f).

196. *Id.* § 793(d).

197. *Id.* (emphasis added).

198. *See, e.g.*, Fondren v. United States, 63 F. Supp. 3d 601, 608–09 (E.D. Va. 2014) ("[T]he Petitioner simply cannot defend himself from charges of illegally transmitting a classified report by arguing that the information should not have been classified . . . . Other courts have rejected improper classification as a defense . . . ."); United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979) ("The fact of classification of a document or documents is enough to satisfy the classification element of the offense."). Senator Benjamin Cardin proposed an amendment to the Espionage Act in 2011 that would have added a "Defense of Improper Classification," but it was not enacted. The Espionage Statutes Modernization Act of 2011, S. 355, 112th Cong. (2011).

199. Stephen I. Vladeck, *Prosecuting Leaks Under U.S. Law*, *in* WHISTLEBLOWERS, LEAKS, AND THE MEDIA 34–35 (Paul Rosenzweig, Timothy J. McNulty & Ellen Shearer

The decision of the courts to defer almost entirely to whether a piece of information has been classified in determining whether its release meets the intent standard under the modern iterations of the 1917 Espionage Act has the effect of making the classification scheme inviolable. And as a result, the classification scheme that has been disseminated by the executive branch alone through a parade of executive orders, which formally have the power only to regulate the executive branch—has ended up directly affecting people who are *not in the executive branch*.

As noted above, Congress itself has been caught in this vise. Because many of the materials on which the Senate Committee relied in preparing its torture report had been classified Top Secret by the Bush Administration, the report itself had to be classified Top Secret (and likely SCI) as well. And because the executive branch, in a process spearheaded by the CIA, asserted control over the decision to declassify the report, disclosure of the Senate's report by the Senate Committee members or their staff could subject them to possible prosecution for violation of the Espionage Act, because they would be disclosing information marked classified. That is true even though Congress passed the Espionage Act *three decades* before the executive-run classification system even came into existence, and thus

eds., 2014) ("[E]very court to consider the issue has rejected the availability of an 'improper classification' defense—a claim by the defendant that he cannot be prosecuted because the information he unlawfully disclosed was in fact improperly classified."). Additional research did not turn up any contrary cases. Courts have not entertained improper classification defenses to prosecution under the Espionage Act because the statute does not require or specify that the disclosed information must be properly classified. *See Boyce*, 594 F.2d at 1251 (holding that under 18 U.S.C. § 798 "the propriety of the classification is irrelevant."); United States v. Lee, 589 F.2d 980, 990 (9th Cir. 1979) (finding no error in the exclusion of testimony from a classification expert at trial because an inquiry into the propriety of classification is "totally irrelevant" as "there is no requirement in [18 U.S.C. §§ 793, 794] that the documents be properly marked 'Top Secret' or for that matter that they be marked secret at all"). Under 18 U.S.C. §§ 793 and 794, "[i]t is enough that [the disclosed documents] related to the national defense and that they are transmitted with the intent to advantage a foreign nation or injure the United States." *Id.* Even where classification procedures may not have been followed entirely, a court affirmed a conviction under 18 U.S.C. § 793 because evidence adduced at trial "show[ed] that information contained in the [disclosed document] was secret information and related to the national defense." United States v. Dedeyan, 584 F.2d 36, 41 (4th Cir. 1978). For the same reason, courts have also held that improper classification is not a defense to prosecution under 50 U.S.C. § 783. *See Fondren*, 63 F. Supp. 3d at 608–10; Scarbeck v. United States, 317 F.2d 546, 558 (D.C. Cir. 1962) (holding that the government was not required to prove proper classification at trial because the language of 50 U.S.C. § 783 does not suggest that the disclosed information "must properly have been classified").

could not have intended the Act to serve as a cudgel to enforce that system—and almost certainly not against itself!

The many pathologies generated by the criminal law enforcement of the classification rules are discussed in more depth in Part III below. For now, the key point is that the main cudgel wielded to enforce the executive branch's unilateral decisions about what is classified—criminal sanctions—were not meant to serve that purpose at the time they were enacted. Moreover, these penalties can be applied to anyone who contravenes the rules—not just those who had authorized access to classified information and knowingly mishandled it or improperly disclosed it, but journalists who receive and publish it, or even (theoretically) those who download it from a publicly accessible website (for example on Wikileaks).

2. Administrative Sanctions

Criminal penalties are perhaps the most severe penalties that face a person who might run afoul of the classification rules, but they have been, at least to date, relatively infrequent (more on that in the next Part). Yet there are other sanctions that can apply to those who are found to have mishandled classified information—administrative sanctions: if a person is still employed by the U.S. government in a position that requires security clearance, they may be fired or have their security clearance revoked—which can have the same effect. Indeed, if the clearance is a qualification for the position, then losing the clearance means losing the job as well—it may also mean the end to not just a job but a career. The revocation of a security clearance is usually not reviewable by the Merit Systems Protection Board.[200]

Thomas Drake, a senior executive at the National Security Agency, worked in intelligence for most of his adult life, beginning when he volunteered for the Air Force in 1979. In 2005, he raised concerns about a program, codenamed Trailblazer, that he thought was an expensive boondoggle that violated citizens' privacy rights. After he raised the issue internally and did not get the response he wanted, he leaked what he claimed to believe was unclassified information about the program to the press. The FBI raided his home and found material that, while marked unclassified, it found to be related "to the national defense." Drake was prosecuted under the Espionage Act. He ultimately pled guilty to one count of exceeding the authorized use of a government computer, for which he would serve no jail time but

200. *See* Dep't of the Navy v. Egan, 484 U.S. 518, 526–30 (1988). However, courts may review constitutional challenges to the revocation of security clearances. *See* Webster v. Doe, 486 U.S. 592 (1988).

would agree to a year of probation and 240 hours of community service. He was forced, moreover, to resign from the NSA, and he lost his ability to ever work for the federal government again.[201]

For anyone seeking a security clearance—or seeking to have it renewed—mishandling classified information can be career ending. There are thirteen "adjudicative criteria" used to determine whether an individual should be given access to classified information.[202] One of the thirteen, "Guideline K," regards "handling protected information."[203] As the website "ClearanceJobs"—used by those seeking jobs that require a clearance—puts it,

> This criteria is more often used to revoke an existing clearance and comes down to the ability to responsibly carry out your duties in handling classified information. Repeatedly failing to lock a safe, for instance, may be seen as a callous attitude toward your duties, and could result in a clearance revocation if the situation is serious.[204]

It cites several examples of people who lost their clearances for this reason, among them Peter van Buren, who was a long-serving foreign service officer with Top Secret clearance.[205] After he linked to a WikiLeaks document on his blog, the State Department suspended his Top Secret clearance indefinitely.[206] By suspending the clearance rather than revoking it, they made it both impossible for him to remain in his job and impossible to appeal—because a final decision had not been reached. He was reassigned to a dead-end human resources job that did not involve sensitive duties or classified information.

Even security clearance revocations by the president that seem improperly motivated might not be subject to substantive review. In August 2018, President Donald Trump announced that he would be revoking former CIA Director John Brennan's security clearance. Trump claimed that Brennan had "leveraged his status as a former high-ranking official with access to highly sensitive information to

---

201. David Wise, *Leaks and the Law: The Story of Thomas Drake*, SMITHSONIAN MAG., (Aug. 2011), https://www.smithsonianmag.com/history/leaks-and-the-law-the-story-of-thomas-drake-14796786 [https://perma.cc/J2NT-BHMB].

202. *Security Executive Agent Directive*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE 4, 6 (June 8, 2017), https://www.hsdl.org/?view&did=815869 [https://perma.cc/5LUF-DWM3].

203. *Id.* at 21.

204. Lindy Kyzer, *What Are the Security Clearance Adjudicative Guidelines?*, CLEARANCEJOBS (Mar. 5, 2021), https://news.clearancejobs.com/2021/03/05/security-clearance-adjudicative-guidelines [https://perma.cc/DK77-CU2G].

205. *Id.*

206. Kim Zetter, *Diplomat Loses Top Secret Clearance for Linking to WikiLeaks*, WIRED (Oct. 19, 2011), https://www.wired.com/2011/10/diplomat-loses-security-clearance [https://perma.cc/LY39-VCDA].

make a series of unfounded and outrageous allegations—wild outbursts on the internet and television."[207] The most likely explanation, however, is that it was done in retaliation for Brennan's criticism of President Trump.

Outrageous as the decision appeared to be, most commentators concluded that the courts were unlikely to review the substantive reasons for security clearance determinations.[208] In 1988, in *Department of the Navy v. Egan*, the U.S. Supreme Court concluded that the decision to grant or deny a security clearance was an "inherently discretionary judgment call" committed by law to the executive branch.[209] Lower courts have found that revocations could be reviewed if agency regulations were violated in the course of the denial, but none has exercised meaningful review even on these grounds.[210] Moreover, it would be unconstitutional to revoke a security clearance in retaliation for First Amendment protected speech.[211] Brennan was poised to test the

---

207. Steve Holland & Jeff Mason, *Trump Revokes Ex-CIA Chief's Security Clearance, Slamming Critic*, REUTERS (Aug. 15, 2018), https://www.reuters.com/article/us-usa-trump-brennan/trump-revokes-ex-cia-chiefs-security-clearance-slamming-critic-idUSKBN1L01ZA [https://perma.cc/UJ8Z-Q59P].

208. *See* Annie Himes, A Call on Congress and the Courts: Protecting Constitutional Rights and Preventing the Politicization of Adverse Security Clearance Determinations 27 n.115 (May 13, 2019) (unpublished manuscript) (on file with author). The Trump White House also invoked *Egan* to push back against congressional efforts to oversee its decisions to unilaterally grant security clearances, including to his son-in-law and senior adviser, Jared Kushner. *See, e.g.*, Maggie Haberman, Michael S. Schmidt, Adam Goldman & Annie Karni, *Trump Ordered Officials to Give Jared Kushner a Security Clearance*, N.Y. TIMES (Feb. 28, 2019), https://www.nytimes.com/2019/02/28/us/politics/jared-kushner-security-clearance.html [https://perma.cc/GAG8-HREW]. One commentator suggested that President Trump had created a "loyalty model" to guide security clearance determinations. Kel McClanaham, *President Trump's Cronyism and Excesses Should Prompt Security Clearance Reform*, JUST SEC. (Mar. 8, 2019), https://www.justsecurity.org/63108/president-trumps-cronyism-excesses-prompt-security-clearance-reform [https://perma.cc/6LTN-Y6VV].

209. 484 U.S. 518, 527 (1988).

210. *See, e.g.*, Tenenbaum v. Caldera, 45 F. App'x 416, 418 (6th Cir. 2002); Stehney v. Perry, 101 F.3d 925, 934 (3d Cir. 1996); Jamil v. Sec'y, Dep't of Def., 910 F.2d 1203, 1209 (4th Cir. 1990).

211. *See* Kristy Parker & Ben Berwick, *How White House Threats to Revoke Security Clearances Violate the First Amendment*, LAWFARE (July 27, 2018), https://www.lawfareblog.com/how-white-house-threats-revoke-security-clearances-violate-first-amendment [https://perma.cc/R8PA-USEH] (citing Okwedy v. Molinari, 333 F.3d 339, 340–41 (2nd Cir. 2003) ("[A] public-official defendant who threatens to employ coercive state power to stifle protected speech . . . violates a plaintiff's First Amendment rights even if the public-official defendant lacks direct regulatory or decision-making authority over the plaintiff or a third party that facilitates the plaintiff's speech.") (first alteration in original); and then citing Backpage.com, LLC v. Dart, 807

limits of courts' deference to the president on these matters, threatening to sue to challenge the decision, but it was never clear whether the White House had taken the necessary steps to actually revoke his clearance and thus the matter never made it to the courts.[212]

All this serves to demonstrate that the executive branch has significant authority to suspend, revoke, or refuse to grant security clearances—whether for improper handling of classified material or any other reason—and Congress and the courts have thus far rarely intervened. Fear of losing security clearance access can be a powerful motivator for those whose careers depend on maintaining that access.

3. Civil Sanctions

A key tool that the U.S. government uses to try to discourage the disclosure of classified information is the threat of civil action. When a person receives access to a classified program, he or she is usually required to sign a nondisclosure agreement. Violating that agreement can bring civil penalties—meaning money damages rather than jail. Some statutes specifically build in civil penalties for violating security regulations. For example, any person who violates Department of Energy security regulations can be subject to a civil penalty not exceeding $100,000.[213] And those who violate the Espionage Act or the Atomic Energy Act may not only be subject to criminal sanctions, but may also lose their retirement pay.[214] But the main source of civil sanctions for violating security rules is what is called "prepublication review" requirements.

Prepublication review began in the 1950s as a small and largely informal process at the CIA. In the beginning, "few employees, current or former, were engaged in writing or speaking publicly on intelligence," and review could be handled by existing agency components.[215] But in the 1970s, prompted by the Vietnam War, Watergate,

F.3d 229, 230 (7th Cir. 2015) ("[A] public official who tries to shut down an avenue of expression of ideas and opinions through [sic] actual or threatened imposition of government power or sanction [sic] is violating the First Amendment.")).

212. *See* David Frum, *The Mystery of the Disappearing Security Clearance*, ATLANTIC (Jan. 13, 2019), https://www.theatlantic.com/politics/archive/2019/01/does-john-brennan-have-security-clearance/579772 [https://perma.cc/W8UQ-DUVR]. For more on security clearance revocations, see Himes, *supra* note 208.

213. *See, e.g.*, 42 U.S.C. § 2282b(a).

214. 5 U.S.C. § 8312(a)–(c) (listing violations of 18 U.S.C. §§ 793, 798, 42 U.S.C. §§ 2272–76, and 50 U.S.C. § 421, among those for which forfeiture of retirement pay or annuities may be imposed).

215. Memorandum from Charles A. Briggs, Inspector General on Inspection Report of the Office of Public Affairs 1 (1981) (declassified Nov. 6, 2003) https://www

and the Church and Pike Committee investigations into the intelligence community, active and former CIA officers began speaking and writing publicly more frequently. To review the increased number of public writings (still a tiny number by modern standards), the CIA created a Publications Review Board in 1976.[216]

A challenge to the process that reached the Supreme Court in 1980 unwittingly set the stage for its massive expansion. Frank Snepp was a former CIA officer who had signed "an agreement promising that he would 'not . . . publish . . . any information or material relating to the Agency, its activities or intelligence activities generally, either during or after the term of [his] employment . . . without specific prior approval by the Agency.'"[217] After leaving the CIA, he published a "book about CIA activities on the basis of this background and exposure" and "deliberately and surreptitiously violated his obligation to submit all material for prepublication review."[218] The government sued to enforce its agreement, and the district court enjoined Snepp from violating his agreement and imposed a constructive trust on the book's proceeds.[219] When the case reached the Supreme Court, the Court ruled summarily, without merits briefing or oral argument.[220] In a footnote, it concluded that a former employee's contractual duty of prepublication review could overcome the presumption against prior restraint: the CIA had "a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality," and the "agreement that Snepp signed [wa]s a reasonable means for protecting this vital interest."[221]

Today every U.S. intelligence agency and many other federal agencies impose a lifetime prepublication review requirement on at least some subset of former employees. In 2017, 4,030,625 people held security clearances—or 1.2 percent of the entire U.S. population.[222] This actually understates the reach of the modern prepublication review process, because all former government employees who

.justsecurity.org/wp-content/uploads/2015/12/prb1981.pdf [https://perma.cc/PZ73-8W6K] [hereinafter 1981 CIA IG Report]. This description draws in part from Brief of Professors Jack Goldsmith & Oona Hathaway as Amici Curiae in Support of Appellants & Reversal, Edgar v. Ratcliffe, No. 20-1568 (4th Cir. Aug. 21, 2020).

216. 1981 CIA IG Report, *supra* note 215, at 2–5.

217. Snepp v. United States, 444 U.S. 507, 508 (1980) (alterations in original).

218. *Id.* at 511.

219. United States v. Snepp, 456 F. Supp. 176, 182 (E.D. Va. 1978).

220. *Snepp*, 444 U.S. at 526 n.17 (Stevens, J., dissenting).

221. *Id.* at 509 n.3 (per curiam opinion).

222. Nat'l Counterintelligence and Sec. Ctr., *supra* note 131, at 5.

have held classified access but who are no longer employed by the federal government (including the author) are bound to comply with prepublication review for life.

Every agency, moreover, has its own prepublication office and its own prepublication submission rules.[223] The Department of Defense, for example, requires that, "former DoD employees . . . use the DoD prepublication review process to ensure that information they intend to release to the public does not compromise national security as required by their nondisclosure agreements."[224] This sweeping language applies to works of fiction as well as nonfiction, even if the drafts clearly contain no classified information.[225] The State Department, meanwhile, requires prepublication review of "writings on foreign relations topics by former Department personnel [with security clearances], including contractors and detailees."[226] Prepublication review obligations also are no longer limited to "voluntar[y]" nondisclosure "agreement[s]" or fiduciary relationships with a specific agency considered in *Snepp*.[227] Agencies impose prepublication review obligations through regulations, policies, and guidance documents that extend beyond the express terms of any agreement the former employee signed.

What is the penalty for failing to comply? There are the administrative sanctions noted above—firing, loss of security clearance, exclusion from future employment that requires classified access. And, if classified information has been disclosed, there can be criminal sanctions, again described at some length above. Last but not least are civil sanctions: in brief, the government can lay claim to any proceeds a current or former employee has earned as a result of violating their nondisclosure agreement. For example, Matt Bissonette, a member of the SEAL team that killed Osama Bin Laden, published his book, *No Easy Day*, without going through the review process. As a result, the

223. *See Interactive Chart: Prepublication Review by Agency and Secrecy Agreement*, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Aug. 27, 2019), https://knightcolumbia.org/content/prepublication-review-by-agency-and-agreement [https://perma.cc/BQV2-MFF7].

224. DEP'T OF DEF., DOD INSTRUCTION 5230.09: CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE 4 (Jan. 25, 2019).

225. Brief of Professors Jack Goldsmith & Oona Hathaway as Amici Curiae in Support of Appellants & Reversal, *supra* note 215, at 13 (noting that the Department of Defense refuses to exclude any form of document from prepublication review).

226. 22 C.F.R. § 9.14 (2020).

227. Snepp v. United States, 444 U.S. 507, 509 n.3 (1980).

government sued him and eventually seized his book advance of $6.8 million.[228]

Civil damages and the threat of civil damages mostly work to constrain those who intend to publish longer works, which generally entail significant research and writing time and from which they might earn some money. Civil damages are largely ineffective against those who might leak information to the media, because leakers don't provide the government advance warning and they usually do not receive any financial reward that the government might seize.[229]

III. PATHOLOGIES

The system for keeping information secret described above shows that classification has grown exponentially over the last several decades. But is that really so bad? That secret-keeping is cumbersome and expensive, but maybe that's justified if the upside is better protection of our national security. Unfortunately, however, the truth is that the costs are much more significant than a merely cumbersome system. As this Part will show, the system poses threats to our system of democratic governance and even to the very national security it is supposed to protect.

A. KEEPING INFORMATION FROM THE PUBLIC—AND CONGRESS

The democratic costs of the massive accumulation of classified information are hard to overstate. To note the obvious: a state cannot keep secrets from its enemies without keeping them from its own citizens. Massive secret keeping by the government makes it impossible for democratic checks to operate, at least with regard to those things kept secret. Philosopher Jeremy Bentham put it this way: "Secre[c]y is an instrument of conspiracy, it ought not, therefore, to be the system of a regular government."[230] Woodrow Wilson, arguably hypocritically given his role in the passage of the Espionage Act, argued in 1912 that "government ought to be all outside and no inside," and that "there ought to be no place where anything can be done that everybody does not know about."[231]

---

228. Christopher Drew, *Ex-SEAL Member Who Wrote Book on Bin Laden Raid Forfeits $6.8 Million*, N.Y. TIMES (Aug. 19, 2016), https://www.nytimes.com/2016/08/20/us/bin-laden-book-seal-team-6.html [https://perma.cc/9EKE-CC5S].

229. David Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 539 (2013).

230. Jeremy Bentham, *Essay on Political Tactics*, *in* THE WORKS OF JEREMY BENTHAM 299, 315 (John Bowring ed., 1843).

231. WOODROW WILSON, THE NEW FREEDOM 113–14 (1913).

Certainly, the state has good reason to keep some things hidden from public view. Details of military plans must remain secret or a mission may be compromised and U.S. forces could lose their lives. And when a problem first emerges—like the reemergence of Ebola or the splintering of the Islamic State from al Qaeda—government officials need to have the space to air all the options, to think creatively without worrying about premature public judgment. As philosopher Sissela Bok once put it, "[A]dministrators must be able to consider and discard a variety of solutions in private before endorsing some of them in public; the process of evolving new policies requires a degree of concealment."[232] And there are even some cases where we *rely* on the state to keep secrets. No one thinks that personal medical records or ordinary citizens' tax returns, for example, should be made public as a matter of course. But the fact that *some* secrecy is necessary does not mean that more secrecy is better.

Government secrecy at the level it currently exists in the U.S. government is at odds with our nation's most deeply held commitments to effective democratic governance and rule of law. Put simply, in order for the people to hold government accountable, they need to know what their government is doing. A system that cloaks a great deal of government activity under a protective layer of secrecy undermines this basic premise of democracy; and if the people are not well informed, they cannot effectively govern. Even advocates of secrecy admit as much. In his 2003 Executive Order 13,292, which ratcheted up government secrecy, President George W. Bush began with this acknowledgment: "Our democratic principles require that the American people be informed of the activities of their Government."[233]

We have seen that the U.S. government is capable of not only bad decisions, but even horrific abuses, when acting in secret. Acting on secret legal opinions issued in the year after the September 11 attacks,[234] CIA officers at a secret prison in Kabul, Afghanistan subjected

232. BOK, *supra* note 143, at 175.

233. Exec. Order No. 13,292, 68 C.F.R. 15,315 (Mar. 28, 2003). Unfortunately, the order then went on to reverse President Bill Clinton's 1995 reforms that had encouraged declassification and discouraged classification, permitting more information to be classified for longer periods of time by, for example, eliminating the Clinton-era standard that information should not be classified if there is significant doubt about the need to do so, automatically treating information obtained in confidence from foreign governments as classified, easing the reclassification of declassified documents, and eliminating the requirement that agencies prepare plans for declassifying records.

234. *See* Letter from John Yoo, Deputy Assistant Att'y Gen., to Alberto R. Gonzales, Counsel to the President (Aug. 1, 2002) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB127/020801.pdf [https://perma.cc/FA29-T7DJ]; Memorandum from Jay S.

Gul Rahman to "enhanced interrogation techniques," including water-boarding.[235] Naked from the waist down, he was then shackled to a cold concrete floor in a cell, where he died of hypothermia. The cause of his death only became public years later, after several of his fellow former prisoners filed suit and forced the release of 274 documents in pre-trial discovery.[236]

He was not alone in suffering horrific abuse in secret. The aforementioned U.S. Senate Select Committee on Intelligence report released in 2014 acknowledged that there were CIA black sites around the world at which hundreds of prisoners had been kept and tortured.[237] These disclosures, however, took place years after the programs had ended and the politicians most responsible for them had long left office. The secrecy thus frustrated the democratic process—preventing the American public from learning the scope of illegal programs until after it was too late to vote those responsible out of office.

There is a more subtle way in which secrecy undermines the effectiveness of government: when government keeps secrets, those secrets enable—and sometimes require—lies. When the secrets are later disclosed, the lies are revealed as well, and the American public learns that it cannot trust its government to tell the truth. Public trust took a blow in 2013 when Edward Snowden, a former CIA employee, revealed the existence of PRISM, a program that allowed court-approved access to Americans' Google and Yahoo accounts, under which the NSA had gathered millions of email and instant messaging contacts, searched emails, tracked and mapped cell phones locations, while working to defeat encryption programs installed to prevent just

---

Bybee, Assistant Att'y Gen., Off. of Legal Couns. to John Rizzo, Acting Gen. Couns. Cent. Intel. Agency, (Aug. 1, 2002), https://www.justice.gov/sites/default/files/olc/legacy/2010/08/05/memo-bybee2002.pdf [https://perma.cc/YEK3-M463] (regarding interrogation of al Qaeda operative); Memorandum from John C. Yoo, Deputy Assistant Att'y Gen., to William J. Haynes II, Gen. Couns. for the Dep't of Def. (Mar. 14, 2003), https://www.aclu.org/sites/default/files/pdfs/safefree/yoo_army_torture_memo.pdf [https://perma.cc/TJT7-QNEM] (regarding interrogation of "unlawful combatants").

235. S. REP. NO. 113-288, at 54 (2014).

236. Larry Siems, *Inside the CIA's Black Site Torture Room*, GUARDIAN (U.K.) (Oct. 9, 2017), https://www.theguardian.com/us-news/ng-interactive/2017/oct/09/cia-torture-black-site-enhanced-interrogation [https://perma.cc/6QYE-KK82].

237. S. REP. NO. 113-288, at 97 (2014) (explaining the process of the CIA opening detention sites in various countries and transporting detainees to and from those sites).

such surveillance.[238] For a myriad of reasons, likely including such disclosures, public trust in government has fallen from seventy percent in the 1950s (before, among other things, the leak of the Pentagon Papers) to just seventeen percent in 2019.[239] That has, in turn, eroded the effectiveness of the very institutions secrecy is meant to protect.

The distrust in the U.S. government that secrecy breeds extends abroad—making counterterrorism efforts less effective. For the better part of two decades, the CIA has reportedly carried out an extensive program of targeted killing abroad. These strikes have been, according to news reports, classified as "covert actions": "activities of the United States Government . . . where it is intended that the role . . . will not be apparent or acknowledged publicly, but does not include traditional . . . military activities."[240] As a result, these strikes could not be acknowledged. Indeed, when President Obama publicly acknowledged the covert U.S. drone program in Pakistan in 2012, it caused a huge stir.[241] The program was what CNN rightly called "the worst kept secret in Washington and Pakistan."[242] When a building blows up—and the United States refuses to acknowledge that it is responsible—distrust of the U.S. government is the predictable result. In 2011, for example, a U.S. military airstrike is said to have killed a sixteen-year-

238. Connor Simpson & Abby Ohlheiser, *Why Edward Snowden Leaked the Secret NSA Information*, ATLANTIC (June 9, 2013), https://www.theatlantic.com/national/archive/2013/06/why-edward-snowden-leaked-secret-nsa-information/314449 [https://perma.cc/4LXM-C3FG] ("Now that the story has a face, the answer could say a lot about how it ends – with Snowden in chains and the government continuing its spying without restraint, or with Snowden lionized and the government backing off. If purity of motive is the measure – and if Snowden's account of his actions holds up – he might fit the hero's mold." (quoting Editorial, *NSA Whistle-Blower Hero or Villain? Our View*, USA TODAY (June 9, 2013), https://www.usatoday.com/story/opinion/2013/06/09/nsa-whistle-blower-edward-snowden-editorials-debates/2406409 [https://perma.cc/4KHS-W269]).

239. *See Public Trust in Government: 1958–2021*, PEW RSCH. CTR. (May 17, 2021), https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021 [https://perma.cc/MAF6-B4RV].

240. *See* 50 U.S.C. § 3093(e) (2018); *see also* Mark Mazzetti, *A Secret Deal on Drones, Sealed in Blood*, N.Y. TIMES (Apr. 6, 2013), https://www.nytimes.com/2013/04/07/world/asia/origins-of-cias-not-so-secret-drone-war-in-pakistan.html [https://perma.cc/E5CJ-NFJA] (highlighting a case where the Pakistani army claimed responsibility for hunting and killing one of its enemies when in reality the CIA had conducted the operation in exchange for use of Pakistan's airspace).

241. Ariel Zirulnick, *Obama Admits 'Worst-Kept Secret': US Flies Drones over Pakistan*, CHRISTIAN SCI. MONITOR (Jan. 31, 2012), https://www.csmonitor.com/World/Security-Watch/terrorism-security/2012/0131/Obama-admits-worst-kept-secret-US-flies-drones-over-Pakistan [https://perma.cc/H5DX-GZ8C] (citing condemnation of the covert missions at home and by foreign leaders).

242. *See id.*

old American citizen in Yemen. The United States did not acknowledge that it was responsible for the strike.[243] According to reporting, one reason for the reluctance to acknowledge U.S. strikes in Yemen around this period was to allow another foreign leader to mislead his own people: President Ali Abdullah Saleh of Yemen is said to have consented to secret strikes by the United States in Yemen against suspected members of al-Qaeda in the Arabian Peninsula.[244] Reporting indicated that Saleh had claimed drone strikes in the country as his own, in order to conceal from the Yemeni parliament and people that he was cooperating with the United States.[245]

All of this secrecy means that people don't know what their government is doing—and therefore cannot use any of the ordinary democratic or rule of law constraints on government to put an end to them. But the problem is not simply that information is kept secret. The bigger problem is that information is kept secret *selectively*. Overclassification opens the door not just to hiding things from the American public about what its government is doing. The massive overclassification of government-held information *also* allows the government to *manipulate* public access to information through selective declassification. Selective declassification can have a deeply corrupting influence on public discourse.[246] It is possible because, in addition to providing for some forms of mandated declassification, Executive Order 13,526 permits discretionary declassification when information "no longer meets the standards for classification" or in "exceptional cases" where "the need to protect such information may be outweighed by the public interest in disclosure of the information . . . ."[247] A 2007 report found that such discretion is not often exercised, but when it is, it is

243. Craig Whitlock, *U.S. Airstrike that Killed American Teen in Yemen Raises Legal, Ethical Questions*, WASH. POST (Oct. 22, 2011), https://www.washingtonpost.com/world/national-security/us-airstrike-that-killed-american-teen-in-yemen-raises-legal-ethical-questions/2011/10/20/gIQAdvUY7L_story.html [https://perma.cc/V9CP-FYA9].

244. *See* Robert Booth & Ian Black, *WikiLeaks Cables: Yemen Offered US 'Open Door' to Attack Al-Qaida on Its Soil*, GUARDIAN (U.K.) (Dec. 3, 2010), https://www.theguardian.com/world/2010/dec/03/wikileaks-yemen-us-attack-al-qaida [https://perma.cc/2BK3-MWCD] (quoting President Ali Abdullah Saleh to U.S. General David Petraeus) ("We'll continue saying the bombs are ours, not yours.").

245. *Id.*

246. *See* Sasha Dudding, *Spinning Secrets: The Dangers of Selective Declassification*, 130 YALE L.J. 708, 736 (2021) ("By revealing preferred information, the disclosures tilted the playing field toward the [Bush] Administration's desired outcomes: going to war and maintaining public support for war.").

247. Exec. Order No. 13,526 § 3.1(d), 75 Fed. Reg. 707 (Dec. 29, 2009).

"more often been because the department or agency wants to get its own position out . . . ."[248]

In the early years of the Cold War, there was a CIA program to manipulate the media—an effort that sometimes involved directly employing journalists as well as collaboration and cooperation between the U.S. government and news organizations.[249] Although such extensive and direct programs have long since been disbanded, this history has unfortunately helped fuel current QAnon conspiracy theories. Believers in the conspiracy dismiss news stories contrary to the QAnon narrative as part of the CIA's program of media manipulation—indeed, the stories disproving the narrative are sometimes taken as *evidence* of the complicity of "fake news."[250] This is a perhaps under-appreciated cost of secret programs to manipulate public information—the public begins to doubt what is "real."

Although the direct manipulation of the press is no longer permitted in the United States, selective declassification is used by the government to shape the public narrative. This can be seen in a host of situations. Consider the Senate hearings on Gina Haspel's nomination to serve as the director of the CIA. Haspel reportedly oversaw a CIA black site in Thailand at which detainees were tortured and then participated in the decision to destroy video tapes of that torture in an effort to prevent information about the torture from coming to light. The government declassified favorable information including a memo that cleared Haspel of responsibility for destroying evidence of the coercive methods used as part of the interrogation program.[251] It also

---

248. *See Improving Declassification: A Report to the President from the Public Interest Declassification Board*, PUB. INT. DECLASSIFICATION BD. 29 (2007), https://www.archives.gov/files/declassification/pidb/improving-declassification.pdf [https://perma.cc/7RBC-QZSY].

249. *See CIA's Use of Journalists and Clergy in Intelligence Operations: Hearing Before the Select Comm. on Intel. of the U.S. S.*, 104th Cong. (1996).

250. Erick Trickey, *Fact-Checking QAnon Conspiracy Theories: Did JP Morgan Sink the Titanic?*, WASH. POST (Aug. 4, 2018), https://www.washingtonpost.com/news/retropolis/wp/2018/08/04/how-j-p-morgan-didnt-sink-the-titanic-and-other-qanon-conspiracy-theories-debunked [https://perma.cc/7VMS-4EZN] ("QAnon posters dismiss press reports they do not like by claiming they are part of 'Operation Mockingbird,' supposedly a continuation of a 1950s CIA program to distribute propaganda through the media.").

251. Karoun Demirjian, *CIA Refuses to Declassify More Information About Gina Haspel, Trump's Pick to Lead the Agency*, WASH. POST (Apr. 25, 2018), https://www.washingtonpost.com/powerpost/cia-refuses-to-declassify-more-haspel-documents-angering-democrats/2018/04/25/4616846e-48b0-11e8-9072-f6d4bc32f223_story.html [https://perma.cc/6DB5-N3G9] (explaining that the report clearing Hapsel was released but that the CIA refused to release "basic biographical details about Haspel's career").

encouraged former clandestine officers to grant interviews to support her nomination.[252] But it refused to declassify other information about her career, including regarding her role in the torture that took place at the black site in Thailand, leading one senator to assert that the CIA was running a "full-on propaganda campaign but withholding the information that the American people need to be able to make an informed decision about this nominee's fitness for the job."[253] Perhaps that wasn't so surprising: because she was the current acting director, Haspel herself was the declassification authority over her own record.

Selective declassification has also been used to make the case for war: in 2002, the Bush Administration sought to build the case for war against Iraq. After finding no significant connections between the Iraqi government, led by Saddam Hussein, and al-Qaeda, the administration began investigating whether Hussein's regime had an active weapons of mass destruction (WMD) program that might provide an alternative justification for war. In late 2002, at Congress's request, the CIA quickly prepared a national intelligence estimate summarizing the intelligence community's findings.[254] That report concluded that Iraq had chemical and biological weapons and was planning to develop nuclear weapons—but it acknowledged that there was evidence to the contrary.[255] The report was of course highly classified. The White House released an unclassified "summary" that removed all the caveats.[256] The summary helped shape public opinion in favor of the war, and members of Congress who did not have access to the full classified report *based their votes* on the authorization for the use

252. Adam Goldman & Matthew Rosenberg, *How the C.I.A. Is Waging an Influence Campaign to Get Its Next Director Confirmed*, N.Y. TIMES (Apr. 20, 2018), https://www.nytimes.com/2018/04/20/us/politics/gina-haspel-cia-director-influence-campaign.html [https://perma.cc/7HEM-S25C] (highlighting the various ways current and former CIA agents were working to help Haspel get confirmed through selective dissemination of information).

253. *Id.* (quoting Sen. Martin Heinrich).

254. *See* S. REP. NO. 108-301, at 298 (2004) (offering an example of portion marking, as each portion has its own classification marking).

255. *See National Intelligence Estimate 2002–16HC: Iraq's Continuing Programs for Weapons of Mass Destruction*, NAT'L INTEL. COUNCIL 14 (2002), https://documents2.theblackvault.com/documents/cia/iraq-wmd-nie-01-2015-Dec2018Release-highlighted.pdf [https://perma.cc/YWB5-23TA] ("The information we have on Iraqi nuclear personnel does not appear consistent with a coherent effort to reconstitute a nuclear weapons program.").

256. *See Iraq's Weapons of Mass Destruction Program*, NAT'L INTEL. COUNCIL (2002), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB254/doc02.pdf [https://perma.cc/2Q3A-UTU7].

of force against Iraq largely on this unclassified summary.[257] It was only after the war that it became clear that the summary's unequivocal conclusions were false: there was no WMD program after all.

More recently, selective classification was used to limit access to information about the government's response to COVID-19. The Trump White House ordered the Department of Health and Human Services to hold its meetings on the pandemic in a Sensitive Compartmented Information Facility.[258] This decision was highly unusual and, some argued, entirely unjustified.[259] It had the effect of limiting who could attend—government experts who lacked the right clearances, for example, were excluded. It also limited the information about the meetings that could be released. Information about the meetings came almost exclusively from official sources—which put, we now know, an unduly rosy spin on the state of the pandemic response. The arrangement also prevented information about the virus from being shared within the Administration, potentially slowing the response to the crisis.

There also have been what might be considered more positive instances of selective declassification. Perhaps the single most expansive use of the discretionary declassification authority in recent years was the massive post-Snowden declassification of material about surveillance activities—which continues today. The revelations from Snowden's unauthorized disclosure triggered a vigorous debate about government surveillance activities. In response, the government declassified significant information, some voluntarily and some under

257. Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 116 Stat. 1498 (2002) (codified at 50 U.S.C. § 1541); *see* Dudding, *supra* note 246 (providing a more detailed recounting of these events).

258. Aram Roston & Marisa Taylor, *Exclusive: White House Told Federal Health Agency to Classify Coronavirus Deliberations–Sources*, REUTERS (Mar. 11, 2020), https://www.reuters.com/article/us-health-coronavirus-secrecy-exclusive/exclusive-white-house-told-federal-health-agency-to-classify-coronavirus-deliberations-sources-idUSKBN20Y2LM [https://perma.cc/49YQ-7W2N].

259. Matthew Collette, *The Legally Troubling Treatment of COVID-19 Meetings as Classified*, JUST SEC. (Mar. 17, 2020), https://www.justsecurity.org/69237/the-legally-troubling-treatment-of-covid-19-meetings-as-classified [https://perma.cc/G5M9-G9QP] (emphasizing that there was no connection to national security about the information that was learned from the meeting and, given that disseminating timely and accurate information is key in the response to the pandemic, the classification was unprecedented).

government order.[260] The voluntary releases were likely made to assuage public concerns about excessive surveillance and to inform debates taking place in Congress.[261]

Massive overclassification, and the selective declassification it enables, can turn the press into a tool for shaping the narrative in ways that government agencies (or those within them) favor. David Pozen, in his provocative article, *The Leaky Leviathan*, shows that what may appear to be unauthorized "leaks" (unauthorized releases) may in fact be "plants" (that is, authorized releases) or what he terms "pleaks," which fall somewhere in between the two. He argues that such "pleaks" in fact predominate over true leaks. Journalists benefit from these "pleaks" because they get juicy information that they can report. But such semi-authorized releases are far from unproblematic, even aside from the fact that they are illegal. Those with access to classified information can selectively release information to shape a narrative. Journalists often don't know when they are being used in this way. They have no way of knowing whether a particular bit of information is a true leak or a plant or "pleak." And they often don't have visibility into the broader context, to understand, for example, whether a piece of information that has been shared is contested or not.[262]

Keeping documents and decisions secret can allow the executive branch not only to manipulate the narrative and avoid public oversight but also to limit and sometimes even avoid congressional oversight, as well.[263] As noted above,[264] members of Congress automatically receive security clearances by virtue of their office—but they are

260. Spencer Ackerman, *FISA Judge: Snowden's NSA Disclosures Triggered Important Spying Debate*, GUARDIAN (U.K.) (Sept. 13, 2013), https://www.theguardian.com/world/2013/sep/13/edward-snowden-nsa-disclosures-judge [https://perma.cc/7FSQ-ZAQU] (providing examples of courts ordering the disclosure of secret intelligence rulings).

261. Andrea Peterson, *A Year After Snowden Revelations, Government Surveillance Reform Still a Work in Progress*, WASH. POST (June 5, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/06/05/a-year-after-snowden-revelations-government-surveillance-reform-still-a-work-in-progress [https://perma.cc/H4XW-GHKW] ("Over the course of the past year, Clapper's office has posted a veritable treasure trove of declassified documents related to NSA spying programs on a Tumblr set up for that purpose.").

262. Pozen, *supra* note 229, at 567 (comparing how a high-level official may make a statement of equal merit as a low-level official, but the former's statement will likely be vetted in a much more lenient way).

263. This is a point made powerfully in Josh Chafetz, *Whose Secrets?*, 127 HARV. L. REV. F. 86 (2013). As Chafetz puts it, "'secret' is a political category, not a natural one." *Id.* at 86. Moreover, "[s]ecrets are treated as belonging to the executive;" which helps explain why the executive branch finds it so appealing. *Id.* at 87.

264. *See supra* notes 139–41 and accompanying text.

not automatically entitled access to Special Compartmented Information. Meanwhile, relatively few congressional staff have access to classified information, and secure facilities for accessing and storing classified information are often difficult for those with the proper clearances to access. This severely hampers the capacity of congressional committees to provide adequate oversight over any operation or activity that is classified, especially those that entail compartmented information.[265] Restricted congressional oversight can be yet another advantage of classification for the executive branch—it gives the executive branch a freer hand to act without constraint—and yet another reason that classification can both be anti-democratic and lead to inadequately considered decisions.

B. INTIMIDATING THE PRESS

In May 2019, the DOJ indicted the eccentric founder and leader of WikiLeaks, Julian Assange, on seventeen counts of violating the Espionage Act for participating in obtaining and publishing classified documents nine years earlier.[266]

Assange had already been indicted by federal prosecutors on earlier charges of conspiring to commit unlawful computer intrusion for agreeing to help Chelsea Manning, then an intelligence analyst in the United States Army, crack a password so that she could log onto a classified Department of Defense network under a different username.[267] The new indictment charged that Assange encouraged the disclosure of protected information, including classified information.[268] Among other things, WikiLeaks posted a detailed list of "The Most Wanted Leaks of 2009" organized by country. For the United States, that included bulk databases such as "Intellipedia," an unclassified but non-public, CIA Open Source Center database and "'Military and Intelligence' documents, including documents . . . classified up to the SECRET level, [such as the] 'Iraq and Afghanistan Rules of Engagement 2007-2009 (SECRET);' operating and interrogation procedures at

265. *See* Oona A. Hathaway, Tobias Kuehne, Randi Michel & Nicole Ng, *Congressional Oversight of Modern Warfare: History, Pathologies, and Proposals for Reform*, 63 WM. & MARY L. REV. (forthcoming 2021) (manuscript at 45–46) (highlighting frustrations within congressional committee work when some members have clearance to information and others do not).

266. *See* Charlie Savage, *Assange Indicted Under Espionage Act, Raising First Amendment Issues*, N.Y. TIMES (May 23, 2019), https://www.nytimes.com/2019/05/23/us/politics/assange-indictment.html [https://perma.cc/64KF-EER7]; Superseding Indictment, United States v. Assange, No. 1:18-CR-00111 (E.D. Va. May 23, 2019).

267. Savage, *supra* note 266.

268. Superseding Indictment, *supra* note 266, at 2.

Guantanamo Bay, Cuba; documents relating to Guantanamo detainees; CIA detainee interrogation videos; and information about certain weapons systems."[269]

The indictment alleged that Chelsea Manning responded to Assange's solicitation by searching the classified network for the information on Assange's "most wanted" list. Manning downloaded four databases containing approximately 90,000 Afghanistan war-related significant activity reports, 400,000 Iraq war-related significant activities reports, 800 Guantanamo Bay detainee assessment briefs, and 250,000 U.S. Department of State cables and provided them to WikiLeaks. Many of the documents, which Wikileaks proceeded to publicly disclose, were labeled Secret.[270]

Assange's case was the third in which the government brought Espionage Act charges against someone not affiliated with the U.S. government.[271] But it was the very first time the Justice Department had obtained an indictment with Espionage Act charges based exclusively on the act of publication.[272] Counts 15 through 17 against Assange are based only on posting documents on the Internet.[273] In particular, he was charged with "having unauthorized possession of significant activity reports, classified up to the SECRET level, from the Afghanistan war," from the "Iraq war" and "State Department cables," which included the names of individuals, and he "communicated the documents containing names of those sources to all the world by publishing them on the Internet."[274] Although the indictment emphasizes

269. *Id.* at 3.

270. *Id.* at 11.

271. *See* Danielle Brian & Scott H. Amey, *Assange's Indictment: A Threat to Everyone*, JUST SEC. (June 27, 2019), https://www.justsecurity.org/64719/assanges-indictment-a-threat-to-everyone [https://perma.cc/MH6P-JG5E]. One of the previous cases was a 2005 prosecution of Steven Rosen and Keith Weissman, employees of the American Israel Public Affairs Committee, for allegedly conspiring with Pentagon analyst Larry Franklin to receive and disseminate classified information about Iran. That case was dropped after the federal district court interpreted the Act to require a high evidentiary threshold. The other case dated to 1971, in which Anthony Russo was prosecuted for helping Daniel Ellsberg copy the Pentagon Papers—a case that collapsed due to prosecutorial misconduct. *See generally* Gabe Rottman, *Special Analysis of the May 2019 Superseding Indictment of Julian Assange*, REPS. COMM. FOR FREEDOM PRESS (May 30, 2019), https://www.rcfp.org/may-2019-assange-indictment-analysis [https://perma.cc/3DS9-KA65].

272. Brian & Amey, *supra* note 271; Gabe Rottman, *The Assange Indictment Seeks to Punish Pure Publication*, LAWFARE (May 24, 2019), https://www.lawfareblog.com/assange-indictment-seeks-punish-pure-publication [https://perma.cc/V5VL-PT67].

273. Superseding Indictment, *supra* note 266, at 32–34.

274. *Id.*

the disclosure of source names, the director of the Technology and Press Freedom Project at the Reporters Committee for Freedom of the Press pointed out that little in the case turned on the publication of informants' names and therefore, "as a legal matter, the publication of informants' names won't serve to distinguish this case from a future Espionage Act prosecution based on pure publication."[275]

Manning was arrested in 2010, but Assange evaded prosecution by hiding out in the Ecuadorian embassy until 2019, when Ecuador allowed him to be removed, and he was placed into custody in the United Kington. A U.K. court found that the extradition request was valid but blocked his extradition to the United States to face charges due to his mental health conditions. As of this writing, he remains in custody pending appeal of the extradition denial.[276]

The indictment raised fears among journalists that the DOJ might begin using the Espionage Act to prosecute journalists.[277] Indeed, the language in the Act is extremely broad; as broad as, if not broader than, the laws used by the governments of Turkey and China to prosecute journalists.[278] The charges, many worried, relied on behavior that investigative journalists in the United States engage in on a daily basis. Jameel Jaffer of the Knight First Amendment Institution at Columbia University labeled the indictment "a frontal attack on press freedom."[279] The DOJ argued that Assange was not a real journalist

275. Rottman, *supra* note 272.

276. Megan Specia, *British Court Hears Appeal in Julian Assange Extradition Case*, N.Y. TIMES (Oct. 29, 2021), https://www.nytimes.com/2021/10/29/world/europe/appeal-julian-assange-extradition.html [https://perma.cc/MW2P-7FPN].

277. Alexandra Ellerbeck & Avi Asher-Schapiro, *Why the Prosecution of Julian Assange is Troubling for Press Freedom*, COMM. TO PROTECT JOURNALISTS (Apr. 12, 2019), https://cpj.org/2019/04/why-prosecution-julian-assange-press-freedom [https://perma.cc/YS9R-HT3N] (emphasizing the fear journalists felt that Assange's indictment would set a dangerous precedent for other journalists engaged in legally similar activity).

278. Ned Levine, Espionage Acts in Turkey, China, and the United States 4 (2018) (unpublished manuscript) (on file with author) ("The laws are broadly similar; authorities in China and Turkey would doubtless make good use of the language of the Espionage Act to prosecute the same journalists they prosecute under their own laws.").

279. Savage, *supra* note 266 (quoting Jaffer); *see also* Jameel Jaffer, *The Espionage Act and a Growing Threat to Press Freedom*, NEW YORKER (June 25, 2019), https://www.newyorker.com/news/news-desk/the-espionage-act-and-a-growing-threat-to-press-freedom [https://perma.cc/BUJ5-9ZZG] (claiming that some of Assange's fiercest critics have come to his defense arguing against government use of the Espionage Act to target a publisher).

and WikiLeaks not a news outlet.[280] But in its reporting on the indictment, the *New York Times* noted that the charges against Assange were for actions that it too had taken. Indeed, it had obtained precisely the same documents as WikiLeaks, also without government authorization, and had also published subsets of the files, albeit with the names of informants withheld.[281]

The fears are not unwarranted. Before the Assange indictment, the Espionage Act had never been used to prosecute a journalist or media organization for publishing or disseminating unlawfully disclosed classified information.[282] But that is not because the Act could not be read to permit such indictments. Journalists were protected from prosecution by a longstanding U.S. government policy of not prosecuting such cases. The Justice Department's guidelines for investigating leaks state that "members of the news media will not be subject to prosecution based solely on newsgathering activities."[283] This approach, the guidelines explain, strikes "the appropriate balance between two vital interests: protecting the American people by pursuing those who violate their oaths through unlawful disclosures of information and safeguarding the essential role of a free press in fostering government accountability and an open society."[284] In 2014, Attorney General Eric Holder reaffirmed the Department's commitment to this policy, stating, "As long as I am attorney general, no reporter who is doing his job is going to go to jail."[285] President Trump's Attorney Generals (first Sessions, then Barr) declined to make the same public commitments.[286] Observers were not entirely surprised, then, at the announcement of the Assange indictment.

---

280. Savage, *supra* note 266 (quoting John Demers, then head of the Justice Department's National Security Division).

281. *Id.* (emphasizing the confusion major news outlets like the *New York Times* felt at the time of the indictment).

282. *WikiLeaks and the Espionage Act of 1917*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/journals/wikileaks-and-espionage-act-1917 [https://perma.cc/V2A6-2TBY] ("The U.S. government has never successfully prosecuted anyone other than a government employee for disseminating unlawfully leaked classified information . . . .") (quoting Steven Aftergood, Director of the Project on Government Secrecy for the Federation of American Scientists)).

283. *Report on Review of News Media Policies*, U.S. DEP'T OF JUST. 1 (July 12, 2013), https://www.justice.gov/sites/default/files/ag/legacy/2013/07/15/news-media.pdf [https://perma.cc/F47A-EH25].

284. *Id.*

285. Zachary Roth, *Holder: I Won't Send Journalists to Jail for Doing Their Job*, MSNBC (Oct. 14, 2014), http://www.msnbc.com/msnbc/holder-i-wont-send-journalists-jail-doing-their-job [https://perma.cc/2VQS-HDYZ].

286. Michael Calderone, *Jeff Sessions Doesn't Commit to Not Jailing Journalists for*

Section 793(e) of the Espionage Act worries journalists the most. It is worth quoting in full:

> 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 same and fails to deliver it to the officer or employee of the United States entitled to receive it[.][287]

Willful retention and communication of national defense information is effectively the job description of many journalists in the Washington, D.C. area. When Dana Priest published a series of articles in the *Washington Post*, beginning in 2004, revealing a "secret world of U.S. interrogation"—CIA black sites at which prisoners were interrogated and often tortured—she violated the Espionage Act on its face.[288] After all, Priest had unauthorized possession of national defense information (she and her frequent co-author Joe Stephens had carried out extensive investigative reporting, which included talking to government officials about highly classified programs). And she knew that publishing the story would "communicate" the information to the public, which was not "entitled" to receive it, because the information remained classified. She moreover knew that doing so could "be used to the injury of the United States"—the revelation that the United States was running an extensive program of torture harmed the image of the United States world-wide and forced the halt of the programs she detailed. But she was not prosecuted, at least in part because of

---

Doing Their Jobs, HUFFPOST (Jan. 10, 2017), https://www.huffpost.com/entry/jeff-sessions-comments-jailing-journalists_n_58753d8ee4b02b5f858ba2a2 [https://perma.cc/63E5-XGTQ] (responding to Sen. Amy Klobuchar's question about whether or not he would jail reporters, Sessions responded, "I'm not sure, I have not studied those regulations"); Li Zhou, *Attorney General Nominee William Barr Doesn't Reject the Possibility of Jailing Journalists*, VOX (Jan. 15, 2019), https://www.vox.com/policy-and-politics/2019/1/15/18183952/amy-klobuchar-william-barr [https://perma.cc/5A3D-5Z9W] (saying jailing a reporter for doing their job would likely be a "last resort").

287. 18 U.S.C. § 793(e).

288. *See, e.g.*, Dana Priest & Joe Stephens, *Secret World of U.S. Interrogation*, WASH. POST (May 11, 2004), https://www.washingtonpost.com/archive/politics/2004/05/11/secret-world-of-us-interrogation/7e39ee61-7539-4c8c-a536-a63a57ccad80 [https://perma.cc/AS5V-DLRP]. Priest won the Pulitzer Prize for this work in 2006. *See Dana Priest of The Washington Post*, PULITZER, https://www.pulitzer.org/winners/dana-priest [https://perma.cc/5CV7-CGGT] (listing several pieces from the series published in 2005).

the longstanding policy of respecting the freedom of the press by not enforcing the law against journalists.[289]

But will that policy remain? Whatever one may think of Assange, the government's decision to indict him on Espionage Act charges raises worrying signs that a policy that has long protected the nation's press is fragile. Indeed, not long after President Joe Biden took office, there were disclosures that under President Trump the Justice Department had secretly taken aggressive steps to identify reporters' confidential sources. President Biden ordered prosecutors to stop, but the revelations have left lingering questions about how secure those protections might be.[290]

C. SELECTIVE PROSECUTION

There is so much classified information in so many millions of peoples' hands that there are inevitably millions of possible violations of the Espionage Act and the various other criminal statutes monitoring the release of classified information. Of course, not every possible violation faces sanction—in truth, very few do. Leak cases are perceived as difficult to prosecute. But to point out that the rules are only rarely enforced is not a defense of those rules. It suggests instead that the rules are not as necessary as they might seem. And the lack of clarity about when and where they will be enforced contributes to the sense of vulnerability among those who worry that they may be covered by the overbroad legal prohibitions.

The potentially vast scope of criminal liability can open the door, moreover, to selective prosecution. As a result, this systematic overclassification creates tools that could be used to crack down on political opposition by those in power, on journalists doing their jobs, and even on former government officials. Here I examine two cases that illustrate these dangers.

---

289. *See* Interview by Philip Bennett with Dana Priest, Investigative Reporter, Wash. Post (Oct. 19, 2009), https://livinghistory.sanford.duke.edu/interviews/dana-priest [https://perma.cc/KA2Y-KWF3] (discussing her conflicting feelings when publishing her Pulitzer Prize winning articles in the early 2000s); *supra* text accompanying notes 282–85.

290. Charlie Savage, *Garland Confronts Long-Building Crisis over Leak Inquiries and Journalism*, N.Y. TIMES (June 12, 2021), https://www.nytimes.com/2021/06/12/us/politics/government-leaks-garland-biden-administration.html [https://perma.cc/MSZ5-V4PH] ("Among them: How broadly will prosecutors define the journalistic activities that the new protections apply to? And will the changes be easy or difficult for a future administration to roll back?").

1. Lock Her Up!

During the 2016 presidential campaign, the halls of Donald Trump's rallies rang with chants calling to "Lock her up! Lock her up! Lock her up!" The chants were fed by claims that while serving as Secretary of State, Hillary Clinton—Trump's opponent in the campaign—had set up a private email server over which she sent and received classified information from hdr22@clintonemail.com.[291]

The FBI opened an investigation after a referral from the Intelligence Community Inspector General to determine whether classified information had, in fact, been transmitted or improperly stored, making it vulnerable to foreign powers.[292] In July, just a few months before the election, FBI Director James Comey stepped to the microphone and gave what he described as an "unusual" speech describing in detail what the FBI had found: in the course of the almost year-long investigation, investigators read approximately 30,000 emails. Out of those 30,000, the FBI found 110 emails in 52 chains contained classified information at the time they were sent or received, though "[o]nly a very small number" of the emails contained classification markings that would have signaled the presence of classified information.[293] (While all documents marked classified are presumed to contain classified information, the fact that a document is unmarked does not guarantee that it does not include information that meets the standard for classification.) Eight of the chains contained information that was Top Secret, thirty-six contained information that was Secret, and eight

---

291. Michael S. Schmidt, *String of Emails Raises Questions About When Hillary Clinton Began Using Personal Account*, N.Y. TIMES (Sept. 25, 2015), https://www.nytimes.com/2015/09/26/us/politics/string-of-emails-raises-questions-about-when-hillary-clinton-began-using-personal-account.html [https://perma.cc/YT4G-8M9A]; Peter W. Stevenson, *A Brief History of the "Lock Her Up!" Chant by Trump Supporters Against Clinton*, Wash. Post (Nov. 22, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/11/22/a-brief-history-of-the-lock-her-up-chant-as-it-looks-like-trump-might-not-even-try [https://perma.cc/3NYM-HR6E]. ("His fans broke out in the chant at any mention of the Clinton Foundation, the email server or any other of his attacks on her.").

292. Less widely noted was the fact that the use of a private email address also created the possibility that her emails would not be preserved, violating federal rules that require federal records—including emails—to be preserved (and thus available for FOIA). *See* OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF STATE, NO. ESP-16-03, OFFICE OF THE SECRETARY: EVALUATION OF EMAIL RECORDS MANAGEMENT AND CYBERSECURITY REQUIREMENTS 4 (2016).

293. James B. Comey, *Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System*, FBI (July 5, 2016), https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system [https://perma.cc/TVW3-Y949].

contained Confidential information. In addition to the 30,000 emails, there were thousands that were not provided to the government by Secretary Clinton's lawyers, but which the FBI found through other means. Of these, three were classified—one at the Secret level and two at the Confidential level. Though it found no direct evidence that hostile powers had accessed Secretary Clinton's email account, Comey stated that the FBI assessed that it was "possible" that they had.[294]

Comey announced that the FBI had recommended against bringing charges against Secretary Clinton or any of her colleagues. The FBI had not found "clear evidence" that Secretary Clinton or her State Department colleagues intended to violate laws governing the handling of classified information. To be sure, there was evidence that they were "extremely careless in their handling of very sensitive, highly classified information."[295] But he explained that "we cannot find a case that would support bringing criminal charges on these facts."[296] Prior cases, he explained, involved some combination of "clearly intentional and willful mishandling of classified information," "vast quantities of materials exposed in such a way as to support an inference of intentional misconduct," "indications of disloyalty to the United States," or "efforts to obstruct justice."[297]

Demonstrating intent is, of course, considerably more complicated in situations like Secretary Clinton's, where almost none of the classified information was marked classified. Comey announced that the FBI had found that she "should have known" that the information was classified, but the FBI apparently did not conclude that it was so clear as to be prosecutable.[298]

But what about gross negligence?[299] Indeed, Comey called Clinton's actions "extremely careless."[300] But he also noted that there was no direct evidence that the information had, in fact, been accessed by

294. *Id.*

295. *Id*.

296. *Id.*

297. *Id.*

298. *Id.*; *see* 18 U.S.C. § 793(d) (providing for criminal liability if one "willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" national defense information).

299. *See* 18 U.S.C. § 793(f) (providing for criminal liability for permitting mishandling of national defense information "through gross negligence").

300. James B. Comey, *Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System*, FBI (July 5, 2016), https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system [https://perma.cc/TVW3-Y949].

a foreign adversary.[301] He thought it was likely, but he could not show, that the classified information in the servers had been "removed from its proper place of custody or delivered to anyone in violation of [her] trust."[302]

After the episode—which may have played a role in Clinton's electoral loss to Donald Trump—it came to light that several of her predecessors had used private email accounts, including to send information later deemed classified.[303] What's more, seven members of Trump's own team, including Jared Kushner and Ivanka Trump, used personal email accounts or the messaging application WhatsApp to conduct official business.[304] When Kushner's attorney was asked whether Kushner had shared classified information using WhatsApp, he answered, "that's above my pay grade."[305] The FBI did not investigate, and no one was charged.

2. Reality Winner

In 2016, Reality Winner left the Air Force after working there for six years, mostly as a cryptologic linguist assigned to listen to intercepted foreign chatter in Persian, Dari, and Pashto to provide U.S. forces with intelligence. She received an Air Force Commendation Medal for "aiding in 650 enemy captures, 600 enemies killed in action and identifying 900 high value targets."[306] After leaving the Air Force,

---

301. *See A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election*, OFFICE OF INSPECTOR GEN., U.S. DEP'T OF JUSTICE 26–36 (June 2018), https://www.justice.gov/file/1071991/download [https://perma.cc/955K-J8QT] (discussing the reasons for the rules).

302. 18 U.S.C. § 793(f); *see A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election*, *supra* note 301, at 193 ("[H]er use of the private server was 'really sloppy, but it doesn't rise to the level of prosecution'").

303. *See, e.g.*, David Smith, *Colin Powell and Condoleezza Rice Used Private Accounts for Classified Emails*, GUARDIAN (U.K.) (Feb. 4, 2016), https://www.theguardian.com/us-news/2016/feb/04/colin-powell-condoleezza-rice-private-email-accounts-classified-hillary-clinton [https://perma.cc/Q7H2-EAWL] (naming high-level government officials who received classified information on personal accounts).

304. *See* Philip Bump, *But Their Emails: Seven Members of Trump's Team Have Used Unofficial Communication Tools*, WASH. POST (Mar. 21, 2019), https://www.washingtonpost.com/politics/2019/03/21/their-emails-seven-members-trumps-team-have-used-unofficial-communications-tools [https://perma.cc/67BA-X4JD] ("It wasn't just Kushner and Ivanka Trump. The committee learned that former deputy national security adviser K.T. McFarland and former adviser Stephen K. Bannon had also, at times, used personal email accounts for official business.").

305. *Id.*

306. Johnny Edwards, *Air Force Commended Reality Winner for Taking out Enemy*

Winner was hired by an intelligence contractor in Augusta, Georgia. There, she saw a Top Secret government report on Russian hacking. The report detailed hacking attacks by Russian intelligence against local election officials and voter registration databases.

On May 9, 2017, upset by what she had read in the report, which detailed Russian government efforts to penetrate a voting software supplier and the accounts of election officials ahead of the 2016 election, she printed it out, folded it up, and smuggled it out in her pantyhose. She then mailed it to the online news source, *The Intercept*. *The Intercept* contacted the NSA to confirm the veracity of the report before publishing it. Finding it was indeed a leaked Top Secret document, the NSA notified the FBI, which went looking for the person who leaked it. It was not difficult to track down Winner. The copies sent to the NSA by *The Intercept* showed that the pages "appeared to be folded and/or creased, suggesting they had been printed and hand-carried out of a secured space."[307] Winner was one of six people who printed the report in the relevant time period, and she was the only one of the six to have emailed *The Intercept* from her work computer.[308] In addition, the printer she used reportedly placed microdots in the background, which made it possible to identify the serial number of the printer.[309]

Two days before *The Intercept* published the report, the FBI arrested Winner.[310] Pictures of her that suddenly flooded the news showed a young woman with blond hair and a knowing half smile. Winner was charged with violating the Espionage Act. To win a conviction under the Act, the government has to establish that the person had lawful possession of documents or "information relating to the national defense."[311] And it has to show the person willfully communicated, delivered, or transmitted the document or information to

---

Combatants, ATLANTA J.-CONST. (June 7, 2017), https://www.ajc.com/news/national/air-force-honored-reality-winner-for-taking-out-enemy-combatants/XoEbupm6P318Eun9ZGOo1O [https://perma.cc/TP67-JHPH].

307. *Id.*; Arrest Warrant at 5, United States v. Winner, 464 F. Supp. 3d 1575 (S.D. Ga. 2020) (No. 1:17-MJ-024).

308. *See* Complaint at 5, United States v. Winner, 464 F. Supp. 3d 1575 (S.D. Ga. 2020) (No. 1:17-MJ-024).

309. *See* David Gilbert, *NSA Leak Suspect Was Ratted Out by an Office Printer*, VICE NEWS (June 6, 2017), https://www.vice.com/en/article/vbznza/nsa-leak-suspect-was-ratted-out-by-an-office-printer [https://perma.cc/M288-LMQY].

310. *See* Dave Philipps, *Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report*, N.Y. TIMES (Aug. 23, 2018), https://www.nytimes.com/2018/08/23/us/reality-winner-nsa-sentence.html [https://perma.cc/49NL-DZAD].

311. 18 U.S.C. § 793(d).

someone not entitled to receive it.[312] Winner admitted to the FBI that she knew exactly what she was doing. In June 2018, she pleaded guilty to a single count of transmitting national security information, and in August she was sentenced to more than five years in jail.[313] She was granted good behavior release to a halfway house in June 2021 and is scheduled for full release in November.[314]

Reactions were mixed. On the one hand, the five-year sentence for the leak of a single document seemed like a hefty penalty. That was particularly true given the contrast with General David Petraeus, former director of the CIA, who engaged in what many security professionals considered to be the more shocking and dangerous abuse. The salacious details have been covered in the press: when he was serving as director of the CIA, General Petraeus took home eight personal notebooks in which he had recorded highly sensitive information, including code words for classified intelligence programs, information about military strategy, discussions with other members of the National Security Council, and even the identities of covert officers.[315] This information is among the most highly protected and most jealously guarded in the U. S. government. As director of the CIA, Petraeus had access to information that very few in government ever see, aside from the president. He then gave the notebooks containing highly classified information to Paula Broadwell, his biographer, and, as it would later turn out, his mistress.[316] Even though the government had pre-

312. *See id.* If the disclosure is of intangible information (rather than, say, a document), the government also must show that the person had reason to believe the information could be used to the injury of the U. S. or to the advantage of a foreign nation. *See id.* It is also insufficient to show that the information was classified to show that it is "information relating to the national defense." United States v. Rosen, 599 F. Supp. 2d 690, 692–93 (E.D. Va. 2009). Because Winner had disclosed a document, these limitations did not apply to her case.

313. *See* Philipps, *supra* note 310.

314. Julian E. Barnes, *Reality Winner, Who Leaked Government Secrets, Is Released From Prison*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/14/us/politics/reality-winner-is-released.html [https://perma.cc/Z7T6-BFD6].

315. *See* Adam Goldman, *How David Petraeus Avoided Felony Charges and Possible Prison Time*, WASH. POST (Jan. 25, 2016), https://www.washingtonpost.com/world/national-security/how-david-petraeus-avoided-felony-charges-and-possible-prison-time/2016/01/25/d77628dc-bfab-11e5-83d4-42e3bceea902_story.html? [https://perma.cc/88L7-CZE2].

316. *See* Justin Miller & Nancy A. Youssef, *Petraeus Mistress Got Black Books Full of Code Words, Spy Names, and Obama Briefings,* DAILY BEAST (Apr. 14, 2017), https://www.thedailybeast.com/petraeus-mistress-got-black-books-full-of-code-words-spy-names-and-obama-briefings [https://perma.cc/AW6J-ZLWU] (detailing Petraeus's unauthorized removal and retention of classified material in connection with his affair with Broadwell).

pared to charge Petraeus with lying to the FBI and violating the Espionage Act, Petraeus was allowed to plead guilty to a misdemeanor charge of mishandling classified information.[317] He received a two-year probationary period and a fine of $100,000.[318]

Winner's five-year sentence for what, on the face of it, was a much less severe violation, seems disproportionate. The disparities between the two raise questions about whether Winner's harsh treatment might have been politically motivated. Might she have been treated more harshly merely because President Trump was eager to keep information about Russian election tampering from 2016 out of the public eye? It is impossible to know.

The occasional prosecution of low-level violations like Winner's serves to create fear among those who work with classified information that they, too, could be exposed to criminal liability. While Winner's actions were intentional and unmistakably prosecutable, ordinary government workers with classified access see a massive amount of classified information that makes it difficult for them to engage with those outside of government without fear of disclosing classified information and thus opening themselves up to criminal charges and other penalties. The prepublication review system, which in theory could serve a valuable purpose of allowing current and former government officials to ensure that their writing and public engagements will not disclose classified information, has in reality served to discourage and silence them, impoverishing public discourse in the process.

D. SILENCING CURRENT AND FORMER GOVERNMENT OFFICIALS

If the press is silenced, what about current and former government officials who did not obtain *unauthorized access* to information because they had *authorized* access? It turns out that they are silenced too.

As already noted, the Espionage Act has been used only three times against those not affiliated with the government—which of course means that every other indictment under the Act has been

317. *See* 18 U.S.C. § 1924; *see also* United States v. Petraeus, No. 3:15-CR-047-DCK, 2015 WL 3606028, at *1 (W.D.N.C. Mar. 3, 2015).

318. *See* Bill Chappell, *Petraeus Sentenced to 2 Years' Probation, Fine for Sharing Classified Info*, NPR (Apr. 23, 2015), https://www.npr.org/sections/thetwo-way/2015/04/23/401672264/gen-david-petraeus-will-be-sentenced-Thursday-over-secret-notebooks [https://perma.cc/8THA-NSYD] ("The charge's maximum possible punishments include a fine of $100,000 and a one-year prison sentence. Instead, prosecutors agreed that Petraeus should serve a two-year probation and pay a fine of $40,000.").

against those *affiliated with the government*. A separate provision of the Act prohibits anyone from "knowingly and willfully" communicating classified information in any manner that might harm the U.S. or benefit a foreign government.[319]

That such rules apply to disclosure of information by current government officials makes some sense—after all, they have up-to-the-minute access to classified information that could, in some cases, do real damage to national security. Arguably the rules on disclosure are not so much the problem here so much as is the scope of classified information, which has the effect of making it difficult for a government official to discuss anything of significance with *anyone* outside of government (or even those within government who are not cleared into the same programs). But major restrictions apply to millions of *former* government officials as well. And it is no exaggeration to say that the rules are at times Kafkaesque.[320]

Even after leaving government, former employees are not only subject to potential criminal prosecution if they disclose classified information that they learned while in government. As noted above, they are also supposed to submit their writings—and drafts of public talks—for prepublication review. Once a former employee submits a draft for review (which they are directed to do by sending an email to an *unclassified* email account), the department or agency is supposed to review it in a timely manner to ensure that it contains no information that could compromise U.S. national security. In practice, however, review can take months and sometimes even years. And review

319. 18 U.S.C. § 798(a).

320. See Jack Goldsmith & Oona A. Hathaway, Opinion, *The Government's Prepublication Review Process Is Broken*, WASH. POST (Dec. 25, 2015), https://www.washingtonpost.com/opinions/the-governments-prepublication-review-process-is-broken/2015/12/25/edd943a8-a349-11e5-b53d-972e2751f433_story.html [https://perma.cc/C2TB-VFPQ], for a discussion of prepublication review. *See also* Jack Goldsmith & Oona Hathaway, *More Problems with Prepublication Review*, LAWFARE (Dec. 28, 2015), https://www.lawfareblog.com/more-problems-prepublication-review [https://perma.cc/CT84-Q8RD]; Oona Hathaway & Jack Goldsmith, *Path Dependence and the Prepublication Review Process*, JUST SEC. (Dec. 28, 2015), https://www.justsecurity.org/28552/path-dependence-prepublication-review-process [https://perma.cc/6DHC-FXUF]; Jack Goldsmith & Oona Hathaway, *The Scope of the Prepublication Review Problem, and What to Do About It*, LAWFARE (Dec. 30, 2015), https://www.lawfareblog.com/scope-prepublication-review-problem-and-what-do-about-it [https://perma.cc/S3JJ-ESZD]; Oona Hathaway & Jack Goldsmith, *Important First Step by HPSCI on Pre-Publication Review Reform*, JUST SEC. (May 26, 2016), https://www.justsecurity.org/31279/important-step-hpsci-pre-publication-review-reform [https://perma.cc/E28H-42SL]; Oona Hathaway & Jack Goldsmith, *Disappointing DOD Inspector General Report on Pre-Publication Review*, JUST SEC. (June 23, 2016), https://www.justsecurity.org/31636/disappointing-dod-inspector-general-report-pre-publication-review [https://perma.cc/A46S-QLWD].

is often not limited to national security concerns. It is well known that writings that express views favorable to government often get preferential treatment and those unfavorable to the government are sometimes held longer.[321] John Bolton became the unexpected poster boy for this kind of politicization of the prepublication review process when his book was subject to delays that appeared politically motivated.[322] Submitted manuscripts may circulate extensively, moreover, not only within the original department or agency but in other parts of the government as well, particularly if the subject of a manuscript involves "interagency equities."[323] At the end of the process, the agency reviewing the manuscript may approve it for publication as is, approve it with revisions, or reject publication altogether.[324] A recent lawsuit by the Columbia University Knight Institute illustrates the problem.[325] All of the plaintiffs in the suit are former government employees who had held security clearances. They all submitted book manuscripts for pre-publication review and were subject to lengthy review processes and negotiations over redactions—many of them ultimately determined not to be justified as necessary to protect classified information.

Former government employees are often unsure of the scope of the duty to submit their work for prepublication review. In my own experience, the Department of Defense was unwilling to ever say that a document was *not* subject to review or to offer any clear guidelines about what written materials I should and should not submit. Perhaps the most absurd example I experienced firsthand was an op-ed that I co-authored with another former employee of the Department, Jack Goldsmith. The subject? The government's prepublication review process. Instead of telling us that the piece need not be reviewed, because

321. Goldsmith & Hathaway, *The Scope of the Prepublication Review Problem, and What to Do About It*, *supra* note 320; Goldsmith & Hathaway, *More Problems with Prepublication Review*, *supra* note 320; Brief of Professors Jack Goldsmith & Oona Hathaway as Amici Curiae Supporting Appellants & Reversal, *supra* note 215, at 3.

322. *See* Charlie Savage, *Government Lawsuit over John Bolton's Memoir May Proceed, Judge Rules*, N.Y. TIMES (Oct. 1, 2020), https://www.nytimes.com/2020/10/01/us/politics/john-bolton-book-proceeds-lawsuit.html [https://perma.cc/2S4G-9HER] ("Political appointees of Mr. Trump prevented Ms. Knight from sending . . . [a publication approval] letter.").

323. *See* Complaint at 11, Edgar v. Coats, 454 F. Supp. 3d 502 (D. Md. 2020) (No. 8:19-cv-00985-GJH). The Fourth Circuit affirmed the District Court holding that the defendant agencies' prepublication review regimes do not violate the First Amendment. Edgar v. Haines, 2 F.4th 298 (4th Cir. 2021).

324. *See id.* at 9.

325. *See id.* at 2 ("[M]any would-be authors self-censor, and the public is denied access to speech by former government employees that has singular potential to inform public debate.").

it obviously contained no classified information, the Department implicitly found that we had a duty to submit when it approved publication only on the condition that we attach a disclaimer that the views expressed in the op-ed were our own and did not reflect the official policy or position of the Department of Defense or the U.S. government.[326] It took the Department roughly a month to review the 800 word draft and arrive at that conclusion.

Former government employees respond to the problems with the review process in one of two ways. Some decide the system is so unreasonable and cumbersome that they choose to ignore it, accepting the risk that comes as a result. Others choose silence. Wanting to comply and fearful of harming their reputations or careers, many former government employees simply don't write or speak at all.[327]

The real harm, however, is not to former government employees. It is to the quality of public discourse. If those who have actually worked on national security issues are unable to speak or write without subjecting themselves to a cumbersome system of prior review or accepting the risk of violating inconsistent and unclear rules, many will choose to stay silent. That means less and less accurate information will be available to members of the public as they seek to understand and evaluate the actions taken by the government on their behalf.

E. COSTS TO NATIONAL SECURITY

That the system of government secrecy imposes costs on democratic values wouldn't come entirely as a surprise to those paying attention to the field of national security. Many who work in the field would say that these costs are real but that they are necessary to bear because the system protects the country's national security. But what if that is not the case? What if the system of secrecy undermines national security too?

326. Goldsmith & Hathaway, *The Scope of the Prepublication Review Problem, and What to Do About It*, *supra* note 320; Goldsmith & Hathaway, *More Problems with Prepublication Review*, *supra* note 320.

327. While not a formal exemption, many interpret the prepublication rules not to apply to extemporaneous speech. This can open the door to some participation in the public sphere, but it of course raises a question of inconsistency: why require review of a planned speech and not of one where a former official plans to speak off the cuff?

1. "When everything is classified, then nothing is classified"[328]

To begin with, keeping secrets from the public and thus generating distrust in the government, as detailed above, can harm national security. The government needs public trust to govern. When the public no longer trusts government institutions, it is much less likely to cooperate on a range of government programs—including law enforcement and counterterrorism.[329] Moreover, because classification leads to a less informed public, it can undermine support for effective government programs: if the public does not understand the real nature of our security environment, and is unable to evaluate whether decisions made are good or bad (perhaps because it does not know about them at all), it cannot accurately hold officials to account for poor decisions. The democratic corrective is unable to function in an information-poor environment.

But there are more direct effects as well. Generating roughly 50 million new classified documents per year, while declassifying only a fraction of that number, means that the edifice of classified material continues to grow.[330] This has several consequences. Given how much is classified, millions of people need to have classification access in order to simply do their jobs. In October 2017, 4,030,625 people held security clearances—or 1.2 percent of the entire U.S. population.[331] If 1.2 percent of the U.S. population has access to classified information, it's hard to defend the idea that the information is truly secure. Even if they are rigorous in following their obligations and do not intentionally divulge information to which they have access, each of them is a point of vulnerability for adversaries seeking to gain unauthorized access.

When government keeps too many secrets, it is difficult to keep the secrets that really matter. As Justice Potter Stewart put it in his concurring opinion in the case ordering the release of the so-called Pentagon Papers (a classified history of the United States' political and military role in Vietnam from 1945 to 1967 produced by the Depart-

328. N.Y. Times Co. v. United States, 403 U.S. 2140, 2149 (1971) (Stewart, J., concurring).

329. *See, e.g.*, Tom R. Tyler, Stephen Schulhofer & Aziz Z. Huq, *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 L. & SOC'Y REV. 365, 370 (2010).

330. *See 2016 ISOO Report*, *supra* note 127, at 8.

331. Nat'l Counterintelligence & Sec. Ctr., *supra* note 131, at 5. If anything, that number has grown since then. A report from 2019 shows 4,243,937 people held security clearances. *See* NCSC, Fiscal Year 2019 Annual Report on Security Clearance Determinations, *supra* note 1.

ment of Defense and later leaked to the *New York Times* and *Washington Post*): "[w]hen everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion."[332] In fact, Justice Stewart observed, "the hallmark of a truly effective internal security system would be the maximum possible disclosure 'since' secrecy can best be preserved only when credibility is truly maintained."[333] That is more true today than when Justice Stewart wrote, for today the United States' adversaries have sophisticated tools for gaining access through compromising cyber security. More secrets mean more people with access to secrets—which in turn increases vulnerability.

Indeed, the huge amount of classified information has meant that the government must hire private contractors to store and manage much of that information. This, in turn, has led to greater vulnerability. Consider the case of Edward Snowden, the former CIA employee who copied and leaked 1.5 million documents from the NSA in 2013.[334] Snowden began downloading documents on the government's electronic spying programs in April 2012, while working for Dell. The government had to hire Dell—and a number of other outside subcontractors—because there was just more secret information than it could possibly handle on its own. When the information copied by Snowden leaked, the world witnessed some of the absurdity of the classification system. There were tens of thousands of mundane documents with uninteresting and unimportant information whose disclosure had no discernable impact on U.S. national security. But nestled among those mundane documents were some true national security secrets—some of the most damaging were details related to CIA sources whose lives were put at risk by the disclosure. The disclosures also are said to have provided Russia and China more technical details about NSA surveillance programs and may have contributed to a switch by terrorist groups away from monitored communication networks.[335] If the mundane documents had been left unclassified and the real secrets—those

332. *N.Y. Times Co.*, 403 U.S. at 2149 (Stewart, J., concurring).

333. *Id.*

334. *See* Luke Harding, *How Edward Snowden Went from Loyal NSA Contractor to Whistleblower*, GUARDIAN (U.K.) (Feb. 1, 2014), https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract [https://perma.cc/VB9V-HFY3] (explaining the methods and sequence of Snowden's illegal disclosures).

335. *See* Eric Schmitt & Michael S. Schmidt, *Qaeda Plot Leak Has Undermined U.S. Intelligence*, N.Y. TIMES (Sept. 29, 2013), https://www.nytimes.com/2013/09/30/us/

whose disclosure could do real harm—were the only secrets the government worked to keep, the important information would have been much less likely to be revealed.

2. Classification Can Breed Sloppiness and Vulnerability

Another drawback of classification is that it may breed sloppiness and thus vulnerability. Those in government may assume that as long as information is classified, it is automatically protected. They may feel confident sharing it widely, as long as they share it only with those who have authorized access. Yet this assumption may be mistaken. The more widely distributed information is, even if on a classified system and to those with proper access, the more vulnerable it is likely to be. In the absence of classification, it is possible that those who have information they believe to be important to U.S. national security might be more cautious about broadcasting it.

It is difficult to document, but it may also be that the system of classification might have led to less careful efforts to address basic cyber vulnerabilities—in both classified and unclassified systems. The 2014 Office of Policy Management (OPM) hack, which compromised the personnel data of persons who had gone through the security clearance process (including me), took place in part because the office had failed to institute simple security measures, including two-factor authentication. OPM only implemented two-factor authentication in January 2015, after the network had been badly compromised.[336]

What's more, the classification system may actually prove counterproductive. If government computer systems are vulnerable to foreign hackers, as seems to be the case,[337] the argument can be made

qaeda-plot-leak-has-undermined-us-intelligence.html [https://perma.cc/G4EF-BNLS] ("[T]he level of intercepted communications will continue to fall as terrorists most likely find new ways to communicate with one another.").

336. *See* Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO (Feb. 12, 2020), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html [https://perma.cc/9H8C-G4GC] (explaining how the "two-factor authentication scheme" functions).

337. *See, e.g.*, David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (May 10, 2021), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html [https://perma.cc/B6EU-DPY9] ("[O]ne of the most sophisticated and perhaps largest hacks in more than five years."); *see also* Greg Myre, *U.S. Security Agencies: Massive Computer Hack Is 'Likely Russian'*, NPR (Jan. 5, 2021), https://www.npr.org/2021/01/05/953677826/u-s-security-agencies-massive-computer-hack-is-likely-russian [https://perma.cc/BP83-CXPZ] ("Microsoft . . . identified 40 government agencies . . . that have been infil-

that the classification system may largely serve to curate information for our enemies—pointing them in the direction of the more valuable information.

3. Secrecy and Compartmentalization Lead to Bad Decisions

Too much secrecy not only makes it hard to protect the secrets that matter. It can also frustrate efforts to protect the American public from national security threats by limiting information sharing that can inform decision-making and unearth new dangers. Recall the debate over secrecy during the development of the nuclear bomb discussed in Part I. The scientists brought on to work on the project were worried they couldn't do science in the absence of the ability to consult with those both inside and outside government. The government largely overcame that problem by simply hiring most of the top scientists in the country working at the cutting edge of the relevant fields. But that solution is not generally feasible (or desirable). Today the government is facing the same problem across a range of fields. In many cases, it has had to grant security clearances to a number of outside scientists in order to access their expertise, but this limits who can be brought into the conversation and thus slows scientific progress.[338]

Much classified information, including some of the most highly classified information, is "compartmented." As noted earlier, compartments are often identified by codewords—which are themselves classified: those "read in" to a sensitive compartment are the only ones who are even supposed to know the codeword that identifies the compartment. Compartments make information less vulnerable to attack (if an adversary compromises one compartment, it doesn't necessarily have access to another).[339]

---

trated."); David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. TIMES (May 28, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html [https://perma.cc/B349-27N8] ("[The intrusion] raised questions about how and why the nation's cyber defenses failed so spectacularly.").

338. *See* Julian E. Barnes, *Spy Agencies Turn to Scientists as They Wrestle with Mysteries*, N.Y. TIMES (July 8, 2021), https://www.nytimes.com/2021/07/08/us/politics/intelligence-agencies-science.html [https://perma.cc/6EWA-K5TL] ("While scientific research has been a strength of American intelligence agencies . . . the current problems may require a different approach, bringing in more people from outside.").

339. *See* Controlled Access Program Coordination Off., *Intelligence Community Authorized Classification and Control Markings: Register and Manual, Version 5.1*, OFF. OF THE DIR. OF NAT'L INTELL. 39–71 (2011), https://www.dni.gov/files/documents/FOIA/Public_CAPCO_Register%20and%20Manual%20v5.1.pdf [https://perma.cc/EDY3-R3E8].

Such compartments are created to keep information secured inside, but they also serve to keep those with clearance into those compartments penned in. Government officials who are "read in" to the compartments are unable to share what they know with those who might have insights who are not. That is not only true of experts outside government, but also of those in government who are not cleared into the relevant compartment. This means that the expertise within government that can be drawn upon depends a great deal on how the compartment is defined and who is granted access. A compartment, for example, may be defined based on a particular country. Those working on that program cannot consult outside experts on the country, but they also likely cannot speak with experts on the region within government to determine, for example, what the reaction could be to a proposed operation. That self-imposed blindness can lead to ill-informed decisions on the most important and sensitive national security matters.

The case of satellite imagery is an all-too rare instance in which information was moved out of SCI in bulk, to make it more accessible. For many years, satellite imagery was designated SCI. A former government official explained to me, "we convinced Bill Casey, then DCI, to move some 80% of this product to simply 'Secret' so that it could be utilized by the military and others who needed it and did not have SCI access. He did it with the stroke of a pen and nothing bad happened that we know of."[340]

The compartmentalization of information about the most sensitive national security programs limits government officials' ability to identify new and unexpected threats that don't fit neatly within preexisting boxes. Indeed, a key reason the September 11 attacks were not detected in advance, the September 11 Commission found, was *too much secrecy*. Thomas Kean, chairman of the September 11 Commission, and a former Republican governor of New Jersey, said that barriers to sharing information between agencies and with the public led to the intelligence community's failure. "We're better off with openness. The best ally we have in protecting ourselves against terrorism is an informed public."[341]

Secrecy also serves to insulate bureaucratic decisions from criticism and oversight, making it more difficult to identify and correct

340. E-mail from Abraham Wagner to Oona Hathaway, *supra* note 138.

341. *See* Scott Shane, *Increase in the Number of Documents Classified by the Government*, N.Y. TIMES (July 3, 2005), https://www.nytimes.com/2005/07/03/politics/increase-in-the-number-of-documents-classified-by-the-government.html [https://perma.cc/9K3J-H3LL] (citing examples of excessive secrecy).

mistakes. As one of the most famous scholars of bureaucracy and a founder of the field of sociology, Max Weber, observed, "Bureaucratic administration always seeks to evade the light of the public as best it can, because in so doing it shields its knowledge and conduct from criticism."[342] I saw this when I worked at the Pentagon: some documents and decisions were kept secret not so much because revealing them would cause grave harm to national security, but because it was easier. But insulating decision-making from outside critique can lead to "groupthink" and, as a result, to bad decisions.[343] As former head of the Office of Legal Counsel at the DOJ once said of the Bush Administration's secret surveillance program, "There's no doubt that the extreme secrecy . . . led to a lot of mistakes."[344]

4. The System Does Not Protect Much of the Information Most Worth Protecting

Last, the classification scheme does not protect much of the information that is most worth protecting: the intellectual property, confidential business information, and other key data held in private hands.

This problem is not new. In 1991, Robert Gates, then director of the CIA, sent the CIA to uncover "foreign economic espionage in the United States and gathering information about the attempts of other governments to violate international trade agreements and 'other basic rules of fair play.'"[345] A story in *Foreign Affairs*, entered into the Congressional Record by Senator Arlen Specter, reported that "[o]ver

342. Scott Horton, *Weber — 'Official Secrets' and Bureaucratic Warfare*, HARPER'S MAG. (July 18, 2009), https://harpers.org/2009/07/weber-official-secrets-and-bureaucratic-warfare [https://perma.cc/KFP2-Y437] (quoting MAX WEBER, WIRTSCHAFT UND GESELLSCHAFT [ECONOMY AND SOCIETY] 730–31 (S.H. trans. 1918)). He continued: "The concept of the 'official secret' is the specific invention of bureaucracy, and nothing is so fanatically defended by the bureaucracy as this attitude, which cannot really be justified beyond [a few] specifically qualified areas." *Id.*

343. *See* IRVING L. JANIS, VICTIMS OF GROUPTHINK: PSYCHOLOGICAL STUDIES OF POLICY DECISIONS AND FIASCOES 74 (2d ed. 1972) ("[A]dhering to a set of norms that were promoted by the leader . . . enabled the members to maintain a sense of group solidarity at the expense of suffering from many of the major symptoms of groupthink.").

344. *Preserving the Rule of Law in the Fight Against Terrorism: Hearing Before the S. Comm. on the Judiciary,* 110th Cong. 9 (2007) (statement of Jack L. Goldsmith, Professor of Law, Harvard Law School). For more on the dangers of "groupthink," see JANIS, *supra* note 343, at 206. Similarly, see Daphna Joel, Yael Niv & Eytan Ruppin, *Actor-Critic Models of the Basal Ganglia: New Anatomical and Computational Perspectives*, 15 NEURAL NETWORKS 535, 544 (2002) for a discussion on how the Actor-Critic model has found that combining an "actor"—a cerebral component that decides which action to take—with a "critic"—a cerebral component that provides critical feedback on the action—is key to human reinforcement learning and for machine learning, as well.

345. Peter Schweizer, *The Growth of Economic Espionage: America Is Target Number One*, 75 FOREIGN AFF. 9, 10–11 (1996).

the past 15 years, the FBI has chronicled numerous cases involving France, Germany, Japan, Israel, and South Korea. An FBI analysis of 173 nations found that 57 were covertly trying to obtain advanced technologies from U.S. corporations. Altogether, 100 countries spent some public funds to acquire U.S. technology."[346]

In 2009, for example, Dongfan "Greg" Chung was discovered to have sent key aerospace technology to the Chinese government for decades.[347] Mr. Chung worked for decades as an employee at Boeing and related companies in the United States. Over the course of his time at the company, "to accomplish his mission, Mr. Chung kept over 300,000 pages of documents reflecting Boeing's trade secret and proprietary information in his home."[348] Mr. Chung had taken "technical documents . . . from work by secreting them within the pages of newspapers."[349] These "documents included design drawings and diagrams, structural and material specifications, project management data, and engineering modification reports for the Space Shuttle and the International Space Station."[350] He then sent that information to a Chinese agent and to the Chinese consulate, and he used the information to prepare briefings that were presented to Chinese officials.[351] Again, none of what he stole was classified—or at least none of the charges against him claimed it was. But the harm to national security was immense.

An even more spectacular example came to light in 2018, when two Chinese hackers were criminally charged by the DOJ for "conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft . . . ."[352] The DOJ alleged that they had worked in concert with the Chinese state to target a "diverse array of . . . industries."[353] The hacking group to which they belonged, APT10,

346. *Id.*

347. *See* United States v. Chung, 633 F. Supp. 2d 1134, 1135 (C.D. Cal. 2009) (upholding the trial conviction under § 1831 of the EEA).

348. *Id.*

349. *Id.* at 1136.

350. *Id*.

351. *Id.* Upon discovery, he was charged with acting as a foreign agent, 18 U.S.C. § 951, and with six counts of possessing a trade secret with the intent to benefit China under the Economic Espionage Act—neither of which require access to classified information. *Id.* at 1137.

352. *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, DEP'T OF JUST. (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion [https://perma.cc/8RXR-2RHN].

353. *Id.*

managed to steal hundreds of gigabytes of sensitive data and information from a huge array of companies, including seven companies involved in aviation, space, and satellite technology: three involved in communications technology, three involved in manufacturing advanced electronic systems and laboratory analytical instruments, and the NASA Goddard Space Center and Jet Propulsion Laboratory. Some of the stolen information had merely economic implications—likely leading to competition from Chinese companies using the pilfered technology. But some had serious national security implications. As one government official put it in speaking of the incident, "[t]he theft of sensitive defense technology and cyber intrusions are major national security concerns . . . ."[354]

This privately held information is essential to U.S. national security—but little of it is classified. The information is protected instead by a set of criminal laws including prohibitions on computer intrusions, particularly the Computer Fraud and Abuse Act. Since 1996, companies have also relied on criminal sanctions to reinforce the protection of their trade secrets. The Economic Espionage Act of 1996 creates criminal penalties for the theft of privately held trade secrets.[355] The enactment of the law resulted from rising concern in the intelligence community that foreign economic espionage was harming U.S. competitiveness abroad. When President Clinton signed the bill into law, he declared it was meant to "protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft."[356]

But there is an immense gap that these laws do not fill—and that is the private and public information about almost everyone in the United States that is relatively unimportant if it remains disaggregated but can be a powerful national security tool if collected and analyzed in the aggregate.

A famous example of the power of aggregating information first was reported in 2012, when a customer made a complaint at Target. Target assigns its customers an ID number tied not only to their in-

354. Much, if not most, of the stolen information was not classified. Nonetheless, stealing it was a crime. They were charged not with violating the Espionage Act (or any of the other laws criminalizing the unauthorized access to classified information—again, because it is not clear that any of the information they stole was classified), but instead with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. *Id.*

355. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489.

356. Presidential Statement on Signing the Economic Espionage Act of 1996, WEEKLY COMP. PRES. DOC. 2040 (Oct. 1, 1996), *as reprinted in* 1996 U.S.C.C.A.N. 4034, 4034 (emphasis added).

store card, but also to their credit card, name, and email address. When a customer makes a purchase, that information is collected and analyzed. In 2012, a statistician working at Target figured out that he could use this data, together with purchase information from women who had set up baby registries, to determine who was likely pregnant. For example, women who were pregnant started buying unscented lotion, and they were more likely to purchase calcium, magnesium, and zinc supplements. Target was able to use this information to create a "pregnancy prediction score" and could even determine where a woman likely was in the course of her pregnancy. It could then send them coupons targeted not only to their pregnancy but to the stage of pregnancy they were in. The potential power of this technology came to public attention when an angry customer complained to a manager that it was sending mailers to his daughter clearly targeted at pregnant women. "Are you trying to encourage her to get pregnant?" he demanded. It turned out Target knew something he did not. He later called to apologize: "It turns out there's been some activities in my house I haven't been completely aware of. She's due in August. I owe you an apology."[357]

More recently, a cupcake piñata led U.S. Immigration and Customs Enforcement (ICE) to Gladys Díaz Tadeo, the undocumented mother of three daughters.[358] Diaz posted a picture of the piñata on Facebook, offering it for sale in a private buy/sell Facebook group in her area. When someone responded, she agreed to meet them at a local bank parking lot. When she arrived, it turned out her "buyers" were ICE officers armed with a printout of her Washington State driver's license. She was handcuffed in front of her daughters, detained, and deported to Mexico one week later. How, her family and friends wondered, did ICE know who she was? It turns out ICE has for years worked with Palantir, a private data firm. It has created a case management software that allows ICE agents to pull personal information not just from government databases but also from various public databases—including information such as home addresses,

357. *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [https://perma.cc/G9YR-WZ8M].

358. *See* McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES MAG. (June 7, 2021), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/A2GW-4A93].

criminal records, financial data, and more.[359] ICE has also used the Thompson Reuters "CLEAR" database, which the company describes as "powered by billions of data points and leverages cutting-edge public records technology to bring all key content together in a customizable dashboard."[360] ICE reportedly used the database to identify an undocumented immigrant when he "checked in" on Facebook at a Home Depot to buy roofing supplies.[361] They arrested him on his way out of the store.

Whatever one may think about ICE's use of these technologies, it demonstrates the power of aggregating public information for tracking the movements of people who prefer not to be found. Now imagine what could happen if a nation state combines public records with data collected, for example, in the OPM hack of private information of tens or hundreds of thousands of persons granted security clearances. And add to this other exfiltrated information—for example, gathered by China's main intelligence service when it "infiltrated more than 100 companies and organizations around the world."[362] Not only was it able to use the information to steal intelligence and extort victims, but it was able to add the information to the growing treasure trove of data held about U.S. companies, universities, government, and citizens. This kind of information, combined with evolving artificial intelligence technology that can detect patterns and identities, means that China is likely to have visibility into key people and institutions in the United States that makes our system of classification look almost silly.

Indeed, bulk data collection can enable relatively easy identification and perhaps even recruitment of U.S. intelligence agents. For example, if someone who is listed as a State Department employee frequently uses a credit card to buy gas at a station in Langley, Virginia,

---

359. Morgan Simon, *Investing in Immigrant Surveillance: Palantir and the #NoTechForICE Campaign*, FORBES (Jan. 15, 2020), https://www.forbes.com/sites/morgansimon/2020/01/15/investing-in-immigrant-surveillance-palantir-and-the-notechforice-campaign [https://perma.cc/X756-72FK].

360. *Thomson Reuters CLEAR*, THOMSON REUTERS LEGAL, https://legal.thomsonreuters.com/en/products/clear-investigation-software [https://perma.cc/324X-WKYE].

361. *See* Max Rivlin-Nadler, *How ICE Uses Social Media to Surveil and Arrest Immigrants*, INTERCEPT (Dec. 22, 2019), https://theintercept.com/2019/12/22/ice-social-media-surveillance [https://perma.cc/7QUM-BL62] ("ICE used . . .[the] CLEAR database, part of a growing industry of commercial data brokers that contract with government agencies, essentially circumventing barriers that might prevent the government from collecting certain types of information.").

362. Katie Benner & Nicole Perlroth, *China-Backed Hackers Broke into 100 Firms and Agencies, U.S. Say*s, N.Y. TIMES (Sept. 16, 2020), https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html [https://perma.cc/KEV7-X5RM].

that may indicate that the person spends a lot of time at CIA headquarters. Past travel records may show that an agent has been in places that do not fit his or her official educational and work history. Or someone whose information was picked up in the OPM hack who has Top Secret clearance may regularly carry a very large credit card balance or be late paying mortgage bills.

If we really want to protect national security, in short, we are likely focused *on the wrong thing*; instead of only protecting classified information held in government hands, we should be more focused on protecting unclassified information held in *private* hands from unauthorized disclosure.[363]

IV. SOLUTIONS

If the problems outlined above are real, then the next question is what should we do to address them? Here I begin by asking what might happen if we abandoned the system of classification altogether. This would not necessitate abandoning secrecy—instead, it would simply entail relying on a set of normal tools available to actors of all kinds, including private businesses. Indeed, despite the problems outlined above, it is worth noting that private businesses do keep secrets without the help of a system of classification. Keeping secrets is a part of nearly every human endeavor, and it is only in the field of national security that a system of classification is used to protect them.[364] Is there anything that government could learn from these techniques that might allow it to abandon the current classification system?

A. ENDING THE SYSTEM OF GOVERNMENT SECRECY? (OR WHAT CAN WE LEARN FROM COKE?)

If we stopped relying on classification to protect government secrets, what would happen? Businesses, after all, don't rely on classification to protect their information. The famous formula for Coke is not classified.[365] But it is a well-kept secret. Are there lessons that government can learn from business that would allow us to protect the information really worth protecting without relying on the crutch of classification?

---

363. A fuller discussion of this problem is the subject of Oona A. Hathaway, The Coming National Security Threat (unpublished working paper 2022) (on file with author).

364. *See, e.g.*, BOK, *supra* note 143 (documenting secrecy in a range of circumstances including secret societies, corporate secrecy, secrecy in science, journalism, policing, and more).

365. It is also not patented, as the tradeoff of patenting a secret such as the formula for Coke is that it requires disclosure, as discussed below.

It turns out that businesses don't have the formal system of classification, but they have developed systems that often mimic those found in government—albeit usually on a smaller scale. Consider what a business does when it comes up with a piece of information it wishes to keep to itself—say, an innovation that it intends to monetize. In order to have an incentive to invent things, a firm (or a person for that matter) needs to know that they can benefit from the time and money they invested by obtaining exclusive rights to sell the thing they have invented for a time. The patent system is one tool for providing those protections—not by keeping the information secret but by giving the inventor monopoly of the invention for a limited time in return for public disclosure (which is made in a patent filing). Steve Jobs and Steve Wozniak, for example, invented a method for displaying high resolution color graphics and filed for a patent in April of 1977, laying the foundation for what would become the Apple empire.[366]

But it turns out that firms don't patent all of their discoveries. Instead, they often choose instead to keep their most important innovations secret. Here's why: when a firm files for a patent, it must explain the innovation in a specific and standardized technical format that can be read and understood by third parties. That information becomes a matter of public record. Competitors aren't able to reproduce a patented technology precisely in the same form as described in the patent. But the patent might nonetheless give the competitors information that would allow them to leap ahead in their own research ("inventing around" the patent).[367] As the academic literature puts it, "disclosure facilitates imitation."[368] This is precisely the point of patents—they are *supposed* to encourage innovation by giving competitors enough information that they might be able to improve on the innovation.

From a public policy perspective, that's a great compromise. The firm that made the initial discovery gets to monetize the benefits, and everyone else gets access to information that they might not otherwise have had that can, in turn, allow them to skip wasteful duplication of research efforts and make it possible for them focus on new innovations instead. That's good for the overall economy. But for the firm that came up with the original innovation, this dynamic poses a

366. U.S. Patent No. 4,136,359 (filed Jan. 23, 1979).

367. Anton & Yao, *infra* note 368, at 2 (describing the considerations a competitor takes in prior to attempting imitation).

368. James J. Anton & Dennis A. Yao, *Little Patents and Big Secrets: Managing Intellectual Property*, 35 RAND J. ECON 1 (2004).

bit of a dilemma: Does the firm file for a patent and capture the revenue from the discovery even though doing so might give away some valuable information to others?

Research in the early 2000s discovered that the answer is often no. A survey of U.S. firms in 2000 found that firms generally protected their innovations with a range of mechanisms that included patents (one form of "formal intellectual property"), but also included secrecy, lead time advantages, and the use of complementary marketing and manufacturing capabilities (together sometimes called "informal intellectual property").[369] Of these, patents were the *least* important and secrecy and lead time *most* important.[370] Secrecy was particularly important for protecting process innovations. Secrecy was tied with lead time as the primary tool for protecting product innovations. Indeed, secrecy was so important that it led some to question what unusual conditions led firms to resort to patents rather than simply rely on secrecy.[371]

It turns out that small process innovations are almost always patented, since the imitation costs are small and a patent offers some increased protection. Large process innovations, on the other hand, are more likely to be protected through secrecy, because the disclosure from patenting is likely to lead to imitation.[372]

---

369. *See, e.g.*, Seliina Päällysho & Jari Kuusitsto, *Informal Ways to Protect Intellectual Property (IP) in KIBS Businesses*, 13 ORG. & MGMT. 62 (2011); Bronwyn H. Hall, Christian Helmers, Mark Rogers & Vania Sena, *The Choice Between Formal and Informal Intellectual Property: A Review*, 52 J. ECON. LIT. 375, 376 (2014) (surveying the literature on the topic through 2014).

370. *See* Wesley M. Cohen, Richard R. Nelson & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not)*, (Nat'l Bureau Econ. Rsch., Working Paper No. 7552, 2000).

371. *Id.*; Anton & Yao, *supra* note 368. An earlier landmark paper found a similar difference regarding process innovations and product innovations. It hypothesized that firms had an incentive to advertise advantages of new or improved products—hence maintaining secrecy about product innovations was likely to be both more difficult and less undesirable than maintaining secrecy about process innovations. Richard C. Levin, Alvin K. Klevorick, Richard R. Nelson & Sidney G. Winter, *Appropriating the Returns from Industrial Research and Development*, 1987 BROOKINGS PAPERS ON ECON. ACTIVITY 783 (1987), https://www.brookings.edu/wp-content/uploads/1987/12/1987c_bpea_levin_klevorick_nelson_winter_gilbert_griliches.pdf [https://perma.cc/XD54-X9HS]. Notably, secrecy appeared to have increased in importance between 1987 and 2000. *See* Cohen et al., *supra* note 370; *see also* Hall et al., *supra* note 369 (surveying the literature on the topic through 2014).

372. David Encaoua & Yassine Lefouili, *Choosing Intellectual Protection: Imitation, Patent Strength and Licensing*, 79/80 ANNALES D'ÉCONOMIE ET DE STATISTIQUE 241 (2005) (finding that innovation size is a key factor in determining the probability of a patent).

If secrecy is so important, how do companies protect their secrets? Perhaps unsurprisingly, they use some tools that mirror those used by government. I briefly describe the key techniques here, summarizing how they compare to government tools and techniques in Table 2 below.

Limiting Information Flow and Access. Put simply: the fewer people who know the information, the less likely it is to be disclosed. The private sector, like government, limits information flow as a means of protecting secrets. This can be as simple as including some people and not others in regular meetings, email chains, and systems of data access. Some private firms very intentionally compartmentalize information as a means of reducing harm if there is an information leakage or someone leaves the firm. One way to ensure limited information flow is through access restrictions. This can include physical access restrictions—restricting access to facilities or to particular parts of the facilities—and limits on information sharing, for example limiting information on a given project to those directly involved in the project. One study acknowledged, however, that "too strict restrictions inside the company may lead into insufficient knowledge sharing that becomes a barrier to innovativeness."[373]

But how are these requirements enforced? There are a number of that private actors use to enforce secrecy requirements.

Building Loyalty. One tool that private entities use to protect secrets is to cultivate commitment by engaging in staff loyalty-building strategies. One study found that effective methods for cultivating loyalty include financial incentives and occupational development opportunities such as training opportunities. These tools were found to be more effective than other tools such as contract and non-disclosure agreements, which can have the opposite effect.[374] The federal government also uses similar tools, though perhaps not expressly for the purpose of maintaining control over confidential information. Traditionally, federal employment has been secure and pensions excellent. There are often, though not always, training opportunities. And, of course, the U.S. government can draw on a well of patriotic loyalty felt by many who choose to work for the government, particularly in the field of national security.

Criminal Penalties. Since 1996, companies have also relied on criminal sanctions to reinforce the protection of their trade secrets.

373. Päällysho & Kuusisto, *supra* note 369, at 69.

374. *Id.* ("Positive methods in personnel management can enhance employee motivation whereas negative and restrictive methods such as contracts and agreements may have quite opposite impacts.").

The Economic Espionage Act[375] creates criminal penalties for the theft of privately held trade secrets. The enactment of the law resulted from rising concern in the intelligence community that foreign economic espionage was harming U.S. competitiveness abroad. When President Clinton signed the bill into law, he declared it was meant to "protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft."[376]

Administrative Penalties. The flip side of loyalty is administrative penalties for employees that violate confidentiality rules. For the private sector, this could entail a simple reprimand, a negative employee evaluation, or, at an extreme, firing the offending employee.[377] Private companies can also hold out the threat of providing a negative job evaluation to future employers as a penalty for violating company rules regarding protection of proprietary information. This mirrors government tools; the government also has access to more far-reaching penalties by placing information in the employee's file that could lead to loss of security clearance and the inability to obtain a security clearance in the future, effectively barring an employee from an entire line of government work.

Civil Penalties. Another tool companies use, which again mirrors government practice, is the non-disclosure agreement (NDA). An NDA creates a contractual obligation not to reveal proprietary information.[378] Companies also utilize noncompete clauses for the same purpose, prohibiting employees from working in the same industry for some period of time if they leave the company—a technique meant to prevent them from using know how learned on the job to help a competitor.[379] These NDAs are backed by civil remedies—if a former employee breaks the restrictions in the contract, they can be sued for money damages.

---

375. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489.

376. Presidential Statement on Signing the Economic Espionage Act of 1996, WEEKLY COMP. PRES. DOC. 2040 (Oct. 14, 1996), *as reprinted in* 1996 U.S.C.C.A.N. 4034, 4034 (emphasis added).

377. *See generally* Sampson Quain, *Types of Discipline Used in the Workplace*, SMALL BUS.: HOUS. CHRON. (Oct. 19, 2018), https://smallbusiness.chron.com/types-discipline-used-workplace-10890.html [https://perma.cc/L3QB-X8RR].

378. Richard Harroch, *The Key Elements of Non-Disclosure Agreements*, FORBES MAG. (Mar. 10, 2016), https://www.forbes.com/sites/allbusiness/2016/03/10/the-key-elements-of-non-disclosure-agreements [https://perma.cc/64N7-PWBM].

379. Marci Martin, *What is a Noncompete Agreement?*, BUS. NEWS DAILY (Jun. 27, 2017), https://www.businessnewsdaily.com/4803-non-compete-agreement.html [https://perma.cc/UP6A-RRGC].

TABLE 2: TOOLS FOR KEEPING SECRETS

	Government	Private Sector
Limiting Information Flow and Access	Limits on who is included in knowledge streams, compartmentalization of information access to limit damage if one compartment is compromised—organized by means of a formal classification system. Limiting physical access (keys, badges, access codes to limit access to building or parts of building) and electronic access (passwords; gapped computer systems).	Similarly limits knowledge streams and compartmentalizes information access, but without using a formal classification system. Government may be able to enforce physical access restrictions more effectively due to its monopoly on the legitimate use of force.
Encouraging Compliance		
Building Loyalty	Traditionally offers good job security, pension, salary for jobs requiring secrecy. Often also provides training opportunities. Can often count on patriotism, as well.	May offer financial incentives, training opportunities, and engage in other loyalty-building efforts.
Criminal Law Penalties	Espionage Act of 1917 & range of other criminal penalties for intentionally disclosing classified information.	Economic Espionage Act of 1996, 18 USC Sec. 1831.
Administrative Penalties	Can fire employees who violate confidentiality rules; may deny security clearance in the future, which limits access to government jobs as well as private contractors that require security clearance.	Can fire employees who violate confidentiality rules; may give poor reference to potential future employers.

Civil Penalties	Require employees to sign non-disclosure agreements requiring employees to protect information, including commitment to prepublication review with civil penalties attached (an employee that publishes a book without prior review, for example, can have all royalties seized by the government).	Also require employees to sign non-disclosure agreements requiring employees to protect information, with civil penalties attached (lawsuit for damages), but no access to prepublication review. May also employ noncompete clauses.

In short, what is perhaps most striking about looking to private sector efforts to protect secrets is how much those efforts have come to mirror the government's own. The information flow and access practices mirror those used in government to protect classified information—for example, only those with TS/SCI clearance are allowed unmonitored inside Special Compartmented Information Facilities and then only into those they need to access. And the information sharing limitations mirror "compartmentalization" of classified data—with the attendant downsides.

Comparing the public and private systems, we can see that the government's national security classification system is really just a formalized and standardized system for regulating the flow of and access to information. The classification markings on a document simply provide information on who can access the document (for example, those with Top Secret clearance are the only ones who can access Top Secret documents—and then only if they are "read in" to the relevant program).[380] Classification, however, has no independent power.

What gives it power are the set of criminal, civil, and administrative penalties associated with sharing information outside the designated channels. Even when it comes to enforcement, the private sector methods have increasingly mirrored the government's. The differences in the enforcement systems between the public and private sector exist but are subtle. First, criminal penalties for disclosing classified information are so threatening because they are both so broad in application and because courts defer to classification markings as evidence of intentional harm to national security.[381] By contrast, to

380. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

381. *See Dept. of Justice Guide to the Freedom of Information Act: Exemption 1,* DEPT. OF JUST. 3–10 (2014), https://www.justice.gov/oip/doj-guide-freedom-information-act-0 [https://perma.cc/8VL2-6NPQ].

demonstrate a violation of the Economic Espionage Act, the prosecutor has to show that the company whose information was disclosed took reasonable steps to protect the information.[382] It is not enough for the company to place a "trade secret" stamp on a document. Second, administrative penalties differ primarily in that the government can revoke a security clearance—thus ending not only a job but a career.[383] Third, the key difference in civil penalties is that the government can insist on prior restraint—and can seize all proceeds from a publication if a former employee fails to comply.[384] Aside from these differences, the structure of the system for enforcing the protection of secrets is remarkably similar across the two sectors. In short, the private sector uses much the same tools to much the same ends.

That, in turn, is interesting for two principal reasons: On the one hand, it means that eliminating the classification system is not such a crazy idea after all. If much of the system can be replicated without a classification scheme, then perhaps the system isn't all that essential. On the other hand, it suggests that eliminating the classification system would not necessarily eliminate the problems outlined above. If we gave up on classifying information, there would still be rules for managing the storage and flow of information, but they would be determined through means other than something called a system of classification, though it would likely have a similar effect—much as rules that govern information flow in the private sector do. And they would likely still be enforced through a mix of criminal, civil, and administrative penalties.

Last, it is worth noting that private actors have many of the same blind spots as the federal government. As pointed out at the end of Part III, one crucial area of national security vulnerability is information that is held in private hands. This information is vulnerable to those who would wish to obtain unauthorized access for the same reasons government databases have been breached—the information is valuable and there is a remarkable amount of sloppiness when it comes to protecting it. Even simple protections like effective passwords and two-factor authentication are far from universal. Security costs money, and companies—like the government—have cut corners in ways that leave them vulnerable.

---

382. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489.

383. Exec. Order No. 12,968, 60 Fed. Reg. 40, 245 (Aug. 2, 1995).

384. N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (holding that the government's urging of security was not enough to overcome First Amendment concerns); *see also* Snepp v. United States, 444 U.S. 507 (1980) (allowing seizure of profits for publishing classified information for personal gain).

Are there other institutions from which we might learn instead? In 2012, Jack Goldsmith wrote of the U.S. Supreme Court's remarkable capacity to keep secrets, noting that it "leaks less than the CIA" and that perhaps the executive branch could learn a thing or two from its success.[385] He speculated that there were several reasons the Court was so good at keeping secrets. One was that there were fewer people with access to the information—about seventy as opposed to the (then) 4.2 million people with security clearances. He also noted that "the likelihood of a leak increases with the time span of the secret," and the secrets at the court—at least the outcome of cases—last at most the length of a term, or nine months.[386] He points, moreover, to the personal incentives—justices benefit from the mystique and clerks are motivated by loyalty and concerns about professional consequences if they disclose information and are later identified. These tools—keeping a smaller circle of people with access to confidential information, reducing the lifespan of a secret, and relying on loyalty are lessons from which the rest of government can learn. But they are likely not sufficient, on their own, to serve the purposes meant to be served by the system of national security classification.

B. PROPOSALS FOR REFORM

Considering elimination of the system of classification is illuminating in part because it reveals what the classification scheme really is: it is simply a system for managing information flow and access backed by a mix of sanctions. Every organization—private businesses, universities, even law journal offices—has its own systems in place for managing information flow and access. The national security classification scheme is simply a system that formalizes and standardizes the rules for information flow and access across a sprawling government bureaucracy. It allows millions of people to coordinate their behavior in managing access to tens of millions of documents. As noted above, if this classification scheme did not exist, it would have to be invented.

---

385. Jack Goldsmith, *Temple of Silence*, NEW REPUBLIC (June 22, 2012), https://newrepublic.com/article/104219/jack-goldsmith-scotus-leaks-cia [https://perma.cc/26XG-P9U9]. Goldsmith may be right about the comparison, but the Court is still far from perfect: In 1998, the book EDWARD LAZARUS, CLOSED CHAMBERS: THE RISE, FALL, AND FUTURE OF THE MODERN SUPREME COURT (1998), based almost entirely on tales told by former clerks was published, prompted Chief Justice John Rehnquist to require all of the clerks (including me) to sign a non-disclosure form. Goldsmith acknowledges that the Court is not as good at keeping secrets over the long term, specifically noting *Closed Chambers* as an example of the problem. *Id.*

386. Goldsmith, *supra* note 385.

That does not mean, however, that the system is working well. Here I explore three reform proposals that do not entail complete elimination of the classification system but that nonetheless go far beyond the minor adjustments to the system that have animated past reform efforts. The first two aim to eliminate elements of the system but leave the essential structure in place. First, automatic declassification of documents older than ten years would effectively eliminate much of the mountain of classified information, while preserving the system for the records most likely to be necessary to protecting national security. Second, revising the criminal laws to reduce criminalization would significantly curtail the most corrosive aspect of the enforcement system, which is currently so broad that it sweeps journalists and even those who reveal good Christmas wishes into its ambit.

The third proposal takes aim at one of the core reasons that derivative classification decisions have grown so out of hand: individual incentives all run in favor of classifying up; little pushes in the opposite direction. This proposal offers some ideas for shifting that dynamic. If adopted, these proposals would go a good distance to curing many of the problems with the existing system.

It is worth noting that all three of these proposals could be enacted by Congress through legislation (meanwhile the first and third could be done by the president alone through executive order). Some may question whether Congress can constitutionally exercise such power over the classification system.[387] That question is a product of longstanding executive unilateral control over the classification system. But, as noted in Part I, the earliest executive orders on executive power were enacted precisely to carry out legislative priorities *enacted by Congress*. After a few iterations, presidents dropped the references to the congressional statutes and continued unilaterally. But this does not rob Congress of the power to regulate classified information systems. While the president is Commander in Chief, Congress has *seven* different national security-related authorities in Article I,[388] among them the power to "make Rules for the Government and Regulation of the land and naval Forces."[389] No one disputes, for example, Congress's power to protect information relating to nuclear weapons

387. Notably, it has considered proposals in the past. *See* HAROLD C. RELYEA, CONG. RSCH. SERV., 98-298, MANAGING SECRECY: SECURITY CLASSIFICATION REFORM—THE GOVERNMENT SECRECY ACT PROPOSAL 4 (July 8, 1998) (discussing various legislative proposals for reforming classification policy and procedure that ultimately were not enacted).

388. U.S. CONST. art. I, § 8, cls. 10–16.

389. *Id.* cl. 14.

technology.[390] And Congress included a number of undisputed provisions in the Foreign Intelligence Surveillance Act[391] that call for declassification of certain opinions and statistics. Moreover, the criminal sanctions that give the classification scheme its force are the result of congressionally enacted laws. Hence Congress clearly has the authority to legislate to carry the following proposals into effect.

1. Automatic Declassification

A first step that could eliminate the classification backlog and go a significant distance toward curing the overclassification problem would be to put in place an automatic ten-year declassification rule for all classified information. In effect, this proposal would adopt the proposal for abolishing the classification system but only for information that is more than a decade old.

Under rules first adopted in the 1995 executive order issued by President Bill Clinton and retained in the current executive order, "Information shall be declassified as soon as it no longer meets the standards for classification under this order."[392] Moreover, classified records older than twenty-five years are supposed to be released. As the current executive order puts it: "all classified records that (1) are more than twenty-five years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed."[393] Finally, an Interagency Security Classification Appeals Panel serves a number of functions including reviewing requests for exemptions from Automatic Declassification—including requests to exempt entire file series. That body is made up of senior level representatives from agencies in the intelligence community.[394]

The 25-year rule was meant to remove much of the discretion that had slowed the declassification process to that point. But it added in so many exemptions and opportunities for challenge that it hasn't really served that purpose. Shortly after the 25-year rule was adopted in 1995, the Department of Defense held a series of sessions to evaluate how well the system of declassification was working. The then

390. *See supra* Section I.D. (describing historical protections of nuclear research).

391. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et. seq*. (1978).

392. *See* Exec. Order. No. 12,958, 60 Fed. Reg. 19,825 (1995) for the original quote by Clinton, reprinted in Exec. Order No. 13,526, 75 Fed. Reg. 707 § 3.1 (2009) issued by President Obama.

393. Exec. Order No. 13,526, 75 Fed. Reg. 707 § 3.3 (2009).

394. *Interagency Security Classification Appeals Panel*, NAT'L ARCHIVES, https://www.archives.gov/declassification/iscap [https://perma.cc/6GE2-7BN7].

head of the Information Security Oversight Office, Mr. Garfinkle, explained then that "we essentially run into only two or three reasons why it [older classified information] continues to be classified after twenty-five or thirty years. Those reasons essentially are a foreign government information situation or intelligence sources or methods."[395] He noted that if the rule had been set at forty years, it likely would have been possible to adopt narrower exceptions. When the 25-year rule was adopted, the exceptions adopted along with it changed it from an automatic declassification program rule to an "enforced systematic review"—in part because the exemptions allowed entire file series to be exempted from automatic declassifications. As Garfinkle put it, "we came to the conclusion that systematic review was not working, and therefore we needed to go to an automatic system, but when we lowered the automatic system to the 25-year frame, what in effect we created was enforced systematic review."[396]

The only remedy for someone seeking access to information is to pursue Mandatory Declassification Review (MDR), "a means by which any individual or entity can request any Federal agency to review classified information for declassification, regardless of its age or origin, subject to certain limitations."[397] Unfortunately, requests for MDR come with long wait times. Agencies have one year to provide a decision on the initial MDR request as well as 180 days to respond to any appeals.[398] Despite these deadlines, it's unclear how efficiently different agencies process MDR requests. FOIA requests, for example, have deadlines of twenty business days to respond,[399] but in practice wait times are months[400] and sometimes even years.[401]

---

395. *Third Session of the DoD Historical Records Declassification Advisory Panel*, U.S. DEP'T OF DEF. 27–28, https://fas.org/sgp/advisory/dod-hrdap-1996.pdf [https://perma.cc/TP74-AXNP].

396. *Id.* at 30–31.

397. *Mandatory Declassification Review (MDR)*, INFO. SEC. OVERSIGHT OFFICE (July 19, 2021), https://www.archives.gov/isoo/training/mdr [https://perma.cc/5URD-ZBMM].

398. *Id.*

399. *FOIA Guide, 2004 Edition: Procedural Requirements*, U.S. DEPT. OF JUST. (2014), https://www.justice.gov/oip/foia-guide-2004-edition-procedural-requirments [https://perma.cc/7RHR-H9QB].

400. *Time Periods Under FOIA*, DIGIT. MEDIA L. PROJECT (Jan. 22, 2021), http://www.dmlp.org/legal-guide/time-periods-under-foia [https://perma.cc/YW5Y-MMMX].

401. Josh Gerstein, *Judge Balks at FBI's 17-Year Timeline for FOIA Request*, POLITICO (July 29, 2017), https://www.politico.com/blogs/under-the-radar/2017/07/29/judge-balks-fbi-foia-timeline-17-years-241127 [https://perma.cc/FE47-CCSQ].

In short, the 25-year rule has replicated the very problems it was meant to solve. Today, an immense amount of information, for which there is no ongoing justification to classify and that is older than twenty-five years old, remains classified. One can see this by simply looking at recent declassification decisions. For instance, it took until 2018 to declassify 2,800 classified records relating to the assassination of President John F. Kennedy—and even then, the Trump administration held some records back.[402] The cost to our ability to understand our history is immense. To take just one example, records of CIA covert action in Ethiopia from the 1970s still remain classified.[403] Relevant papers in the Jimmy Carter Presidential Library are closed with the notice: "These papers contain documents restricted in accordance with applicable executive order(s), which governs National Security policies, applicable statutes/agency restrictions, and material which has been closed in accordance with the donor's deed of gift,"[404] or the 25X1 exemption from automatic declassification.[405]

A new non-negotiable date of ten years should be set with only two exceptions—(1) information classified as "Restricted Data" under the Atomic Energy Act[406] and (2) information identifying CIA and other intelligence agency informants who are still alive.[407] For other information that could do real harm to national security, there should be an independent board made up not only of former government officials, but also of historians and public advocates—including journalists and civil rights advocates. A government agency facing automatic

402. Sarah Pruitt, *Trump Holds Some JFK Assassination Files Back, Sets New 3-Year Deadline*, HISTORY (Nov. 21, 2018), https://www.history.com/news/final-jfk-files-assassination-documents-release [https://perma.cc/H4Z8-KMBA].

403. Esther Araya, Covert Action in Ethiopia (1974–1981): Revealed and Concealed (2019) (unpublished manuscript) (on file with author).

404. Off. of the Nat'l Sec. Advis., *Records of the Office of the National Security Advisor: A Guide to Its Records at the Jimmy Carter Library*, JIMMY CARTER PRESIDENTIAL LIBR. & MUSEUM, https://www.jimmycarterlibrary.gov/assets/documents/findingaids/National_Security_Advisor.pdf [https://perma.cc/BC2D-JS9B].

405. 25X1 is an exemption for information that would "reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development." *Declassification F.A.Q.*, U.S. DEPT. OF JUST. ARCHIVES, https://www.justice.gov/open/declassification/declassification-faq [https://perma.cc/2KK9-XTKB].

406. *See* Atomic Energy Act of 1954, Pub. L. 83-703, § 141–46, 68 Stat. 919, 940–43 (1954) ("It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data . . . to assure the common defense and security.").

407. For the history of the 25-year rule, see Steven Aftergood, *A "Drop Dead" Date for Classified Info*, FED. OF AM. SCIENTISTS (Jan. 25, 2021), https://fas.org/blogs/secrecy/2021/01/drop-dead-date [https://perma.cc/ZVC7-YLVN].

declassification of information that could do real harm to national security could file a request to extend the classification period for that information. In essence this rule would flip the default. Rather than requiring researchers and journalists to appeal for the release of information through Mandatory Declassification Review, which can take years, if not decades, the presumption would be declassification and the government would be able to request extension of the date where really necessary. Shifting the default would create incentives for the government to adequately resource the process of review so that it could take place in a timely manner.

The independent board may be granted the authority not only to permit continued classification of a particular set of information but of, for example, a particular method of intelligence collection that could cut across different geographic or substantive areas. Where the independent board determines that a method that is more than ten years old but still in use, or not in use but sufficiently similar to current methods that it could give adversaries information to infer the current method, the board may conclude that national security could be harmed by its disclosure and therefore classification should be extended for a period longer than ten years. In such cases, the board should carefully circumscribe and define the instances where information may continue to be classified—and it should put in place a process for periodically reassessing how that continued authority is used.

Some may argue that ten years is too aggressive, others that it is too lenient. The logic behind a ten-year rule is it allows the exclusion of most matters of true strategic value. Information older than ten years is likely to be of less significant national security value. It is true that information more than ten years old may be politically embarrassing to sitting officials—though the time period ensures that the information will not be automatically released while the U.S. president in office when the information was created will still be in office when it is released. But embarrassment is not, by itself, a good reason for keeping information from the public sphere.

One matter that will require careful consideration is how to address concerns about revealing information about foreign governments. According to then-ISOO director Garfinkle, in 1996, one of the biggest holdups to automatic declassification then (and likely now) was over exchanges with and information about foreign government officials.[408] But such concerns are not so much national security con-

408. *See Third Session of the DoD Historical Records Declassification Advisory Panel*, *supra* note 395, at 27.

cerns as much as they are political or diplomatic ones (though, admittedly, the line between these categories can be blurry). A foreign government official may not be pleased to see a discussion with a U.S. government official released. But it is far from clear that this is a proper reason to classify the information. If the information should be protected, national security classification is the wrong tool.

Here, the distinction between classification and release is worth clarifying. The fact that information is declassified does not mean it necessarily must be released to the public. Declassifying the information means that releasing it would not trigger Espionage Act or other criminal charges. But it does not compel release. The government may use other tools for keeping information secret—tools shared with private enterprises. Unlike private entities, however, if information is no longer classified, it may be subject to a FOIA Request, from which Exemption 1 (the national security exemption) would no longer be available. Though there are reasons to be wary of adding to the exemptions under FOIA, it would make more sense to exempt diplomatically or politically sensitive foreign government information from FOIA than to keep it classified. Indeed, FOIA already includes an exemption for another set of information that is apparently a common hold up to automatic declassification—intelligence sources.[409] FOIA Exemption 7 exempts from release any information that "could reasonably be expected to disclose the identity of a confidential source."[410]

Last, it is important to emphasize that information for which there is no national security justification to classify should be declassified as soon as possible—even if it is *less* than ten years old. To assist with this process, the U.S. government should make much more use of artificial intelligence (AI) technology, which could review records and determine which may be good candidates for release and which should be subject to review before release.[411] A report issued by the Public Interest Declassification Board in May 2020 endorsed greater

409. The Freedom of Information Act, 5 U.S.C. § 522(b)(7).

410. 5 U.S.C. § 552 (b)(1).

411. In her confirmation hearing, DNI Avril Haines recognized the importance of better using technology in the classification and declassification system. John Powers, *New DNI Avril Haines Discusses Overclassification at Senate Confirmation Hearing*, NAT'L ARCHIVES, PUB. INT. DECLASSIFICATION BD., (Jan. 21, 2021), https://transforming-classification.blogs.archives.gov/2021/01/21/new-dni-avril-haines-discusses-overclassification-at-senate-confirmation-hearing [https://perma.cc/REZ8-GPQK].

use of AI and machine learning for declassification purposes.[412] That report rightly notes that "[o]utdated and excessively costly, the current method for classifying and declassifying national security information remains unsustainable in the digital information age."[413] Indeed, it may even be possible to use AI in the future to check classification decisions at the time they are made—or to recommend revisions to them. Some may worry that AI will not make the "right" decisions, but as systems improve, it seems likely that they will be able to outperform individual persons when it comes to determining which information may do real harm. That is because AI systems are capable of aggregating far more information than is a single human being—even a subject matter expert of long experience.

2. Reduce Criminalization

As we saw in Part I, Congress has been significantly cut out of decisions about the national classification system. That is true even though the key reason that it has force—criminal statutes, chief among them the 1917 Espionage Act—were enacted *by Congress*.[414] The decision of the executive branch to regulate the system since World War II through a series of executive orders (once justified by reference to congressional statutes, but no longer), and the courts' willingness to treat the classification of information as unimpeachable evidence that the information is a threat to national security, means that Congress has become almost entirely irrelevant.

Congress, in failing to act, has not only allowed itself to be cut out of the process of deciding how to protect national security information. It has also left in place laws that are overbroad and thus deeply damaging to public debate and democratic discourse. The Espionage Act is the legacy of a xenophobic period that led to mass overcriminalization of the release of information that might have national security consequences. It has undergone little change in the century since. It sweeps many journalists within its reach—journalists who are seeking to bring to the public information they regard as essential to informing the public discourse. The overbroad criminal statute also leaves former government employees and even members of Congress themselves at the mercy of federal prosecutors. It is past time for Congress to reassert its role in the process by revisiting the Espionage Act

412. *A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System*, PUB. INT. DECLASSIFICATION BD. (May 2020), https://www.archives.gov/files/declassification/pidb/recommendations/pidb-vision-for-digital-age-may-2020.pdf [https://perma.cc/WND5-ZXD8].

413. *Id.* at 3.

414. *See* Espionage Act of 1917, Pub. L. No, 65–21 § 1, 40 Stat. 217, 217.

and the array of laws that criminalize the release of classified information to make them much less capacious—and subject to abuse—than they currently are.

Among the changes to the law that should be adopted to reduce criminalization are the following: first, a person prosecuted for releasing a document or other information marked classified should be able to effectively defend themselves if they can prove that the released information did not actually threaten to harm national security. In other words, the fact that a document is marked classified should not be taken as irrefutable evidence that the person "knowingly" put national security at risk. Courts should be willing to entertain evidence that information was improperly classified. Second, Congress should be able to make independent judgments about when and how to declassify information that it judges is in the public interest, and agencies should be prohibited from retaliating by reducing classified information provided in the future. The risk of politicization could be reduced in a number of ways—for example, the decision could require a vote of the so-called "Gang of 8."[415] Third, there should be explicit account taken of the fact that there is likely to be public value to some disclosures that may overcome the prohibition on disclosure. In particular, there should be a defense that allows the accused to demonstrate that the release of the information was in the public interest because, for example, it revealed an action or program that violated the law (for example, a program of torture in violation of both domestic and international law and there was no alternative method available for addressing that violation). Fourth, there should be an exception for journalists. After all, only one has been prosecuted under the Act—Julian Assange.[416] Nonetheless, many journalists worry that their reporting could make them criminally liable because the work they do on a daily basis falls within the plain language of the Espionage Act's

415. The Gang of 8 is made up of the chair and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate. 50 U.S.C. § 3093(c)(2).

416. There is a live question of whether Assange is properly considered a "journalist," but critics pointed out that he was indicted for "'conduct that investigative journalists engage in every day.'" Savage, *supra* note 266 (quoting Jameel Jaffer of the Knight First Amendment Institute at Columbia University). *See also* Deanna Paul, *How the Indictment of Julian Assange Could Criminalize Investigative Journalism*, WASH. POST. (May 27, 2019), https://www.washingtonpost.com/national-security/2019/05/27/how-indictment-julian-assange-could-criminalize-investigative-journalism [https://perma.cc/HY6Y-QTNH].

prohibitions. Before the Assange indictment, DOJ had an informal policy against prosecuting journalists for violating the Espionage Act.[417] That should be formally incorporated into the Act so that future administrations cannot reverse course.[418]

Last, there should be a one-year limit on required prepublication review of writings by former government employees, paired with a safe harbor from criminal prosecution for those that voluntarily choose to submit their publications for review after the one-year period has run. In most cases, the information a former government employee possesses will be of greatest national security value immediately after they leave government employment. That value declines precipitously over time. The case for allowing the government to put in place prior restraint on speech declines accordingly over time. An advantage of reducing the application of the requirement to subject writing to prepublication review to just one year is that the massive backlog that has slowed the system would immediately vanish. It could be replaced with a voluntary system for those who are more than one year past government service: if a former government employee is more than a year out but unsure whether something they have written or wish to say may contain classified information, there should be a swift way to seek and receive a determination. Such a determination would then provide a safe harbor protecting the person from criminal prosecution in the future if it is later found that the writing did, in fact, contain classified information. Anyone who did not seek and receive the prior review would be able to publish without it, but he or she would potentially be subject to prosecution if they revealed information that actually did harm to national security.

True, some may think that this will reduce the ability of the government to protect national security information. But this objection fails to appreciate that many former employees have decided not to participate in the prepublication review system, because they find it

417. Charlie Savage, *Holder Hints Reporter May Be Spared Jail in Leak*, N.Y. TIMES (May 27, 2014), https://www.nytimes.com/2014/05/28/us/holder-hints-reporter-may-be-spared-jail-in-leak.html [https://perma.cc/46ST-YEK8] (quoting then-Attorney General Eric Holder that "[A]s long as I'm attorney general, no reporter who is doing his job is going to go to jail.").

418. To the extent this is not already taking place through prosecutorial discretion, there should be an effort to better calibrate punishment to the violation. There are what we might term "core secrets" that demonstrably harm national security. And then there are procedural violations of the rules designed to protect those secrets, but that are not themselves exposures of secrets, that merit much less severe punishment. In theory, the marking of a document as "Top Secret" should identify it as containing "core secrets," but in reality, that category is much too broad to reliably serve that purpose.

so cumbersome, restrictive, and time-consuming. More former employees might take advantage of a safe harbor option that allows them to seek review of a publication that might contain national security information if it were voluntary and quick.

3. Shift Incentives to Classify—and Declassify

The fundamental problem in the system right now is pretty simple: all the incentives run in favor of classifying information over not classifying it, and classifying it at higher levels rather than lower ones.

The number of classified documents and the number of people who need security clearances to work for the government has grown at extraordinary rates in the last two decades. Prior efforts at modest reform have had little effect. Both Presidents Clinton and Obama sought to shift the curve by introducing stricter rules for classification. In the case of President Clinton, Executive Order 12958[419] sought to shift incentives toward reducing classification. Most important, it established a default in favor of lower level of classification, stating "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level."[420] But the order had little effect. The year the order was issued, 3.4 million derivative classification documents were created—every subsequent year was higher.[421] Today it is at least fifteen times greater.

President Obama attempted to take bigger steps. On December 29, 2009, he issued Executive Order 13,526, which aimed to improve the system for classifying, safeguarding, and declassifying national security information.[422] Among other things, it created the aforementioned National Declassification Center to conduct a unified and efficient declassification review of historically important older records.[423] On August 18, 2010, he issued an additional directive, Executive Order 13,549, which established for the first time a Classified National Security Information Program to facilitate the sharing and safeguarding of classified national security information with first responders and other officials in state, local, tribal, and private sector entities.[424] And he signed the Reducing Over-Classification Act into

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

420. *Id.* § 1.2(c).

421. *1995 Annual Report to the President*, INFO. SEC. OVERSIGHT OFF., 15 (1995), https://www.archives.gov/files/isoo/reports/1995-annual-report.pdf [https://perma.cc/74EL-XKZX].

422. Exec. Order No. 13,526, §§ 2.1–2.2, 75 Fed. Reg. 707, 712 (Dec. 29, 2009).

423. *See supra* text accompanying note 159.

424. Exec. Order No. 13,549, 3 C.F.R. 13,599 (Aug. 18, 2010).

law in 2010.[425] The findings in that act noted that the 9/11 Commission and others had "observed that the overclassification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information." It acknowledged, too, that overclassification impedes information sharing that could be important to national security. It designated a number of steps to address these problems. And yet, again, it appears to have been to little avail. In 2009, 54 million derivative classification documents were created by the U.S. government.[426] In 2010, that number shot up to 76 million, and then to a whopping 92 million in 2011, before leveling off and beginning to fall in 2013.[427] By the end of his presidency, the numbers had settled back down to something close to where they were at the time the Obama Administration began—around 50 million.

One likely reason for this intransigence is that none of these efforts took account of the personal incentives that government bureaucrats face in making the day-to-day decisions about classification levels. As noted in earlier parts of this article, the reality is that there are few penalties for overclassifying information and immense penalties for underclassifying information. People rationally respond to these incentives by classifying information at higher and higher levels. The machine, moreover, feeds on itself. The more that is classified, the more connected information is classified. As a result, just bending the curve is not enough.

There are a few key steps that could address this problem. The first is again to harness the power of AI and machine learning to identify cases of overclassification. Indeed, individual government employees who routinely overclassify relative to their peers could be notified that they classify documents more often than average and encouraged to be more careful to assess the true need to classify.[428] It may also eventually be possible for AI to suggest classification levels

425. Reducing Over-Classification Act, Pub. L. 111-258, 124 Stat. 2648 (2010).

426. *2013 Report to the President,* INFO. SEC. OVERSIGHT OFF., 5 (2013), https://www.archives.gov/files/isoo/reports/2013-annual-report.pdf [https://perma.cc/QVH2-7DF5].

427. *Id.* As noted earlier, some of this increase may have been due to a change between 2008 and 2009 in the way the number of classified documents were counted.

428. Innovative digital tools have been used, for example, to help identify prescription errors, which are a cause of death for thousands of people each year. *See, e.g.*, Ronen Rozemblum, Rosa Rodriguez-Moriguio, Lynn A. Volk, Katherine J. Forsythe, Sara Myers, Maria McGurrin, Deborah Williams, David W. Bates, Gordon Schiff & Enrique Seoane-Vasquez, *Using a Machine Learning System to Identify and Prevent Medication Prescribing Errors: A Clinical and Cost Analysis Evaluation*, 46 JOINT COMM'N J. ON QUALITY & PATIENT SAFETY 1 (2020).

at the time of writing, to challenge incorrect classification decisions at the time they are made, and to review the classification of stored documents. Simply providing employees feedback that indicates that they may be overclassifying may create feedback and incentives for reducing classification levels that, until now, have been missing.[429] Disciplinary procedures could be applied to employees who are repeatedly unresponsive to such feedback.[430] The key in using AI for these purposes, however, will be to not set the risk tolerance so low that it has the opposite of the intended effect.

Another change that could have a significant effect would be to enforce the requirement that documents be paragraph (or "portion") marked.[431] This could help slow the snowball effect described above, in which a person preparing a new document that uses a single sentence from a document marked Secret or Top Secret means the new document must be classified at the same level or above. Requiring paragraph marking to be done by hand for all documents, much less all emails, is too cumbersome and workable. But it might be done through automated systems. Automatic analysis of stored documents could also be used to paragraph mark documents not already so marked.

In addition, when a decision is made to classify a document, email, or other means of written communication, there is currently a drop-down menu that the employee must use to determine the classification level for the document or email—and when to make it eligible for declassification. At present, the government employee need offer no justification for the decision. One step could be to require that when a decision is made to classify a document at any level, the em-

429. In other contexts, simply providing information about peer behavior has been shown to change behavior. For example, it has been shown that a way to make people save energy is by informing them that "comparable others" save more. Mark A. Ferguson, Nyla R. Branscombe & Katherine J. Reynolds, *The Effect of Intergroup Comparison on Willingness to Perform Sustainable Behavior*, 31 J. ENV'T PSYCH. 275 (2011); Anna Rabinovich, Thomas A. Morton, Tom Postmes & Bas Verplanken, *Collective Self and Individual Choice: The Effects of Inter-Group Comparative Context on Environmental Values and Behaviour*, 51 BRIT. J. SOC. PSYCH. 551 (2012).

430. The psychology literature shows that accountability systems can have positive effects on performance. *See, e.g.*, Jermaine Vesey & Audria N. Ford, *Workplace Accountability*, 14 J. MGMT. STUD. 23 (2019); J.S. Lerner & P.E. Tetlock, *Accounting for the Effects of Accountability: Exploring the Role of Strong and Weak Accountability Environments on Employee Effort and Performance*, 125 PSYCH. BULL. 255 (1999).

431. This requirement is unevenly enforced, though there have been efforts to encourage better compliance.

ployee would be prompted to enter an explanation for the classification decision.[432] The explanation need not be lengthy. But requiring an explanation may encourage the employee to think carefully about the decision to overclassify a document—whereas at the moment, there is often nothing to force that careful consideration.[433] It could also be used later to evaluate employees who are overclassifying documents to see what reasons they have given and providing them corrective feedback.

A more radical way to shift incentives would be to implement a "cap-and-trade" system for classified documents—agencies could be capped at the average number of classified documents in, for instance, the three years preceding the initiation of the program. To go over its allotted amount, an agency would have to trade with another agency that has an under-used allocation (agencies would have to be authorized to offer something—ideally funds—in return). A related idea would be to "cap and reduce"—that is cap the levels and then gradually reduce them year-over-year, with financial penalties for missing the target.[434] Both systems would create incentives for agencies to design systems to disincentivized overclassification. As it stands, by contrast, there are no consequences for significant overclassification and thus little incentive to reign it in.

CONCLUSION

A fundamental responsibility, perhaps *the* fundamental responsibility, of the federal government is to protect the security of the nation and its citizens. The system for keeping national security secrets has

---

432. In theory this is supposed to be done already. The theoretical process, even for derivative classification, is that for each classified fact an employee of the Office of the Director of National Intelligence, for example, is supposed to look at the ODNI classification guide and identify the section of the guide that warrants classification. The guide, in theory, has already identified the national security harm that would result from disclosure. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707 § 2.2 (Dec. 29, 2009). Few follow these rules. The new requirement would be much less formalistic and would simply require a brief explanation of the decision.

433. Requiring reason giving can increase "accountability" and thus performance. *See* Lerner & Tetlock, *supra* note 430, at 255 ("[A]ccountability refers to the implicit or explicit expectation that one may be called on to justify one's beliefs, feelings, and actions to others."). Interventions like requiring reason giving can increase "felt accountability" and thus improve performance. *See, e.g.*, Vesey & Ford, *supra* note 430 (discussing "felt accountability").

434. The two could of course be combined—a cap-and-trade system could include gradual reductions in allocations as well. The advantage of a cap-and-trade system over just a cap or cap-and-reduce system is that it would incentivize agencies to reduce below their cap so that they could trade their excess allocation with agencies that need it.

been created in service of that mission. But over time, the system has grown and expanded in ways that have come to undermine it instead.

When tens of millions of classified documents are created year after year after year, the effort to protect those secrets becomes an end in and of itself. Pursuing this end has come at the cost of fundamental American values: to protect these secrets, we keep information from citizens that have a right to know it, silence the journalists who want to report it, place those who work with the information at risk of criminal prosecution for revealing it, and silence the very people who can best explain it. In the process, we put at risk the democracy that these policies are meant to safeguard.

We also put at risk the very thing the system was meant to deliver: national security. For a nation to pursue policies that are in its best interests in the complex, interdependent world in which we live, those in a position to make life-or-death decisions should not be boxed in by arbitrary and artificial boundaries that are created by classification rules. Classification rules protect information, but they also isolate it and those who possess it.

It may seem that the more secrets we keep, the safer we will be. But that is not true. Yes, some secrets are necessary. But there is a cost—a cost to democratic legitimacy and accountability, but *also* to our security. Only once we recognize that a government system that imposes too much secrecy undermines its own animating purpose will we be able to create a system that truly offers security.