ARTICLE

DO YOU HAVE TO KEEP THE GOVERNMENT'S SECRETS? RETROACTIVELY CLASSIFIED DOCUMENTS, THE FIRST AMENDMENT, AND THE POWER TO MAKE SECRETS OUT OF THE PUBLIC RECORD

JONATHAN ABEL†

† Fellow, Constitutional Law Center, Stanford Law School.

The author would like to thank Shira Levine, Michael McConnell, Andrew Prout, Thomas Sprankling, and the editors of the *University of Pennsylvania Law Review*.

INTRODUCTION

Now you see it. Now you don't.

This is not a magician's incantation. It is a description of retroactive classification, a little-known provision of U.S. national security law that allows the government to declassify a document, release it to the public, and then declare it classified later on. Retroactive classification means the government could hand you a document today and prosecute you tomorrow for not giving it back. Retroactive classification can even reach documents that are available in public libraries, on the Internet, or elsewhere in the public domain.

The executive branch has used retroactive classification to startling effect. The Department of Justice, for example, declassified and released a report on National Security Agency (NSA) wiretapping only to declare, years later, that the report was once again classified. The journalist who had received the report was threatened with prosecution if he did not return it. Retroactive classification has also targeted government documents revealing corruption in Iraq, violence in Afghanistan, and mismanagement of the national missile defense program. In each of these cases, the government released a document in an unclassified form through official channels—not through a leak—and then turned around to classify it.

This practice would be troubling enough if it actually removed the document from the public domain. But in the Internet Age, once a document is released to the public, it is often impossible for the government to retrieve it. While retroactive classification does not remove the document from the public domain, where our enemies can access it, retroactive classification does remove the document from the public discourse,

prohibiting members of Congress, government auditors, and law-abiding members of the public from openly discussing it.

In the ongoing debate about the balance between secrecy and transparency in government affairs, retroactive classification tests the limits of the government's ability to control information in the public domain. The questions raised by retroactive classification go far beyond those raised by the WikiLeaks and Edward Snowden disclosures. In those cases, the information remained classified even though it was widely available in the public domain. A similar situation occurs with retroactive classification when information in the public domain becomes classified. The difference is that in retroactive classification, the government initially released this information in a non-classified form and only later decided to classify it. This difference makes retroactive classification much more complicated from a legal standpoint because it involves the government's going back on its initial classification decision. Retroactive classification thus forces us to ask what limits, if any, exist on the government's authority to control information. Can the government reach into the public domain to make a secret out of something it has already disclosed? Are we obligated to go along with retroactive classification decisions? What are the implications beyond national security law? This Article takes up these pressing questions.

* * *

Retroactive classification is a doctrine rife with contradictions. Just ask the former director of the Information Security Oversight Office, the federal agency charged with overseeing the classification system. He called it "a metaphysical impossibility" to classify information "whose disclosure was authorized in the first place."[1] Members of Congress have been unstinting in their criticism, disparaging retroactive classification as "an insult to the American people, to the public, to this institution of Congress,"[2] "an attempt to stymie public debate,"[3] and an "absurd effort to put the toothpaste

---

[1] Jim White, *Despite Metaphysical Impossibility, U.S. Government Repeatedly Attempts Retroactive Classification*, EMPTYWHEEL (Jan. 23, 2012), http://www.emptywheel.net/2012/01/23/despite-metaphysical-impossibility-us-government-repeatedly-attempts-retroactive-classification, *archived at* http://perma.cc/
N292-VXPR.

[2] *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats and Int'l Relations of the H. Comm. on Gov't Reform*, 108th Cong. 84 (2004) [hereinafter *Too Many Secrets Hearing*] (statement of Rep. John Tierney).

[3] Letter from Rep. Henry Waxman & Rep. John Tierney to Donald Rumsfeld, Sec'y of Def. (Mar. 25, 2004) [hereinafter Waxman & Tierney letter], *available at* http://www.fas.org/sgp/congress/2004/h032504.pdf.

back into the tube."[4] The *Washington Post* editorial board thought retroactive classification "would be funny if it weren't so emblematic of a disturbing new culture of government secrecy."[5] James Bamford, a journalist who experienced it firsthand, warned of "total anarchy for historians and scholars . . . if one administration would be permitted to recall history by forcing these people to return materials released by a previous administration."[6] Even university archivists, generally an even-tempered lot, have expressed outrage, excoriating the retroactive classification of 25,000 documents at the National Archives as "a breathtaking assault on the fundamental principles under which we try to operate."[7]

Despite the criticism, however, retroactive classification remains the law, and an altogether unexplored one, at that. Legal scholarship has provided only glancing treatment. A few authors mention it in passing to point out abuses in the larger classification system,[8] or to draw analogies to Freedom of Information Act and state secrets case law.[9] Two student notes have taken

---

[4] *Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 2, 6 (2006) [hereinafter *Drowning in a Sea of Faux Secrets Hearing*] (statement of Rep. Christopher Shays).

[5] Editorial, *Classifying Toothpaste*, WASH. POST, Feb. 27, 2006, at A14.

[6] *1984: Civil Liberties and the National Security State: Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 98th Cong. 38 (1983) [hereinafter *1984: Civil Liberties Hearings*] (statement of James Bamford).

[7] *H.R. 1255, The Presidential Records Act of 1978: A Review of Executive Branch Implementation and Compliance*, *Hearing Before the Subcomm. on Info. Policy, Census, and Nat'l Archives of the H. Comm. on Oversight and Gov't Reform*, 110th Cong. 106 (2007) (statement of Steven L. Hensen, Dir. of Technical Ser., Rare Book, Manuscript, and Special Collections Library, Duke Univ.).

[8] *E.g.*, Jane E. Kirtley, *Transparency and Accountability in A Time of Terror: The Bush Administration's Assault on Freedom of Information*, 11 COMM. L. & POL'Y 479, 502-05 (2006); *see also* Anthony R. Klein, Comment, *National Security Information: Its Proper Role and Scope in a Representative Democracy*, 42 FED. COMM. L.J. 433, 437 n.23 (1989) (discussing the use of reclassification powers by the Reagan administration); Derigan A. Silver, *National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security Information*, 13 COMM. L. & POL'Y 447, 449-50 (2008) (noting the many ways in which the George W. Bush administration increased government secrecy including through the use of classification and reclassification).

[9] *E.g.*, Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 193-94 (2010); *see also* Susan Nevelow Mart, *Let the People Know the Facts: Can Government Information Removed from the Internet Be Reclaimed?*, 98 LAW LIBR. J. 7, 21, 29 (2006) (focusing on the withholding of documents, rather than classification); Jonathan Turley, *Through a Looking Glass Darkly: National Security and Statutory Interpretation*, 53 SMU L. REV. 205, 215-16 (2000) (citing retroactive classification in an argument about judicial deference in the context of national security); David C. Vladeck, *Litigating National Security Cases in the Aftermath of 9/11*, 2 J. NAT'L SEC. L. & POL'Y 165, 166 (2006) (discussing the Sibel Edmonds case and classification in the context of "how far the Administration has gone to press its national security arguments"); Anthony Rapa, Comment, *When Secrecy Threatens Security:* Edmonds v. Department of Justice *and A Proposal to Reform the*

positions on its constitutional legitimacy—one in favor,[10] and the other opposed.[11] But no systematic examination of the topic exists. No one has looked at how retroactive classification came about, what laws constrain—or fail to constrain—it, or how it is used in practice. Nor has anyone analyzed the essential question of whether retroactive classification can be enforced by criminal prosecution.[12] This Article aims to fill those gaps.

The Article proceeds in four Parts. Part I begins with several examples of retroactive classification and then looks at the evolution of the practice by drawing on congressional hearings, original interviews, and the text of the executive orders that have authorized retroactive classification. Since the late 1970s, retroactive classification has been alternately banned and embraced by successive administrations,[13] and the growth of the Internet has made the notion of reclaiming documents from the public domain increasingly absurd. This Part argues that the current law provides no effective restraint on the practice of retroactive classification.

Part II asks whether retroactive classification can be enforced by criminal prosecution. If the government retroactively classifies a document in my possession, and I ignore the new classification, can I be prosecuted for publishing it? This Part begins with the debate about whether the Espionage Act—the most likely tool for enforcing retroactive classification—can be applied to people outside of the government who receive classified documents and then publish them. Part II next discusses how the Espionage Act analysis would differ if the documents were not just classified but *retroactively* classified. It shows how retroactive classification challenges basic assumptions about what it means to leak information, who has an obligation

State Secrets Privilege, 37 SETON HALL L. REV. 233, 266 (2006) (discussing use of the state secrets privilege to retroactively classify information).

10 Luppe B. Luppen, Note, *Just When I Thought I Was Out, They Pull Me Back In: Executive Power and the Novel Reclassification Authority*, 64 WASH. & LEE L. REV. 1115, 1119, 1156 (2007).

11 Amanda Fitzsimmons, Comment, *National Security or Unnecessary Secrecy? Restricting Exemption 1 to Prohibit Reclassification of Information Already in the Public Domain*, 4 J.L. & POL'Y FOR INFO. SOC'Y 479, 484 (2008).

12 One author dismissed the possibility of prosecution out of hand. *See* Vladeck, *supra* note 9, at 178 ("[N]o court would have upheld the government's right to attach criminal sanctions to the publication of widely available information."). Another concluded that, in fashioning criminal punishments, "Congress has mostly disregarded the Executive's classification scheme." Luppen, *supra* note 10, at 1131.

13 President Carter's executive order on security classifications banned retroactive classification. Exec. Order No. 12,065, § 1-607, 3 C.F.R. 111, 195 (1979). President Reagan's order allowed it. Exec. Order No. 12,356, § 1.4(a), 3 C.F.R. 166, 169 (1983). President George H.W. Bush used President Reagan's order. President Bill Clinton's order banned it. Exec. Order No. 12,958, § 1.8(c), 3 C.F.R. 317, 339 (1996). President George W. Bush allowed it. Exec. Order No. 13,292, § 1.7(c), 3 C.F.R. 159, 200 (2004). So did President Barack Obama. Exec. Order No. 13,526, §1.7(c), 3 C.F.R. 183, 302 (2010).

to keep a secret, and how to define the public record. Part II concludes that a prosecution based on retroactively classified information could go forward despite serious Espionage Act and First Amendment problems.

Part III steps back to survey how other substantive areas of the law deal with their own versions of retroactive classification. Retroactive classification may be mean-spirited, unconstitutional, and even metaphysically impossible, but it is not without precedent. There are many other contexts outside national security where the government attempts to punish the publication of information that it has previously disclosed in the public record, including its attempts to protect Social Security numbers, police officers' home addresses, tax return information, and other sensitive pieces of information. These analogues from other areas of the law not only make retroactive classification seem more plausible as a threat to free speech and the freedom of the press, but also show how retroactive classification fits into a debate that transcends national security law—a debate about the government's ability to control information in the public record. Justice Stewart famously wrote: "So far as the Constitution goes, the autonomous press may publish what it knows, and may seek to learn what it can."[14] But retroactive classification and its analogues challenge that claim.

Finally, Part IV looks at still another constitutional complication for retroactive classification: the separation of powers. Members of Congress claim the executive branch has used retroactive classification to gag legislative debate and impede constitutionally required oversight. But the Constitution's Speech or Debate Clause protects these legislators from being prosecuted or even questioned for anything they say in debate—even if their statements reveal classified information. Part IV explores the paradox that members of the legislative branch are both more protected from and more vulnerable to retroactive classification than members of the public.

The concluding note makes several practical suggestions for reform. These suggestions include changing the executive orders that govern retroactive classification, addressing the problem of retroactive classification statutorily, and amending House and Senate rules to avoid a separation of powers issue.

I. RETROACTIVE CLASSIFICATION IN PRACTICE AND THEORY

What does it mean for the government to disclose a document and later declare it classified? This Part begins with several examples, proceeds

14 Potter Stewart, *"Or of the Press,"* 26 HASTINGS L.J. 631, 636 (1975).

through the history of retroactive classification, and concludes by showing how, in the Internet Age, the rules designed to limit retroactive classification can no longer do so.

A. *Examples of Retroactive Classification*

In 1978, journalist James Bamford sent a Freedom of Information Act (FOIA) request to the Justice Department. He wanted documents related to the Department's investigation of illegal wiretapping performed by the NSA. Among the surveillance programs the Justice Department investigated was Operation MINARET, which spied on Martin Luther King, Jr., Jane Fonda, and other opponents of the Vietnam War.[15] The chief of the Justice Department's special litigation unit, the unit that led the investigation into the NSA, took ten months to review the request.[16] In the end, the Justice Department declassified and released 250 pages of documents to Bamford.[17] When the NSA found out about the disclosure, however, it argued that the documents should never have been released and demanded that the Justice Department label them as classified.[18] The Justice Department refused.[19]

Two years later, with a new administration in the White House and new leaders atop the two agencies, the NSA tried again. This time, the Attorney General agreed. Bamford recalled a meeting with NSA and Justice Department officials. "They threatened to use the espionage statute against me," Bamford recounted, "if I continued to refuse to return the documents."[20] A letter from the Justice Department soon followed: "You are currently in possession of classified information that requires protection against unauthorized disclosure," it said, adding that Bamford should be aware of his "continuing obligation not to publish or communicate the information."[21] Keeping quiet was not enough for the Justice Department, however. "It is . . . your duty and obligation as a United States citizen to return this information to the Department of Justice," the letter insisted.[22] Despite these threats, Bamford published the classified information in *The Puzzle*

---

15 Judith Miller, *U.S. Is Demanding Return of Papers*, N.Y. TIMES, Mar. 14, 1982, at A19; *see also 1984: Civil Liberties Hearings*, *supra* note 6, at 37; James Bamford, *How I Got the N.S.A. Files . . . How Reagan Tried to Get Them Back*, THE NATION, Nov. 6, 1982, at 466.

16 Bamford, *supra* note 15, at 466.

17 *1984: Civil Liberties Hearings*, *supra* note 6, at 37, 40.

18 *Id.* at 40.

19 *Id.*

20 *Id.* at 37, 40.

21 *Id.* at 40.

22 Miller, *supra* note 15. Bamford's attorney received a similar missive threatening a "post-publication judicial remedy." Bamford, *supra* note 15, at 468.

Palace, his book about the NSA, which he called "the only book in history to have been totally unclassified as it was being written, yet top secret by the time it was published."[23] He was never prosecuted.[24]

Retroactive classification has also been used to impede congressional oversight. In 2000, a congressional subcommittee held hearings on the development of the national missile defense system.[25] The program's auditor made approximately fifty recommendations for improving the testing regime.[26] Those recommendations were delivered to Congress in public testimony, discussed by the media, and published in the *Congressional Record*. But four years later, when the subcommittee sought to follow up on those recommendations, it learned that the Defense Department had retroactively classified them.[27] The retroactive classification prevented the subcommittee from discussing the recommendations in open session, where the program would be subject to public scrutiny. This classification also barred the Government Accountability Office (GAO) from issuing a public report on the matter. Representatives Henry Waxman and John Tierney accused the Pentagon of making a "highly dubious" classification decision in "an attempt to stymie public debate."[28] The retroactive classification, they complained, would have "absolutely no effect on whether our adversaries can gain access to this information," but would instead "prevent members of Congress from being able to issue thorough and thoughtful critiques of Administration actions in a public forum."[29]

Retroactive classification also struck the Senate Judiciary Committee after it attempted to investigate misconduct inside the FBI. Sibel Edmonds, a translator working for the FBI, complained that her colleagues were purposefully leaving intelligence intercepts unanalyzed and notifying targets of FBI surveillance that the government was listening in.[30] Concerned by these allegations, Senators Chuck Grassley and Patrick Leahy wrote to the Justice Department's Inspector General. Their inquiry

---

23 *1984: Civil Liberties Hearings*, *supra* note 6, at 37.

24 Telephone Interview with James Bamford, Journalist (Nov. 6, 2013).

25 *National Missile Defense: Test Failures and Technology Development: Hearing Before the Subcomm. on Nat'l Sec., Veterans Affairs, and Int'l Relations of the H. Comm. on Gov't Reform*, 106th Cong. (2000).

26 *Id.* at 96-100; Waxman & Tierney Letter, *supra* note 3, at 1-2.

27 Waxman & Tierney Letter, *supra* note 3, at 1-2.

28 *Id.* at 4.

29 *Id.*; *see also Too Many Secrets Hearing*, *supra* note 2, at 7 (statement of Rep. Dennis Kucinich) ("Even in this committee, we saw how the Pentagon retroactively classified sections of a report critical of the proposed national missile defense plan.").

30 *See* Petition for Writ of Certiorari for Plaintiff–Petitioner at 2, Edmonds v. Dep't of Justice, 546 U.S. 1031 (2005) (No. 05-0190), 2005 WL 1902125, at *2.

prompted the FBI to deliver two unclassified briefings to the Committee about the allegations.[31] Based on the briefings, the senators wrote again to the Inspector General, distributing their letters to the media and posting them on their websites.[32] One letter was even published in the Congressional Record.[33] But when Edmonds filed a wrongful termination suit two years later, the Justice Department retroactively classified the briefings.[34] An email to the Judiciary Committee warned: "Any staffer who attended those briefings, or who learns about those briefings, should be aware that the FBI now considers the information classified and should therefore avoid further dissemination."[35] The email added that anyone with notes from the briefings should contact the Office of Senate Security.[36]

Senator Grassley was furious. In public hearings, he criticized FBI Director Robert Mueller for the classification decision, which struck him as "ludicrous because . . . almost all of this information is in the public domain and has been very widely available."[37] Grassley called this retroactive classification a "very serious" incident that threw "a roadblock in front of Congressional oversight" and attempted "to put a gag order on Congress."[38] His comments to the *New York Times* were just as critical: "To classify something that's already been out in the public domain, what do you accomplish? It does harm to transparency in government, and it looks like an attempt to cover up the F.B.I.'s problems."[39] An aide added that "[p]eople are puzzled and, frankly, worried, because the effect here is to quash Congressional oversight. We don't even know what we can't talk about."[40]

---

31 Eric Lichtblau, *Material Given to Congress in 2002 Is Now Classified*, N.Y. TIMES, May 20, 2004, at A18.

32 Declaration of Danielle Brian in Support of Plaintiffs' Motion for Summary Judgment and Opposition to Defendants' Motion to Dismiss at 8-10, Project on Gov't Oversight v. Ashcroft, No. 04-1032 (D.D.C. Sept. 30, 2004).

33 148 CONG. REC. S5843-44 (daily ed. June 20, 2002) (Letter from Patrick Leahy and Charles Grassley, Sens., to Glen A. Fine, Inspector Gen., Dep't of Justice).

34 *See Emerging Threats: Overclassification and Pseudo-Classification*: *Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 147, 147-48 (2005) (statement of Sibel Edmonds); *see also* Brief for National Security Archive et al. as Amici Curiae Supporting Petitioner at 14, Edmonds v. Dep't of Justice, 546 U.S. 1031 (2005) (No. 05-0190).

35 Declaration of Danielle Brian, *supra* note 32, at 9-10; *see also* Lichtblau, *supra* note 31.

36 Declaration of Danielle Brian, *supra* note 32, at 10.

37 *FBI Oversight: Terrorism and Other Topics: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. 16 (2004) [hereinafter *FBI Oversight Hearings*] (statement of Sen. Grassley).

38 *Id*.

39 Lichtblau, *supra* note 31.

40 *Id*.

Retroactive classification does not just target documents in the news. In fact, the largest known instance of retroactive classification took place at the National Archives and involved historical records that had been largely forgotten. Between 1999 and 2006, the CIA, the Air Force, the Department of Energy, and the Federal Emergency Management Agency retroactively classified more than 25,000 documents and removed them from the public shelves of the National Archives.[41] A number of these documents dated back to World War II and the Korean War and had already appeared in historical collections published by the government.[42] This aggressive reclassification did not come to light until Matthew Aid, a national security researcher, noticed that records he had previously photocopied were no longer publicly available.[43] His questions led the National Archives to admit to the existence of the secret classification program, and the ensuing uproar prompted the only audit to date of retroactive classification.[44] Significantly, the audit found that more than thirty-five percent of the retroactive classification was "questionable" or "clearly inappropriate,"[45] a proportion that Allen Weinstein, then Archivist of the United States, called "stunning[ly] large."[46]

What documents were caught in this retroactive dragnet? As it turns out, many of them hardly seem worthy of classification. The documents included a 1962 telegram translating a Belgrade news article about China's nuclear abilities,[47] a 1950s document entitled *Feasibility of Participating in Exchange Program with USSR to Study Highway Transportation in the USSR*,[48] and a World War II-era study of the Soviet Union's agriculture capacity.[49] Further complicating matters, the government had already published many

---

41 INFO. SEC. OVERSIGHT OFFICE, NAT'L ARCHIVES AND RECORDS ADMIN., AUDIT REPORT: WITHDRAWAL OF RECORDS FROM PUBLIC ACCESS AT THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION FOR CLASSIFICATION PURPOSES 1 (2006), *available at* http://www.archives.gov/isoo/reports/2006-audit-report.pdf. The auditors explained that "severe time constraints" prevented them from looking into all areas of the retroactive classification program. *Id.* at 27.

42 Scott Shane, *U.S. Reclassifies Many Documents in Secret Review*, N.Y. TIMES, Feb. 21, 2006, at A1; *Classifying Toothpaste*, *supra* note 5.

43 *Id.*

44 *Id.*

45 INFO. SEC. OVERSIGHT OFFICE, *supra* note 41, at 1, 16.

46 Allen Weinstein, Archivist of the United States, Remarks on Next Steps, at 1 (Apr. 2006), *available at* http://www.archives.gov/isoo/reports/weinstein-remarks.pdf.

47 Shane, *supra* note 42; Editorial, *Government's Drowning in a Sea of Secrets*, THE DAILY NEWS (June 5, 2008), http://tdn.com/news/opinion/editorial/government-s-drowning-in-a-sea-of-secrets/article_d9cf3ad6-42c8-574d-9df2-b92b2f33c8do.html, *archived at* http://perma.cc/6VF4-GXGE.

48 See *Classifying Toothpaste*, *supra* note 5.

49 Eric Lichtblau, *The Obama Administration's Commitment to Transparency: A Progress Report*, 77 SOC. RES. 975, 977-78 (2010).

of these documents in various anthologies, including the State Department's series *Foreign Relations of the United States*.[50] The documents published in the State Department's series included two CIA memos from 1948. One explored the possible effect of winter conditions on a scheme to use hot air balloons to drop propaganda over the Soviet bloc.[51] The other discussed the bad press the CIA was receiving for failing to predict anti-American riots in Colombia.[52] In addition to the documents published in the State Department series, the government permitted many more to be microfilmed by LexisNexis and Gale.[53] Matthew Aid estimated that at least forty percent of the documents classified by the Air Force, for example, had already been published in these microform collections.[54] Needless to say, this retroactive classification raised some eyebrows.[55]

In each of the cases above—and in others discussed below—the government disclosed documents through official channels and then circled back to retroactively classify them. While the full extent of retroactive classification remains unknown, the concerns raised by this power are significant.[56]

---

50 *See* Matthew M. Aid, *Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program*, NAT'L SEC. ARCHIVE (Feb. 21, 2006), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179 (last visited Feb. 27, 2014), *archived at* http://perma.cc/JY9W-GRLE (discussing the reclassification of over 55,000 pages of records that were publicly available at the National Archives).

51 Memorandum from Commander Robert Jay Williams to Cassady, Chief, Special Procedures Corp. (July 23, 1948), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/Aid-7.pdf. The memo concluded the cold weather would greatly diminish the project's value. *Id.*

52 Note from Humelsine to Jack on the Publicity on Bogota Intelligence Reports (1948), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/Aid-6.pdf.

53 Telephone Interview with Matthew Aid, Researcher (Oct. 26, 2013) (notes on file with author).

54 *Id.*

55 *See, e.g.*, *Classifying Toothpaste*, *supra* note 5 ("[Y]ou don't need to be a classification expert to know that at least some of this reclassification wasn't only inappropriate—it was just plain dumb."); Editorial, *Finding the Wrong Answer*, USA TODAY, Apr. 14, 2006, at A20 ("For the intelligence community, trying to white-out what was once public information just discredits its legitimate concerns about today's real secrets."); Scott Shane, *Why the Secrecy? Only the Bureaucrats Know*, N.Y. TIMES, Apr. 16, 2006, at C4 ("Secrecy comes as instinctively to bureaucrats as dam-building does to beavers.").

56 The Information Security Oversight Office (ISOO) promised to follow up on the extent of the retroactive classification, but no such follow-up has appeared. INFO. SEC. OVERSIGHT OFFICE, *supra* note 41, at 9, 13, 16, 20 & n.21. Nor are there any government-wide statistics on retroactive classification. ISOO reports a handful of cases each year, but its numbers are vastly under-inclusive because they do not count retroactive classification that takes place outside of the executive order's reporting requirements—an issue taken up in depth later on. Telephone Interview with William J. Bosanko, Chief Operating Officer, Nat'l Archives and Records Admin., Former Dir., Info. Sec. Oversight Office (Nov. 1, 2013) (notes on file with author); *see also infra* subsection I.C.2–3.

B. *The History of Retroactive Classification*

To understand the origins of retroactive classification, it helps to look briefly at the development of the classification system as a whole. The current security classification system consists of three tiers: "top secret," "secret," and "confidential."[57] "Top secret" covers information that could be expected to cause "exceptionally grave" damage to national security if disclosed.[58] "Secret" covers information expected to do "serious damage" if revealed.[59] And "confidential" applies to documents whose disclosure would be expected to cause "damage" that is neither "serious" nor "exceptionally grave."[60] The classification rules govern internal access to government information, but they also affect what individuals outside government can do with the information. This effect on outsiders is the focus of the Article.

Americans take the classification system for granted. References to it abound in popular culture.[61] Business organizations have even adopted their own versions of the tiers of secrecy.[62] But in the long history of government secrets—a history that reaches back to the constitutional debates themselves—the classification system is relatively new.[63] Indeed, it was not until 1940 that the formal system for classifying documents started to emerge. In that year, President Franklin Roosevelt issued Executive Order 8381, which adopted a set of rules for classifying military documents.[64] The classification system gained traction over the course of World War II and

---

[57] Exec. Order No. 13,526, § 1.7, 3 C.F.R. 298, 302 (2010), *reprinted in* 50 U.S.C. § 3161 app. (2012).

[58] *Id* § 1.2(a)(1).

[59] *Id.* § 1.2(a)(2).

[60] *Id.* § 1.2(a)(3).

[61] *See, e.g.*, *Todd Wilbur's Top Secret Recipes*, TOP SECRET RECIPES, http://www.topsecretrecipes.com/home.php (last visited Feb. 27, 2014), *archived at* http://perma.cc/65BG-DZ8H; *Top Secret*, OFFICE PLAYGROUND, http://www.officeplayground.com/Top-Secret-P216.aspx (last visited Feb. 27, 2014), *archived at* http://perma.cc/LCS2-8VBF.

[62] *See, e.g.*, Rafael Etges & Karen McNeil, *Understanding Data Classification Based on Business and Security Requirements*, 5 INFO. SYS. CONTROL J. ONLINE 1, 4 fig.2 (2006), *available at* http://www.isaca.org/Journal/Past-Issues/2006/Volume-5/Documents/jopdf0605-understanding-data.pdf.

[63] *See* Louis Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers*, 120 U. PA. L. REV. 271, 273 (1971) ("From our national beginnings, the Government of the United States has asserted the right to conceal and, therefore, in practical effect not to let the people know."); *see also* ARTHUR M. SCHLESINGER, JR., THE IMPERIAL PRESIDENCY 332 (1973) ("[T]he republic was conceived in secrecy.").

[64] Richard C. Ehlke & Harold C. Relyea, *The Reagan Administration Order on Security Classification: A Critical Assessment*, 30 FED. BAR NEWS & J. 91, 92 (Feb. 1983).

the first years of the Cold War.[65] In 1951, President Harry Truman issued an executive order extending the military's classification rules to "all departments and agencies of the Executive Branch of the Government."[66]

In the decades since President Roosevelt established the classification system, Presidents have incrementally modified it through nine executive orders.[67] President Dwight Eisenhower reduced the number of tiers of classified information from four to three.[68] President Jimmy Carter ordered automatic declassification of all but "top secret" documents after six years.[69] President Ronald Reagan put the automatic declassification on hold and decreed that "[i]nformation shall be classified as long as required by national security considerations."[70] For all the changes made by the various executive orders, however, the structure of the classification system today is essentially the same as it was in 1940. The difference is that the number of classified documents has skyrocketed. In 1982, the government classified seventeen million documents.[71] In 2012, the government classified more than ninety-five million.[72] Experts estimate the universe of classified documents to be between four billion and one trillion—but no one knows the exact figure.[73] And the growth of the classification system has been even more pronounced in the decade since the September 11th terrorist attacks.[74]

In this slow progression of executive orders, the history of retroactive classification begins in 1978, when President Carter's executive order

---

65 *See* John Cloud, *American Cartographic Transformations During the Cold War*, 29 CARTOGRAPHY & GEOGRAPHIC INFO. SCI. 261, 264 (2002) ("American scientific and technical mobilization for the Second World War was accompanied by broad adoption of compartmentalized security systems and secrecy protocols.")

66 Exec. Order No. 10,290, 3 C.F.R. 789 (1949–1953), *revoked by* Exec. Order No. 10,501, 3 C.F.R. 979 (1949–1953), *as amended by* 3 C.F.R. 292 (1971), 50 U.S.C. § 401 (1970).

67 *See* ARVIN S. QUIST, SECURITY CLASSIFICATION OF INFORMATION 72 tbl.3.1.C (2002), *available at* http://www.fas.org/sgp/library/quist; *see also* Exec. Order 12,958, § 1.7(c), 3 C.F.R. 333, 338 (1996), *reprinted in* 50 U.S.C. § 435 (1996); Exec. Order No. 13,526, §1.7(c), 3 C.F.R. 298, 302-03 (2010), *reprinted in* 50 U.S.C. § 435 (2011).

68 Exec. Order No. 10,501, 3 C.F.R. 459 (1967). President Truman added a fourth tier. Exec. Order No. 10,290, § 2, 3 C.F.R. 471-472 (1952).

69 Exec. Order No. 12,065, § 1-401, 3 C.F.R. 190, 193 (1979).

70 Exec. Order No. 12,356, § 1.4(a), 3 C.F.R. 166, 169 (1983).

71 INFO. SEC. OVERSIGHT OFFICE, ANNUAL REPORT TO THE PRESIDENT FY 1982, at 1 (1983), *available at* http://www.archives.gov/isoo/reports/1982-annual-report.pdf.

72 INFO. SEC. OVERSIGHT OFFICE, ANNUAL REPORT TO THE PRESIDENT FY 2012, at 7 (2013), *available at* http://www.archives.gov/isoo/reports/2012-annual -report.pdf.

73 *See* Peter Galison, *Removing Knowledge*, 31 CRITICAL INQUIRY 229, 230-31 (2004), *available at* http://www.fas.harvard.edu/~hsdept/bios/docs/Removing%20Knowledge.pdf.

74 *See* Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1, *available at* http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print.

became the first to mention retroactive classification.[75] The order banned the practice by stating that "[c]lassification may not be restored to documents already declassified and released to the public under this Order or prior Orders."[76] Was this a preemptive ban or a response to some existing problem? Steven Garfinkel, the director of the Information Security Oversight Office at the time, said the order was not a response to any particular instance of retroactive classification.[77] Rather, he stated, it was part of the executive order's larger message that openness would be the order of the day.[78]

Four years later, in 1982, President Reagan took a different tack with his order on the classification system. In general, President Reagan's order was seen as "clearly revers[ing]" a thirty-year trend toward declassification by emphasizing the need for secrecy over openness.[79] When it came to retroactive classification in particular, President Reagan's order allowed the president or an agency head to "reclassify information previously declassified and disclosed," provided that "(1) the information requires protection in the interest of national security; and (2) the information *may reasonably be recovered*."[80]

The new classification power encountered profound skepticism during congressional hearings that year. Morton Halperin, who had served on President Richard Nixon's National Security Council, outlined what he saw as "very serious constitutional problems."[81] He feared that people might receive unclassified documents or hear unclassified remarks at a public meeting, only to discover later on that the information had been retroactively classified.[82] This is "a position which many private citizens, journalists and scholars, strive to not ever get into," Halperin said, "a position where they know classified information that they are not supposed to disseminate further."[83] Historian Anna K. Nelson warned of the effect of retroactive classification on memoirs, autobiographies, and interviews of former officials. Not only would retroactive classification "encourag[e] the

---

75 Exec. Order No. 12,065, 3 C.F.R. 190 (1979).

76 Exec. Order No. 12,065, § 1-607, 3 C.F.R. 190, 195 (1979).

77 Telephone Interview with Steven Garfinkel, Former Dir., Info. Sec. Oversight Office (Oct. 11, 2013) (notes on file with author).

78 *Id.*

79 Ehlke & Relyea, *supra* note 64, at 96.

80 Exec. Order No. 12,356, § 1.6(c), 3 C.F.R. 166, 170 (1983) (emphasis added).

81 *Executive Order on Security Classification: Hearings Before the Subcomm. of the H. Comm. on Gov't Operations*, 97th Cong. 56 (1982) [hereinafter *Executive Order on Security Classification Hearings*].

82 *Id.*

83 *Id.*

distortion of history," but it would also harm future decisionmaking.[84] "The knowledge that documents and records are equally available to all has kept many a participant an honest observer," Nelson said. She continued: "This provision has no place in a representative democracy."[85]

In the face of much criticism, the administration sent two officials to the hearings to defend retroactive classification. These officials described retroactive classification as a modest tool for cleaning up the occasional mistake in the declassification process. Steven Garfinkel, the director of the Information Security Oversight Office, explained that President Carter's executive order had been "inflexible" in the sense that a document accidentally declassified and released could never be reclassified even if it "was in the hands of one person . . . quite willing" to give it back.[86] Retroactive classification would fix that problem, Garfinkel insisted, by allowing the government to put the information safely behind the veil of classification.[87]

But what if the recipient of a declassified document refused to return it? The executive order said documents would be retroactively classified only if they could "reasonably be recovered."[88] The subcommittee pressed Garfinkel and Deputy Assistant Attorney General Richard Willard. "What type of recovery action is reasonable?" asked Representative Ted Weiss.[89] Would lying be reasonable? Would force? Weiss pointed to recent reports of a researcher who had received declassified documents from the National Archives and then, at the request of the Archives, sent the documents back.[90] When the government received the documents, it retroactively classified eleven pages of them and refused to return them to the researcher despite earlier assurances that the researcher would get everything back.[91]

---

84 *Id.* at 110 (statement of Anna K. Nelson).

85 *Id.*

86 *Id.* at 179 (statement of Steven Garfinkel, Dir. of the Info. Security Oversight Office); *see also id.* at 130-31 (statement of Steven Garfinkel); George Lardner, Jr., *Officials Defend Deceit In Retrieving Secrets*, WASH. POST, May 6, 1982, at A5 (reporting that during the hearing, Garfinkel took the stance that he would not rule out the use of deception in attempting to reclassify documents).

87 *Executive Order on Security Classification Hearings*, *supra* note 81, at 179.

88 Exec. Order No. 12,356, § 1.6(c), 3 C.F.R. 166, 170 (1983).

89 *Executive Order on Security Classification Hearings*, *supra* note 81, at 179 (statement of Rep. Weiss).

90 *Id.* at 180-81; *see also* George Lardner, Jr., *Air Force Pulls Back on '53 Secret Papers*, WASH. POST, Apr. 5, 1982, at A5; George Lardner, Jr., *Air Force Abandons Attempt To Reclassify Old Documents*, WASH. POST, Apr. 20, 1982, at A2.

91 Lardner, *Air Force Pulls Back on '53 Secret Papers*, *supra* note 90; *see also* Lardner, *Air Force Abandons Attempt to Reclassify Old Documents*, *supra* note 90. Notably, at the time, President Carter's executive order banned retroactive classification. Exec. Order No. 12,065, § 1-607, 3 C.F.R. 190, 195

The incident left the subcommittee concerned about the breadth of what the administration might consider reasonable. Both Garfinkel and Willard said that deception was not preferred but could be used in certain circumstances.[92] While Willard assured the subcommittee that force would not be used to retrieve a document, Garfinkel did not "want to be on the record to say that could never happen."[93] These equivocal assurances did little to assuage the subcommittee's concerns that the power would be abused.

At the end of the back-and-forth, Representative Weiss was still concerned. He asked about the classification status of records that had been stolen from the overrun American embassy in Iran and disseminated throughout the world.[94] An American researcher, returning home with some of these documents, had them confiscated by customs.[95] "Why," asked Weiss, "would the U.S. government have to prevent the American citizens from seeing information, classified or not, that is circulating freely elsewhere in the world?"[96] The question sounds eerily familiar in the wake of the WikiLeaks and Edward Snowden disclosures. "If something is widely known throughout the world, then it is hard for me to see how an additional disclosure would cause damage to the national security," Willard, the Justice Department official, responded.[97] "[I]t is hard for me to see that there would be a justification for classifying information that was widely circulating throughout the world."[98] And yet, that is exactly how retroactive classification has been used—to classify information that is already widely known.

C. *The Rules Governing Retroactive Classification*

This Section explains how, in the Internet Age, the rules governing retroactive classification provide no effective constraint on the practice's use. To see why the rules are flawed, it is necessary to examine the three different methods of retroactive classification. The remainder of Part I discusses the rules that apply to each.

(1979). After two unflattering articles in the *Washington Post*, the government reversed its retroactive classification decision. Lardner, *Air Force Abandons Attempt to Reclassify Old Documents*, *supra* note 90.

92 *Executive Order on Security Classification Hearings*, *supra* note 81, at 181.

93 *Id.*

94 *Id.* at 182-83.

95 *Id.*

96 *Id.* at 183.

97 *Id.*

98 *Id.*

1. Retroactive Reclassification

With retroactive *re*classification, the document starts out as classified. The government then declassifies it and releases it to the public. Somewhere down the line, the government decides to classify it again. This is the type of retroactive classification discussed in the executive order, which says:

> (c) Information may not be reclassified after declassification and release to the public under proper authority unless:
>
> . . .
>
> (2) the information may be reasonably recovered without bringing undue attention to the information;
>
> (3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office.[99]

Under the current executive order, and under President Reagan's and President George W. Bush's as well, the key provision is the one limiting retroactive classification to information that can be "reasonably recovered."[100] That is because retroactive classification seems most absurd when widely known information suddenly becomes secret. The executive order's implementing regulations attempt to prevent that outcome by defining "reasonably recovered" to mean situations where "[m]ost individual recipients or holders are known and can be contacted and all instances of the information to be reclassified will not be more widely disseminated."[101]

The goal is to limit retroactive classification to information that can actually be blotted from the public domain, but the rule cannot live up to that goal. In this age of rapid electronic communications, where information can be instantaneously copied and republished by anyone with Internet access, it is impossible to know whether something can be reasonably recovered. For the government to know that "most" recipients of the document can be contacted, it would have to know how far the information

---

99 Exec. Order No. 13,526, § 1.7(c)(2)-(3), 3 C.F.R. 298, 302 (2010). Special procedures exist for documents in the "physical and legal custody" of the National Archives. *Id.* § 1.7(c)(4).

100 Exec. Order No. 13,292, § 1.7(c)(2), 3 C.F.R. 196, 200 (2004); *see also* Exec. Order No. 12,356, § 1.6(c), 3 C.F.R. 166, 169 (1983).

101 Classified National Security Information, 32 C.F.R. § 2001.13(b)(1)(i) (2010). Every president to allow retroactive classification has employed a similar definition of "reasonably recovered." *See, e.g.*, Classified National Security Directive No. 1, 32 C.F.R. § 2001.13(a)(1) (2004); Classified National Security Information, 32 C.F.R. § 2001.6 (1982).

has spread. But once a document is posted online, that is not possible. And this problem does not just apply to information already online. There is a good chance that any document released, even if only in paper form, is headed online; even if it is not yet online, it can be uploaded at any moment and quickly reproduced. The notion of tracking down information and determining how far it has spread may have been practical in 1982, but it is not in 2015.[102] One need look no further than the WikiLeaks and Edward Snowden disclosures to see the impossibility of tracking down and recovering information that has made it onto the Internet.[103] In fact, the federal government still does not know the full extent of the disclosures today.[104] Thus, in today's networked world, retroactive classification's "reasonably recovered" standard is just not implementable.

Of course, the government could take the uncertainty about a document's recoverability as a sign that it should refrain from retroactive classification. But that is not what the government has done. Rather, the government has gone forward with retroactive classification in spite of the uncertainty. And, as discussed below, much retroactive classification does not even pay lip service to the executive order's recoverability and reporting requirements.

Before discussing the other methods of retroactive classification, however, it is important to note another feature of the executive order, a feature with implications far beyond national security law. Retroactive classification's implementing regulations boldly assert that members of the public have an obligation not to reveal classified information that the government has released to them:

---

102 This is especially true with the so-called Deep Web. *See generally* Lev Grossman & Jay Newton-Small, *The Secret Web: Where Drugs, Porn and Murder Live Online*, TIME, Nov. 11, 2013, at 28, 28, *available at* http://content.time.com/time/magazine/article/0,9171,2156271,00.html#ixzz2q OpDfb5e. President Obama's order seems more aware than its forerunners that the government releases information online. *See* Exec. Order No. 13,526, 3 C.F.R. 183 (2010). When the government makes information available on one of its websites, the implementing regulations state, no retroactive classification can take place until "consideration is given as to the number of times the information was accessed, the form of access, and whether the information at issue has been copied, referenced, or publicized." 32 C.F.R. § 2001.13(b)(1)(iii) (2010). But this provision does not apply to government information posted on private websites. *See* Telephone Interview with William J. Bosanko, *supra* note 56.

103 *See* Scott Shane & Andrew W. Lehren, *Leaked Cables Offer a Raw Look Inside U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1; *see also* Mark Mazzetti & Michael S. Schmidt, *Ex-C.I.A. Worker Says He Disclosed U.S. Surveillance*, N.Y. TIMES, June 10, 2013, at A1.

104 Mark Mazzetti & Michael S. Schmidt, *Officials Say U.S. May Never Know Extent of Leaks From Spy Agency*, N.Y. TIMES, Dec. 5, 2013, at A1.

> The recipients or holders who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to, their obligation not to disclose the information, and be requested to sign an acknowledgement of this briefing.[105]

This is quite a radical statement. It foists an "obligation" of confidentiality on someone without a security clearance, someone who has never bargained for nor agreed to such a duty. But where do we find the authority for such an obligation? The executive order and its implementing regulations do not say. Nor do they specify the scope of the obligation. Does the obligation apply only to citizens? Does it include resident aliens? Does it apply to an Australian national operating a website in Sweden?[106] Again, there are no answers.

The notion of such an obligation is particularly interesting because it echoes a recurring dissent in Supreme Court case law that everyday Americans have a duty to keep the government's secrets. This obligation was epitomized in Chief Justice Burger's *Pentagon Papers* dissent, in which he referred to "one of the basic and simple duties of every citizen with respect to the discovery or possession of stolen property or government documents. That duty, I had thought—perhaps naively—was to report forthwith, to responsible public officers."[107] Chief Justice Burger went on to say that the obligation fell upon "taxi drivers, Justices, and the *New York Times*."[108] Justice Blackmun's dissent in that case also discussed the obligation to keep the government's secrets. Justice Blackmun warned that media outlets should be "fully aware of their ultimate responsibilities to the United States of America" because, if leaks harmed the country, "people will know where the responsibility for these sad consequences rests."[109] The pages of the *United States Reports* contain many other such references. Retroactive classification is fascinating for its willingness to endorse the idea that people outside government bear this obligation of secrecy.[110]

---

105 Classified National Security Information, 32 C.F.R. § 2001.13(b)(3) (2010) (emphasis added).

106 *See* Danny O'Brien, *Technicalities: 10 Questions on WikiLeaks*, COMM. TO PROTECT JOURNALISTS (Apr. 8, 2010, 5:33 PM), http://cpj.org/blog/2010/04/technicalities-10-questions-on-wikileaks.php, *archived at* http://perma.cc/53T7-KUK2.

107 New York Times Co. v. United States, 403 U.S. 713, 751 (1971) [hereinafter *Pentagon Papers*] (Burger, C.J., dissenting).

108 *Id.*

109 *Id.* at 762-63 (Blackmun, J., dissenting).

110 *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524, 547-48 n.2 (1989) (White, J., dissenting); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 560 (1976). *But see, e.g.*, Oral Argument at 34:43, Fla. Star v.

The executive order thus creates an uneasy combination. It provides no effective constraint on the government's ability to retroactively classify documents, even as it foists an extraordinary duty of confidentiality on members of the public. The irony, as the following discussion will show, is that the other methods of retroactive classification are more lawless—more willing to duck even the weak limitations imposed by the executive order.

2. Retroactive "Original" Classification

The second method, retroactive "original" classification, is very similar to retroactive reclassification. The only difference is that the document starts off *un*classified, rather than classified. The government releases this unclassified document to the public and later on decides to classify it. Because the document was not classified to begin with, it is considered an "original" classification, not a *re*classification, and thus does not have to comport with the "reasonably recovered" and reporting requirements of the executive order.[111] This allows retroactive classification to fly below the radar. As Bill Leonard, a former director of the Information Security Oversight Office, confirmed: "[W]here an actual report is released to the public in a non-classified format and someone comes behind later on [to classify it] . . . that may be something that is very dumb but is not prohibited by the executive order."[112]

Examples of retroactive original classification include the following events:

- In 2011, the military posted a report online about Afghan soldiers' attacks on their American colleagues.[113] The report concluded that the resentment driving this violence was far deeper than the military had previously acknowledged.[114] Shortly before the *Wall Street Journal* reported on the findings, however, the military retroactively classified the report, even though it remained publicly accessible on the Internet.[115]

B.J.F., 491 U.S. 524 (1989) (No. 87-0329), *available at* http://www.oyez.org/cases/1980-1989/1988/1988_87_329 ("Unidentified Justice: '[I]f somebody comes over and hands me a classified document that he's not supposed to give me, and I look at it[,] I haven't violated the law.'").

111 *See* Exec. Order No. 13,526, § 1.7(c), 3 C.F.R. 298, 302 (2010).

112 Telephone Interview with Bill Leonard, Former Dir., Info. Sec. Oversight Office (Oct. 9, 2013) (notes on file with author).

113 *See* Dion Nissenbaum, *Report Sees Danger in Local Allies*, WALL ST. J., June 17, 2011, at A8.

114 *Id.*

115 *Id.* A *New York Times* article explained that the report "was first distributed in early May 2011 as unclassified and was later changed to classified." Matthew Rosenberg, *Afghanistan's Soldiers Step Up Killings of Allied Forces*, N.Y. TIMES (Jan. 21, 2012), http://www.nytimes.com/2012/01/

- In 2010, the *Washington Post* disclosed that Kabul Bank had diverted $850 million of its holdings to government insiders.[116] The U.S. Agency for International Development (USAID) concluded that Deloitte, the accounting firm USAID had paid to help Kabul Bank keep the books, should have detected the fraud.[117] USAID released an unclassified report describing its findings, but two months later, the agency retroactively classified it, even though the report was still available online.[118]
- In 2007, the GAO presented an unclassified report to Congress about corruption in Iraq.[119] After the report was presented in public hearings and distributed to the press, the State Department retroactively classified some of the documents on which the report relied, thus forcing the GAO to remove portions of the report.[120] Again, this retroactive classification occurred even though the information had already been publicly released.[121] This and two other incidents of retroactive classification so incensed Congress that 395 members of the House voted for a resolution condemning the practice.[122]

In all of these instances, an unclassified document became classified after it entered the public domain. Granted, there are some limitations on original classification, but they are so lenient that officials joke that "you could easily classify the ham sandwich" under the original classification provisions.[123] Retroactive "original" classification is thus an easy way for

---

20/world/asia/afghan-soldiers-step-up-killings-of-allied-forces.html?pagewanted=all, *archived at* http://perma.cc/K95R-5ZLW.

116 Andrew Higgins, *Banker Feeds Afghan Crony Capitalism*, WASH. POST, Feb. 22, 2010, at A1; Al Kamen, *Now You See the Kabul Bank, Now You Don't*, WASH. POST (May 12, 2011), http://articles.washingtonpost.com/2011-05-12/politics/35265138_1_usaid-energy-resources-kabul-bank, *archived at* http://perma.cc/5HKT-WNNR.

117 Steven Aftergood, *Report on Kabul Bank Corruption Is Classified, Taken Offline*, SECRECY NEWS (May 10, 2011), http://blogs.fas.org/secrecy/2011/05/kabul_bank, *archived at* http://perma.cc/JH6G-LP8V.

118 *Id.*

119 *Examining the Effectiveness of U.S. Efforts to Combat Waste, Fraud, Abuse, and Corruption in Iraq: Hearing Before the S. Comm. on Appropriations*, 110th Cong. 99, 102 (2008) (response of Comptroller General David Walker); 153 CONG. REC. 11,551, 11,577 (2007). Stuart Bowen, the Special Inspector General for Iraq Reconstruction, was "aware of reports that draft documents were made available to the media and that subsequently drafts were marked as classified," but had "not formally reviewed these incidents." *Id.* at 114.

120 153 CONG. REC. 11,551, 11,577 (2007).

121 *Id.*

122 *Id.* at 11,585.

123 Telephone Interview with William J. Bosanko, *supra* note 56; *see also* Exec. Order No. 13,526, 3 C.F.R. 298 (2010).

officials bent on secrecy to employ the retroactive classification power without reporting their actions or worrying about whether the information can be "reasonably recovered."

3. Retroactive Classification of Inadvertently Declassified Documents

The third method of retroactive classification completely skirts the executive order by asserting that the order does not apply to documents inadvertently declassified in the first place. The logic is that the executive order refers to information declassified and released "under proper authority," so if the information was inadvertently declassified and released, it did not become public "under proper authority."[124] Thus, the order's limitations and reporting requirement do not apply. Or so the argument goes. "What often happens," explained attorney Mark Zaid, "is they say, 'It was never properly declassified, so we're not properly reclassifying it.'"[125]

This reasoning was on display in the National Archives scandal. Matthew Aid, the researcher who uncovered the secret retroactive classification program, recalls a meeting during where the CIA's classification chief said, "the documents in question had been found to have been improperly declassified and that the law gave the CIA and the Air Force the authority" to treat those documents as classified.[126] Similarly, the official audit of the retroactive classification noted that the classification authorities had "determined that because of the many mistakes [in declassification], this was not reclassification."[127] The semantics of all these different classification actions are so convoluted that officials have even referred to the National Archives scandal as a "un-declassification."[128]

Among all the methods of retroactively classifying documents, this third method is particularly dubious because it clashes with the historical justification for retroactive classification. As discussed above, the Reagan administration implemented retroactive classification to deal with precisely

---

124 Exec. Order No. 13,526 §1.7(c), 3 C.F.R. 298, 302-03 (2010).

125 Telephone Interview with Mark Zaid, Managing Partner, Mark S. Zaid, P.C. (Oct. 18, 2013) (notes on file with author).

126 Telephone Interview with Matthew Aid, *supra* note 53.

127 INFO. SEC. OVERSIGHT OFFICE, *supra* note 41, at 9.

128 The agencies needed a creative excuse to legitimize their actions. For the first half of the program, President Clinton's executive order banned retroactive classification. Exec. Order No. 12,958, 3 C.F.R. 333 (1996). For the second half, while President George W. Bush's order permitted reclassification, it imposed a reporting requirement that the agencies disobeyed. Exec. Order 13,292 § 1.7(c)(3), 3 C.F.R. 196, 200 (2004). Retroactive "original" classification was not an option because the documents had been classified initially.

the issue of documents that had been inadvertently declassified and released. As a Justice Department official told Congress in 1982, "[p]eople are only human" and retroactive classification "gives us the power in some situations to try to rectify mistakes."[129] In light of this history, it is hard to say that the executive order does not apply if the document was declassified by mistake. That the agencies can get away with this line of argument suggests the lawlessness of retroactive classification.

* * *

No matter what one calls these three methods of retroactive classification, they all lead to the same result: documents the government released to the public later become classified. The laws currently in place are simply inadequate to deal with the retroactive classification power.

II. CAN I BE PROSECUTED FOR DISOBEYING RETROACTIVE CLASSIFICATION?

Now that we have seen how retroactive classification works, the question is whether a retroactive classification decision can be enforced. If the government provides me with a document today, and retroactively classifies it tomorrow, do I have to refrain from publishing it? If I disobey the classification decree, can I be punished?

This Part first looks at whether recipients of traditionally classified documents can be prosecuted for disseminating them. In the wake of the WikiLeaks and Edward Snowden disclosures, this question has become a matter of intense scholarly debate. Next, this Part asks how the analysis would differ if the documents were retroactively classified. Essentially, Part II argues that, despite significant statutory and constitutional hurdles, a prosecution based on retroactively classified documents could pass muster.

A. *Classified Documents*

There is no law against publishing classified documents per se. Rather, a patchwork of criminal laws protects various types of information that happens to be classified. The most prominent law in this patchwork is the Espionage Act, which protects "information relating to the national defense."[130] The Espionage Act is itself a patchwork of provisions covering

---

129 *Executive Order on Security Classification Hearings*, *supra* note 81, at 182 (statement of Richard Willard).

130 Espionage Act, 18 U.S.C. §§ 792–799 (2012).

everything from cloak-and-dagger espionage to activities more often associated with journalism.[131] The most relevant provision for our purposes is subsection 793(e), which punishes those who receive and redistribute classified information. Specifically, the provision targets anyone who,

> having unauthorized possession of . . . 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 . . . 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.[132]

By its terms, this provision would apply to someone outside the government, such as a journalist or a member of the public, who receives and publishes a classified document. Yet no journalist has ever been prosecuted for publishing classified information, and only two members of the public—other than those working for foreign governments—have been prosecuted for disseminating information given to them by a government source.[133]

Indeed, leak recipients are typically seen as protected from prosecution. When the government does decide to prosecute a leak, it usually goes after the source, not the recipient. This practice is so entrenched that some scholars have even attributed doctrinal significance to it, referring to it as the "source/distributor divide."[134] But, in recent years, spurred on by the WikiLeaks disclosures in particular, scholars have debated whether leak recipients really are immune from prosecution under the Espionage Act. Could someone who innocently received classified information be punished for publishing it? The debate remains unsettled, perhaps because there have been no cases with which to test each side's assumptions. The following

---

131 *See id.* § 793(e).

132 *Id.* Subsection 793(d) applies to those lawfully in possession of the information, and subsection 793(g) targets "two or more persons [who] conspire to violate any of the . . . provisions of the section." *Id.* § 793(g).

133 *See infra* notes 159-165 and accompanying text; *see also* Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 197 (2007).

134 David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 516 (2013); *see also id.* at 525 ("As compared to the legal vulnerability of their government sources, journalists and other private actors who publish leaked information appear to occupy a privileged position."). *But see* Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information*, 6 J. NAT'L SECURITY L. & POL'Y 409, 411 (2013).

discussion sets out the chief arguments for and against the success of such a prosecution.[135]

1. Why an Espionage Act Prosecution Would Fail

The case that a prosecution would fail begins with the text of the Espionage Act. Subsection 793(e) uses the verbs "communicates, delivers, [and] transmits," but omits the word "publishes."[136] One of the district court judges in the *Pentagon Papers* case, for example, found the Espionage Act inapplicable to the newspaper for that reason.[137] The judge wrote that if Congress wanted to punish publication—as distinct from communication—it would have used the word "publishes," as other statutory provisions surrounding the Espionage Act do.[138] Justice Marshall's *Pentagon Papers* opinion added that this interpretation "has some support in the legislative history."[139] However, Harold Edgar and Benno Schmidt, Jr., coauthors of the seminal work on the Espionage Act, concluded that there is not "a single clear statement in the lengthy legislative history of these bills that the word 'communicates' does not embrace publishing."[140] Patricia Bellia has explained that the use of the word "publishes" in surrounding statutory provisions does not mean the *expressio unius est exclusio alterius* canon should be invoked because the surrounding provisions either came from different eras than the Espionage Act or dealt with much narrower categories of classified information.[141] Thus, the significance of the omission of the word "publishes" is very much a matter of debate.

The second significant argument for why such a prosecution would fail is the Espionage Act's "bad faith" requirement. In *Gorin v. United States*, the defendant, a Nazi agent, claimed that the Espionage Act provision under

135 *See* Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1495 (2012) ("[C]urrent doctrine does not resolve whether . . . the government can punish ex post what it cannot stop the press from publishing ex ante."); Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 264 (2008) ("Although it is not always clear whether this was Congress's intent, the press plainly is vulnerable to indictment under these provisions."); *id.* at 280 ("[I]t is obvious that the press cannot be confident that the Supreme Court would hold that a criminal prosecution of the press for the publication of national security information is unconstitutional.").

136 *See* Bellia, *supra* note 135, at 1487.

137 *See* United States v. New York Times Co., 328 F. Supp. 324, 328-29 (S.D.N.Y. 1971); *see also Pentagon Papers*, 403 U.S. 713, 745 (1971) (Marshall, J., concurring).

138 *New York Times*, 328 F. Supp. at 328-29; *see also* 18 U.S.C. §§ 794(b), 797–798 (2012).

139 *Pentagon Papers*, 403 U.S. 713, 745 (1971) (Marshall, J., concurring).

140 Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 1034 (1973).

141 Bellia, *supra* note 135, at 1490.

which he was convicted was unconstitutionally vague because it was not clear what information could be communicated without transgressing the Act.[142] The Supreme Court held that the statute "requires those prosecuted to have acted in bad faith."[143] Experts have noted that a "bad faith" requirement would be hard to prove against members of the public, including journalists, because the intent behind their publishing the information may well be to serve the public good, not to aid a foreign nation or hurt the United States.[144]

Beyond the statutory arguments, however, many experts believe that this type of Espionage Act prosecution would fail for First Amendment reasons. Commentators point to *Bartnicki v. Vopper* and its forerunners, in which the Supreme Court held unconstitutional state and federal provisions that punished people for publishing truthful information that they had lawfully received.[145] *Florida Star* and *Cox Broadcasting* concerned state laws against publishing the names of rape victims.[146] *Landmark Communications* in turn dealt with a state law enforcing the confidentiality of judicial misconduct proceedings.[147] Both *Oklahoma Publishing* and *Daily Mail* involved challenges to prohibitions on publishing information about juvenile defendants.[148] And *Bartnicki* itself concerned a federal law prohibiting the disclosure of the contents of an intercepted phone call, even if the person making the disclosure was not the one who intercepted the call.[149] Each of these cases stood for the following proposition, summed up by the Supreme Court in *Daily Mail*: "[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[150]

Many experts say this line of cases would protect one who publishes classified documents, provided he did not break the law in obtaining them. Yochai Benkler writes that any effort to prosecute the *New York Times* or the

---

142 Gorin v. United States, 312 U.S. 19, 23 (1941).

143 *Id.* at 27-28.

144 Papandrea, *supra* note 135, at 266.

145 *See* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) (reasoning that "a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern").

146 Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 471-72 (1975).

147 Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829, 830, 845-46 (1978).

148 Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 98-99 (1979); Okla. Publ'g Co. v. Dist. Court, 430 U.S. 308, 308 (1977).

149 *Bartnicki*, 532 U.S. at 518-19.

150 *Daily Mail*, 443 U.S. at 103.

Guardian for their publication of the WikiLeaks cables, for example, "would founder on the bulwarks of the First Amendment."[151] Jack Balkin argues that "the government cannot punish the press if it obtained the information lawfully and merely published what was leaked unless there would almost certainly be very serious harm to the nation."[152] Geoffrey Stone believes a journalist could not be convicted for publishing classified information unless the prosecution satisfied the same demanding standard required for a prior restraint: Would publication "surely result in direct, immediate, and irreparable damage to our Nation or its people?"[153] Many experts put much confidence in the power of the First Amendment to thwart an Espionage Act prosecution. But not everyone agrees.

2. Why an Espionage Act Prosecution Would Succeed

Those who believe an Espionage Act prosecution could succeed focus not on the potential statutory infirmities of the Espionage Act, but rather on the First Amendment concerns that such a prosecution would raise.[154] Would the First Amendment block prosecution of someone who received, but did not steal, classified documents and then proceeded to publish them?

The strongest evidence that the First Amendment would allow such a prosecution may well come from the *Pentagon Papers* case, long considered a resounding victory for the press. The *Pentagon Papers* case concerned the government's request for a prior restraint to prevent the *New York Times* and

---

151 Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 356 (2011).

152 Jack M. Balkin, *The First Amendment Is an Information Policy*, 41 HOFSTRA L. REV. 1, 21 (2012).

153 *Pentagon Papers*, 403 U.S. 713, 730 (1971) (Stewart, J., concurring); *see* Stone, *supra* note 133, at 202; *see also* Benkler, *supra* note 151, at 354 ("[T]he First Amendment does not permit prosecution of a journalist transmitting truthful information of public interest absent a need of the highest order." (internal quotation marks omitted)); Papandrea, *supra* note 135, at 280-81. First Amendment attorney Abbe Lowell had said courts would apply the "clear and present danger" test in this scenario. *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 34 n.10 (2010) [hereinafter *WikiLeaks Hearing*] (statement of Abbe D. Lowell).

154 There has been much talk of amending the Espionage Act to better address current threats to national security. For example, the SHIELD Act would have amended the Espionage Act to make it a crime for downstream recipients to publish classified information concerning "human intelligence" sources. *See* Securing Human Intelligence and Enforcing Lawful Dissemination (SHIELD) Act, H.R. Res. 703, 112th Cong. (2011); *see also* Michael A. Lindenberger, *The U.S.'s Weak Legal Case Against WikiLeaks*, TIME (Dec. 9, 2010), http://content.time.com/time/
nation/article/0,8599,2035994,00.html, *archived at* http://perma.cc/M8X9-LJT7 (quoting Senator Mitch McConnell, who called for the prosecution of Julian Assange and said that, if the barriers to prosecution "become[] a problem, we need to change the law").

the *Washington Post* from publishing classified documents about the Vietnam War.[155] The Supreme Court held the prior restraint unconstitutional, but in the dicta of the Court's separate opinions, a majority of the justices seemed to believe that the First Amendment would have permitted a criminal prosecution of the reporters who published the classified documents.[156] As Justice Stewart wrote: "Undoubtedly Congress has the power to enact specific and appropriate criminal laws to . . . preserve government secrets. Congress has passed such laws, and several of them are of very colorable relevance to the apparent circumstances of these cases."[157] The dicta in this case support the claim that an Espionage Act prosecution would survive a First Amendment challenge.[158]

Indeed, in 2006, a district court in Virginia relied on the *Pentagon Papers* dicta in allowing an Espionage Act prosecution of two lobbyists for the American Israel Public Affairs Committee.[159] In that case, *United States v. Rosen*, the lobbyists were charged with "conspiring to transmit information relating to the national defense to those not entitled to receive it."[160] They did not have security clearances, were not employed by the government, and did not bribe their way to the classified information, much less steal it.[161] Instead, they built a relationship with a source inside the State Department, and the source passed along the confidential information, much like sources routinely do with journalists.[162] The two lobbyists then disseminated the information to another lobbyist, a journalist, and a representative of the Israeli government.[163] When they were prosecuted, the lobbyists asserted a First Amendment defense, arguing that, because they were outside the government, they had no special position of trust and were thus allowed to

---

155 *Pentagon Papers*, 403 U.S. at 714.

156 The arithmetic supporting this claim may be found, for instance, in a district court opinion from 2006. United States v. Rosen, 445 F. Supp. 2d 602, 638-39 (E.D. Va. 2006).

157 *Pentagon Papers*, 403 U.S. at 730 (Stewart, J., concurring); *see also id.* at 737 (White, J., concurring) ("I would have no difficulty in sustaining convictions under these sections on facts that would not justify the intervention of equity and the imposition of a prior restraint.").

158 Bellia, *supra* note 135, at 1470-71 ("[T]he opinions reveal the consensus of five Justices that Congress either could have or did criminalize the conduct—a proposition that only Justice Douglas (joined by Justice Black) explicitly rejected."); *id.* at 1495.

159 *See, e.g.*, *Rosen*, 445 F. Supp. 2d at 638 ("[A] close reading of these opinions indicates that the result may have been different had the government sought to prosecute the newspapers under § 793(e) subsequent to publication of the Pentagon Papers.").

160 *Id.* at 607.

161 *Id.* at 608-10.

162 *Id.*

163 *Id.* at 610.

disseminate the information they came across.[164] The district court disagreed: "[B]oth common sense and the relevant precedent point persuasively to the conclusion that the government can punish those outside of the government for the unauthorized receipt and deliberate retransmission of information relating to the national defense."[165] While the government ultimately dropped the prosecution, the district court's opinion—and its reliance on the *Pentagon Papers* dicta—is significant because it suggests that an Espionage Act prosecution is viable despite the First Amendment concerns.

Beyond the *Pentagon Papers* dicta, scholars who believe a prosecution could survive First Amendment scrutiny have challenged the relevance of the *Bartnicki* line of cases, on which the argument against prosecution relies.[166] Their main reason for challenging the *Bartnicki* line of cases is the fact that the statutes in those cases made *publication* of sensitive information illegal, but did not forbid its *receipt*.[167] The holding of *Bartnicki*, for instance, is explicitly limited to information lawfully received.[168] The Espionage Act, on the other hand, makes receipt illegal; thus, anyone who republishes the classified information cannot claim that he received it legally because receipt itself is against the law.[169] Experts also distinguish the Espionage Act from the *Bartnicki* line of cases because the Espionage Act concerns national security secrets rather than the matters of personal privacy dealt with in *Bartnicki* and its predecessors.[170] Arguably, national security is a higher state interest. Still others who believe a prosecution could succeed argue more from first principles. Judge Posner asserts that, "[a]s a matter of constitutional law, the government should be allowed to . . . punish the knowing publication or other dissemination of classified material concerning national security, provided that the material was

---

164 *Id.* at 637 ("[D]efendants here contend that the First Amendment bars Congress from punishing those persons, like defendants, without a special relationship to the government for the disclosure of [National Defense Information]. In essence, their position is that once a government secret has been leaked to the general public and the first line of defense thereby breached, the government has no recourse but to sit back and watch as the threat to the national security caused by the first disclosure multiplies with every subsequent disclosure."); *see also* Reply Brief in Support of Defendants Steven J. Rosen's and Keither Weissman's Motion to Dismiss the Superseding Indictment at 15, United States v. Rosen, No. 05-0225 (E.D. Va. Feb. 6, 2006).

165 *Rosen*, 445 F. Supp. 2d at 637.

166 Bellia, *supra* note 135, at 1508.

167 *Id.* at 1494.

168 Justice Breyer's concurrence, which Justice O'Connor joined, narrows the holding. *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (Breyer, J., concurring).

169 Bellia, *supra* note 135, at 1494.

170 *Id.* at 1508; Rodney A. Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. REV. 1099, 1169-70 (2002).

classified in accordance with proper statutory criteria (which do not yet exist)."[171] Kenneth Wainstein, who served in Homeland Security posts under President George W. Bush, told Congress in 2010 that an Espionage Act prosecution against WikiLeaks could survive a constitutional challenge.[172] As he saw it, the key was to distinguish WikiLeaks from the mainstream media, and thus "hopefully lower any First Amendment obstacles."[173] In the same 2010 hearings, Gabriel Schoenfeld emphasized that the First Amendment was originally conceived as a prohibition on prior restraints and censorship, "[b]ut laws punishing the publication of certain kinds of material after the fact were something else again."[174] He quoted Joseph Story's assertion that it was an absurdity "too wild to be indulged by any rational man" to believe that the First Amendment allowed "every citizen an absolute right to speak, or write, or print, whatever he might please."[175] Schoenfeld argued that prosecutorial discretion and the jury system were checks on punishing the publication of classified information:

> [I]f newspaper[] editors or an organization like WikiLeaks disclose[s] a secret vital to our national security—and have no justification for doing so beyond a desire to expose for exposure's sake—they should also be prepared to face the judgment of a jury . . . and the full wrath of the law.[176]

3. What to Make of the Debate

Regardless of which side is right, it is hard to dispute that the tenor of the debate has changed. A generation ago, one could be confident that the press would not be prosecuted. Now, such a prosecution is cause for concern, even for those who think the First Amendment would ultimately prevail. A recent incident involving a Fox News reporter hints at how close the media may be to facing criminal charges. In that case, reporter James Rosen built a relationship with a State Department official who leaked to Rosen classified information about North Korea. The leaker was criminally prosecuted, but surprisingly, the FBI deemed Rosen an

---

171 RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 110 (2006).

172 *WikiLeaks Hearing*, *supra* note 153, at 43.

173 *Id.* at 45; *see also* Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 224 (2007).

174 *WikiLeaks Hearing*, *supra* note 153, at 60.

175 *Id.*

176 *Id.* at 65.

unindicted co-conspirator. In an application for a warrant to search Rosen's email, the FBI said that Rosen was "at the very least . . . an aider, abettor and/or co-conspirator" in the leak.[177] Although Rosen was not prosecuted, the warrant application suggests that at least one arm of the executive branch thought downstream publishers *could* be prosecuted. The impending case against WikiLeaks' founder, Julian Assange, is another sign that the rules on punishing downstream publishers are changing.[178] It remains to be seen whether and how the Espionage Act will be applied to this most famous of leak recipients, but the prospect of prosecution certainly seems real despite the protections of the First Amendment.[179]

B. *Retroactively Classified Documents*

That recipients of classified documents could be prosecuted for republishing them raises the question: How would the analysis differ if the documents were *retroactively* classified? This Section shows that any prosecution based on retroactively classified documents would face serious hurdles, above and beyond those faced by prosecutions based on traditionally classified material. Indeed, retroactive classification challenges many of the Espionage Act's basic assumptions. Despite these challenges, this Section argues that a prosecution could succeed. In the right circumstances, a person could be convicted for publishing information that was declassified when she received it but retroactively classified later on.

1. Are the Threats of Prosecution Real?

It is tempting to say there is no threat of prosecution arising from retroactively classified documents, much less the possibility of sustaining a

---

177 Application for a Search Warrant at 27, *In re* Search of [Redacted], No. 10-0291 (D.D.C. Nov. 7, 2011), *available at* http://www.fas.org/sgp/jud/kim/warrant.pdf; *see also id.* at 3, 29, 36; Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, WASH. POST (May 19, 2013), http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_print.html.

178 A grand jury has reportedly convened to investigate Assange, and many influential voices have called for his prosecution. Lindenberger, *supra* note 154; *see also* Dianne Feinstein, Op-Ed, *Prosecute Assange Under the Espionage Act*, WALL ST. J., Dec. 7, 2010, at A19 (asserting the existence of "ample statutory authority for prosecuting individuals who elicit or disseminate the types of documents at issue" (internal quotation marks omitted)).

179 Of course, he could be charged under a different Espionage Act provision or a different statute altogether. JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 13-15 (2013), *available at* https://fas.org/sgp/crs/secrecy/R41404.pdf. *See generally* James Freedman, Note, *Protecting State Secrets as Intellectual Property: A Strategy for Prosecuting WikiLeaks*, 48 STAN. J. INT'L L. 185 (2012).

conviction. After all, former directors of the Information Security Oversight Office (ISOO) emphasize that no one would be prosecuted for anything related to retroactively classified documents. Bill Leonard, the agency's director under President George W. Bush, said that, "if through the actions of the government, somebody came into possession—legitimate possession—of the material, and the government then subsequently [classified it], those individuals wouldn't find themselves in jeopardy," though he acknowledged that prosecution could, "in theory," occur.[180] William J. Bosanko, who succeeded Leonard, also emphasized that no one would be prosecuted.[181]

But those who have experienced retroactive classification report that threats abound. James Bamford received repeated threats from the Justice Department when he refused to give back retroactively classified documents.[182] Attorney Mark Zaid recounts that the CIA threatened to revoke his security clearance and to prosecute his co-counsel (who did not have a security clearance) if they did not give back documents that had been retroactively classified.[183] Janine Brookner, a CIA-operative-turned-lawyer, reported similar threats in an interview with the *Washington Post*. She said the CIA sometimes "declassifies documents, only to reclassify them years later and demand that a plaintiff's lawyers give them back or be prosecuted."[184] And researcher Matthew Aid, who is in possession of hundreds of retroactively classified documents copied from the National Archives, said the threat of prosecution hangs over him like "the Sword of Damocles."[185] Still, none of these people has been prosecuted, which raises the question of whether the threats amount to anything real. "Is it a real threat?" Zaid asked. "Who knows? The problem is that nobody wants to be the one to risk it."[186] From a First Amendment standpoint, the mere threat of prosecution is significant because it has a chilling effect on protected

180 Telephone Interview with Bill Leonard, *supra* note 112.

181 In answering questions about retroactive classification, William J. Bosanko, former director of ISOO, often senses "there is anxiety about, is somebody going to get locked up." Telephone Interview with William J. Bosanko, *supra* note 56. "Do you know somebody who is facing that?" he asked. *Id.*

182 Telephone Interview with James Bamford, Journalist (Nov. 6, 2013) (notes on file with author).

183 Telephone Interview with Mark Zaid, *supra* note 125.

184 Peter Carlson, *Counter Intelligence: Looking to Sue the CIA? First Find Janine Brookner*, WASH. POST, Mar. 10, 2004, at C1.

185 Telephone Interview with Matthew Aid, *supra* note 53.

186 Telephone Interview with Mark Zaid, *supra* note 125.

speech, even if the threat has yet to be carried out.[187] Thus, the threat of prosecution cannot be dismissed so easily.

2. Source/Distributor Divide

With traditional leaks, the prosecutor's first task is often to separate the source from the distributor. As discussed above, prosecutors usually target the source and not the distributor (or the recipient).[188] Retroactive classification complicates even this simple dichotomy, however, by blurring the line between source and distributor. If I receive a document in response to a FOIA request and that document is retroactively classified the next day, what would I be considered if I proceed to publish the information? On the one hand, I might seem like a distributor because I passively received the document from the FOIA officer and then republished it. On the other hand, I could be considered a source because I am the one breaking the duty imposed by retroactive classification—the "obligation not to disclose the information."[189] I am the insider illicitly parting the curtain of secrecy. While the more likely interpretation is that I am the distributor, not the source, this definitional difficulty is one manifestation of the trouble that retroactive classification would pose for an Espionage Act prosecution.

3. Espionage Act

A prosecution based on retroactively classified material would also encounter problems satisfying the elements of the Espionage Act—problems beyond those discussed in the context of traditionally classified documents.[190] The most significant of these problems is that the Act covers only material that is "closely held" or secret. While the text of the Espionage Act does not mention classification status, the Supreme Court has interpreted the Act's reference to "information relating to the national defense" as a requirement that the information be secret.[191] "Where there is no occasion for secrecy, as with reports relating to national defense, *published by authority* of Congress or the military departments," the Court explained,

---

187 The First Amendment is concerned with the chilling of speech. That is why, for example, litigants can sue on overbreadth grounds. *See* Dombrowski v. Pfister, 380 U.S. 479, 486 (1965) ("The threat of sanctions may deter . . . almost as potently as the actual application of sanctions" (internal quotation marks omitted)); *cf.* Complaint for Declaratory and Injunctive Relief at 5-7, Project on Gov't Oversight v. Ashcroft, No. 04-1032 (D.D.C. June 23, 2004).

188 *See supra* note 134 and accompanying text.

189 32 C.F.R. § 2001.13(b)(3) (2010).

190 *See supra* notes 136-144 and accompanying text.

191 18 U.S.C. § 793(e) (2012).

"there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government."[192] In this passage, we see the Court construct a dichotomy between information for which there is an "occasion for secrecy" and information "published by authority" of the government. The former can be the basis for an Espionage Act prosecution, while the latter cannot. But the distinction falls apart when applied to retroactively classified documents because they are published by the government *and* considered to be secret. The courts would have to decide which of these conflicting statuses—public or secret—prevails.

A leading case from the Second Circuit emphasizes the problem. In *United States v. Heine*, the defendant reported to the Third Reich about America's industrial capacity, but his report was based entirely on public information.[193] The Second Circuit explained that the defendant's "information came from sources that were lawfully accessible to anyone who was willing to take the pains to find, sift and collate it."[194] In reversing the defendant's Espionage Act conviction, the Second Circuit held that it was "obviously lawful to transmit any information . . . which the services had themselves made public" as well as any "information which the services have never thought it necessary to withhold."[195] The court said it would defer to the government's judgment about what information should be considered secret, and if the government made the information public, that would indicate the information was not sensitive.[196] But retroactive classification again raises a difficult problem for this dichotomy between public and secret, because retroactively classified documents were both "made public" and "thought . . . necessary to withhold."[197] In reviewing an Espionage Act prosecution, a court would have to decide whether the initial public release made the document conclusively public or whether that public status could be reversed by the retroactive classification.

Finally, in 2000, the Fourth Circuit addressed a similar question in *United States v. Squillacote*.[198] The defendant, an East German-turned-Russian spy, challenged her conviction on the grounds that the information she transmitted was "available to the public" and thus "can never be considered

192 Gorin v. United States, 312 U.S. 19, 28 (1941) (emphasis added).

193 151 F.2d 813, 815 (2d Cir. 1945).

194 *Id.*

195 *Id.* at 816.

196 *See id.* ("The services must be trusted to determine what information may be broadcast without prejudice to the 'national defense.'")

197 *Id.*

198 221 F.3d 542, 575 (4th Cir. 2000).

national defense information."[199] In *Squillacote*, the information in the contested documents was available from a combination of public sources, but it had never been officially confirmed by the government.[200] Was this information public for purposes of the Espionage Act? The Fourth Circuit articulated the following test: regardless of what "unofficial," "unreliable" information may be in the public domain, "a document containing official government information relating to the national defense will not be considered available to the public (and therefore no longer national defense information) *until the official information in that document is lawfully available*."[201] In short, the court held that leaks and speculation do not remove information from the protection of the Espionage Act; only government releases can do that. But this raises a now-familiar problem when applied to retroactively classified documents because those documents used to be "lawfully available" but no longer are. Again, a court would have to decide whether to privilege the present secret status over the former public one.

4. First Amendment

The key analytical difference between prosecutions based on classified documents and those based on retroactively classified documents lies in how the First Amendment would apply in each case. With prosecutions based on traditionally classified documents, commentators rely on *Bartnicki* for the claim that the First Amendment would quash a prosecution.[202] But, as discussed above, *Bartnicki*'s relevance has been contested because it applies only to instances where the *receipt* of information is lawful, whereas the Espionage Act criminalizes the receipt of classified documents.[203] In the context of retroactive classification, however, *Bartnicki* and several of its predecessors are even less applicable as they pertain to information that the media acquired on its own, whereas retroactive classification concerns information that the *government* itself disclosed.[204]

---

199 *Id.*

200 *Id.* at 576-78.

201 *Id.* at 578 (emphasis added).

202 Stone, *supra* note 133, at 211; *supra* notes 145-152 and accompany text.

203 *See* Bartnicki v. Vopper, 532 U.S. 514, 532 (2001); *see also id.* at 540 (Breyer, J., concurring) (pointing to "lawful nature" of the media's behavior in the case); ELSEA, *supra* note 179, at 27; POSNER, *supra* note 171, at 108; Benkler, *supra* note 151, at 364; *supra* notes 166-169 and accompanying text.

204 Like *Bartnicki*, *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978), and *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979), are not relevant in this respect because they concern information that was not disclosed by the government.

The significance of the government's self-disclosure of information cannot be overstated. Instead of applying *Bartnicki*, the courts reviewing a retroactive classification prosecution would look to *Bartnicki*'s predecessors that dealt with information disclosed by the government. Those cases, described below, wrestle with whether the government may punish those who publish information that the government has itself disclosed. These cases collectively articulate a disclosure principle: Once the government discloses information to the public, it cannot punish someone for republishing it except in the most extreme circumstances.

The first of the cases to articulate the disclosure principle is *Cox Broadcasting Corp. v. Cohn*.[205] In *Cox Broadcasting*, a Georgia law made it a misdemeanor to publish the name of a rape victim.[206] In the trial of the accused rapists, a reporter learned the victim's name from the indictment and revealed it on television, leading the victim's father to sue for invasion of privacy.[207] The privacy suit relied on the law against publicizing a rape victim's name, but the U.S. Supreme Court held that the law violated the First Amendment: "Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it."[208]

The Court soon extended the disclosure principle to judicial gag orders in *Nebraska Press Ass'n v. Stuart*.[209] In that case, a state judge barred journalists from publishing "accounts of confessions or admission[s]" made by the defendant in a high-profile murder prosecution.[210] The judge insisted on this prohibition even though the information had been disclosed in court proceedings attended by the public.[211] However, on appeal, the Supreme Court held the gag order unconstitutional because it "prohibited the reporting of evidence adduced at the open preliminary hearing."[212] As the Court explained, "[t]here is nothing that proscribes the press from reporting events that transpire in the courtroom."[213]

The Supreme Court reached the same conclusion in *Oklahoma Publishing Co. v. District Court*, where a judge prohibited the press from publishing information about a juvenile defendant, even though the information was

---

205 420 U.S. 469 (1975).
206 *Id.* at 471-73.
207 *Id.* at 473-74. The victim herself could not sue because she died as a result of the attack.
208 *Id.* at 496.
209 Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559-62 (1976).
210 *Id.* at 541-42.
211 *Id.*
212 *Id.* at 568.
213 *Id.* (citations omitted).

discussed in open court.[214] In that case, Oklahoma law imposed confidentiality on juvenile proceedings and records unless a judge specifically authorized their publication. Again, the Supreme Court held that the gag order violated the First Amendment because the "widely disseminated information [had been] obtained at court proceedings which were in fact open to the public."[215] In short, once the court system disclosed the information to the public, it could not be recalled.

The most extreme manifestation of the disclosure principle, however, can be seen in *Florida Star v. B.J.F.*, a case involving Florida's prohibition on publishing the names of rape victims.[216] In that case, the sheriff's office maintained a media room where it placed press releases and crime reports. The authorities were supposed to redact the names of rape victims from these documents but on this occasion, the sheriff's office failed to do so.[217] A "reporter–trainee" working for the *Florida Star* newspaper copied the entire report of B.J.F.'s rape and gave it to one of the paper's reporters, who in turn included the victim's name in a short write-up of the crime.[218] The rape victim sued, citing the state law that prohibited publication of a rape victim's name.[219] When the Supreme Court received the case, however, it held that the newspaper was protected by the First Amendment because, "where the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release."[220] It continued: "The government's issuance of such a release, without qualification, can only convey to recipients that the government *considered dissemination lawful, and indeed expected the recipients to disseminate the information further*."[221]

What makes *Florida Star*'s articulation of the disclosure principle so extreme is that the facts of the case so clearly indicate the information was never intended for public disclosure. The authorities intended to redact the victim's name, the *Florida Star*'s reporter–trainee was the only one to pick up and read the unredacted report, a sign in the media room where the press releases and crime reports were kept warned of the state prohibition against

---

214 Okla. Publ'g Co. v. Dist. Court, 430 U.S. 308, 309-10 (1977).

215 *Id.* at 310.

216 Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989).

217 *Id.* at 526-28.

218 *Id.*

219 *Id.* at 528.

220 *Id.* at 535, 540-41.

221 *Id.* at 538-39 (emphasis added); *see also* Boettger v. Loverro, 587 A.2d 712, 718 (Pa. 1991) ("[W]hen the assistant district attorney filed a copy of the transcript with the Clerk of Courts . . . it went in the public domain, irrespective of whether or not the action of the assistant district attorney was inadvertent.").

publishing a rape victim's name, and the reporter was aware of this prohibition.[222] Despite these facts, the Supreme Court characterized the release as an official disclosure sufficient to demonstrate that the government believed that "dissemination [was] lawful, and indeed expected the recipients to disseminate the information further."[223] Disclosure was disclosure, and the Court held that the full protection of the First Amendment applied. To conclude otherwise, the Court explained, would be to impose on the media "the onerous obligation of sifting through government press releases, reports, and pronouncements to prune out material arguably unlawful for publication,"[224] which would invite the ill of "overdeterrence."[225]

The implications of the disclosure principle for retroactive classification are significant. If even the limited, accidental release in *Florida Star* counts as government disclosure, then so must the examples of retroactive classification discussed in this Article. A FOIA response sent to just a single person, a document the government published online or entered into the congressional record—each of these would trigger the full protections of the First Amendment. And, under these precedents, an Espionage Act prosecution based on retroactive classification would face strict scrutiny.

This is not to say that an Espionage Act prosecution would necessarily fail strict scrutiny. Depending on the circumstances of the case, the government could demonstrate a compelling state interest and narrow tailoring in enforcing retroactive classification. But the government would face two obstacles. First, it would have to explain how a document important enough to create a compelling state interest could have been disclosed in the first place.[226] Second, the government would have to show how prosecuting someone *after* publication would do any good in keeping the document secret, much less qualify as the least restrictive method of preserving the document's confidentiality. After all, as *Cox Broadcasting*, *Nebraska Press*, *Oklahoma Publishing*, and *Florida Star* show, the government always has a less restrictive method for protecting a document's confidentiality: it can be more careful at the outset about what information it releases.

---

222 Oral Argument at 5:28, 29:28, Fla. Star v. B.J.F., 491 U.S. 524 (1989) (No. 87-0329), *available at* http://www.oyez.org/cases/1980-1989/1988/1988_87_329.

223 *Fla. Star*, 491 U.S. at 538-39.

224 *Id.* at 536.

225 *Id.* at 535.

226 This could perhaps be accomplished by showing that the document was not important at the time that it was disclosed, but has since become so.

The above analysis shows that a prosecution based on the disclosure of retroactively classified documents would face hurdles even higher than a prosecution involving traditionally classified documents. Those statutory and constitutional challenges might appear to eliminate the threat of the Espionage Act being used to enforce retroactive classification. But the case against such a retroactive-classification prosecution is not as open-and-shut as the above analysis suggests. Part III explains why.

III. RETROACTIVE CLASSIFICATION IN OTHER AREAS OF THE LAW

Despite daunting statutory and First Amendment hurdles, an Espionage Act conviction is not as far-fetched as it may appear. Lower courts have struggled with their own versions of retroactive classification in a wide range of substantive legal areas. Part III examines such cases and argues that, in light of the courts' struggles in resolving them, retroactive classification may well have teeth after all. This Part also situates retroactive classification in a larger debate about the government's ability to control information it has placed in the public record—a debate that asks whether someone can be punished for publishing information that the government has itself disclosed. Scholars tend to assume that the government cannot control information that it has placed in the public record, but this Part challenges that assumption.[227]

At first blush, retroactive classification seems *sui generis* and absurd. Indeed, many doctrines would scoff at the claim that information, once revealed, could be treated as secret. In trade secret law, for example, once information is disclosed to the public—even inadvertently—it no longer receives trade secret protection.[228] The Fourth Amendment is just as

---

227 *See* Edward Lee, *The Public's Domain: The Evolution of Legal Restraints on the Government's Power to Control Public Access Through Secrecy or Intellectual Property*, 55 HASTINGS L.J. 91, 209 (2003) (stating that "[w]hatever lies in the public's domain belongs, by definition, to the people and is, therefore, off-limits to government control," but also noting recent challenges to this view); *id.* at 136-37 ("[T]he function of the public domain . . . is to act as a restraint on government power."); Smolla, *supra* note 170, at 1168-69 ("[The government] may not adopt the simple expedient of penalizing the press for using the material given to it . . . . If the journalist is handed information, the journalist may examine it and publish it."); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1204 (2002) ("[G]overnments cannot establish post-access restrictions on the disclosure or use of information that is publicly available. Once the information is made available to the public, the *Florida Star* case prohibits a state from restricting use."). *See generally* Mart, *supra* note 9.

228 *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information . . . his property right is extinguished." (citations omitted)).

demanding, holding that once a person discloses information to a third party he has "no legitimate expectation of privacy in information he voluntarily turns over."[229] The law concerning testimonial privileges takes the same approach. The marital and attorney–client privileges, for example, are destroyed when secret information is disclosed to a third party.[230]

Scratch a little deeper, however, and analogies to retroactive classification abound. Retroactive classification of sorts has been used to protect atomic secrets, Social Security numbers, police officers' home addresses, rape victims' names—even after *Florida Star*—and tax return information, to name just a few examples.[231] In these cases, the courts have grappled with whether the government may disclose sensitive information in the public record and then punish those who republish the information.[232] Despite the strident language of *Bartnicki* and *Florida Star*, this turns out to be a surprisingly difficult question that some courts have answered in the affirmative and others in the negative. The cases discussed below suggest that, confronted with a prosecution based on retroactive classification, a court may well allow the prosecution to go forward.

A. *"Born Classified" and the Atomic Bomb*

The "born classified" doctrine holds that information related to nuclear weapons can be classified even if the government previously disclosed the information or the information originated from private sources. The standard-bearer for this doctrine is *United States v. Progressive*,[233] a case dealing with a magazine article that described how to build an atomic

---

229 Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

230 *See* Cal. Evid. Code § 912 (2014); John T. Hundley, Annotation, *Waiver of Evidentiary Privilege by Inadvertent Disclosure—State Law*, 51 A.L.R. 5th 603, 636-38 (1997).

231 Commercial speech is not the focus of this Article, but it is worth noting that some states have attempted to limit uses of public records. Despite commercial speech's diminished First Amendment protections, these statutes have often not fared well under judicial review. *See, e.g.*, R.I. Ass'n of Realtors, Inc. v. Whitehouse, 199 F.3d 26, 28 (1st Cir. 1999) (affirming district court's decision to strike down Rhode Island statute prohibiting "information obtained from public records" from being used "to solicit for commercial purposes"); Pellegrino v. Satz, No. 98-7356, 1998 WL 1668786 at *1 (S.D. Fla. Dec. 22, 1998) (striking down Florida statute that prevented use of police reports "for any commercial solicitation of the victims"). *But cf.* L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 34-35, 40 (1999). *See generally* Solove, *supra* note 227, at 1169-70 (giving a brief overview of some commercial use restrictions).

232 *See* Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1127 (2005) (touching on several of these prohibitions in addressing whether the First Amendment protects crime-facilitating speech, but not addressing the public-record aspect of these cases); *see also* Smolla, *supra* note 170, at 1160 (discussing the courts' treatment of information obtained by the press in open court proceedings).

233 467 F. Supp. 990 (W.D. Wis. 1979).

bomb.[234] In 1979, the Justice Department sought an injunction to prevent the publication of this controversial article.[235] The magazine insisted that all of the information in the article was "already in the public domain and readily available to any diligent seeker," so it should not be restrained from publication.[236] The government countered that, even if all the information were already public—a fact that the government disputed—the synthesis of this information should still be classifiable under the Atomic Energy Act because it threatened "immediate, direct and irreparable harm to the interests of the United States."[237] With great trepidation, the district judge attempted to balance the "honored" values of the First Amendment against a risk of "sufficient destructive potential to . . . endanger the right to life itself."[238] In the end, the judge issued the injunction against publication, though he assured the parties that the case would "undoubtedly go to the Supreme Court."[239]

United States v. Progressive has come to stand for the lengths to which the government may go in controlling information in the public domain. While scholarly accounts of the case have focused on the injunction order discussed above, the court's little-discussed ruling on a motion to reconsider is more relevant to retroactive classification.[240] Unlike the injunction order, the ruling on the motion to reconsider discussed documents that were actually retroactively classified. According to the court, two documents containing technical information about nuclear weaponry were errantly declassified by the government and placed in the public section of the Los Alamos Scientific Library, where they remained for years.[241] Under *Florida Star*'s disclosure principle, the government's inadvertent disclosure of these documents would have placed them irretrievably in the public record.[242] But the district court concluded the opposite: "[F]rom a legal point of view, the government's error in inadvertently declassifying [the documents] did not

---

234 *See* Howard Morland, *The H-Bomb Secret: How We Got It—Why We're Telling It*, PROGRESSIVE, Nov. 1979, at 3.

235 Walter Pincus, *Article on H-Bomb Went to Officials 3 Times Before U.S. Acted*, WASH. POST, Mar. 11, 1979, at A1.

236 *Progressive*, 467 F. Supp. at 993.

237 *Id.* at 991, 993; *see also* 42 U.S.C. § 2014(y) (2012) (defining the scope of the "Restricted Data" covered by the Atomic Energy Act).

238 *Progressive*, 467 F. Supp. at 992, 995. Hours before granting the injunction, the judge instructed the parties to consider mediation one last time. *Id.* at 997.

239 *Id.* at 996.

240 United States v. Progressive, Inc., 486 F. Supp. 5 (W.D. Wis. 1979).

241 *Id.* at 7.

242 *See supra* notes 216-220 and accompanying text.

move these documents into the public domain."[243] The *Progressive* case thus provides an example of a court's endorsing retroactive classification. And if retroactive classification could support a prior restraint, as it did in this case, that is all the more reason to believe it could support a post-publication prosecution, which is generally thought to be easier to obtain.[244]

But whatever lessons about retroactive classification can be drawn from *Progressive* are necessarily tentative because the case became moot before the court of appeals or the Supreme Court could decide it. While the magazine's appeal was pending before the Seventh Circuit, another publication printed the most sensitive information in the contested article.[245] Once that information was printed, the Justice Department asked for the injunction to be rescinded.[246] The *Progressive* case may thus undermine the theory behind retroactive classification because, as soon as the information was publicly available, the government ceased trying to keep it secret.

Drawing a lesson from this case is further complicated by the fact that the nuclear bomb is an extreme example. The district judge was convinced that an error in favor of the First Amendment could mean the end of all life on earth.[247] Reading the opinion, one senses that practically any doctrine, no matter how protective of speech, would have given way before the court's fear of atomic incineration.

Thus, when considering retroactive classification's viability, it might be better to consider analogies to less extreme doctrines and circumstances, including those dealing with "important" interests, "compelling" interests, and even "interests of the highest order," but not interests as pressing as the ones posed by a potential nuclear Armageddon. As it turns out, there are quite a few such analogies.

---

243 *Progressive*, 486 F. Supp. at 8 (internal quotation marks omitted).

244 *See, e.g.*, Michael Coenen, *Of Speech and Sanctions: Toward a Penalty-Sensitive Approach to the First Amendment*, 112 COLUM. L. REV. 991, 1017 (2012); Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 899 (2008). The Invention Secrecy Act provides another example of a statute that allows information, once public, to become secret. The Act allows the government to make a patent application secret "[i]f . . . the publication or disclosure of the invention by the publication of an application . . . would be detrimental to the national security." 35 U.S.C. § 181. If the applicant reveals the information anyway, he can face criminal charges. *Id.* §§ 182, 186.

245 Charles R. Babcock, *U.S. Ending Suit Against Magazine*, WASH. POST, Sept. 18, 1979, at A1.

246 *Id.*

247 *See* United States v. Progressive, Inc., 467 F. Supp. 990, 996 (W.D. Wis. 1979).

B. *Social Security Numbers*

The best analogy to retroactive classification may come from *Ostergren v. Cuccinelli*, a case involving the republication of Social Security numbers that were revealed in public records.[248] In the 1990s, officials in Virginia and other states began providing online access to property and other official records.[249] However, the move online came with a cost: many of the records contained Social Security numbers, which could be used to facilitate identity theft.[250] In Virginia alone, the local clerks of court posted 200 million records online, an estimated three percent of which contained Social Security numbers.[251]

Privacy advocate Betty Ostergren began lobbying elected officials in Virginia and other affected states to remove the records from the Internet until the Social Security numbers could be redacted.[252] When state and local officials in Virginia refused to take the records down, Ostergren took a different approach. She tracked down public records revealing elected officials' Social Security numbers and posted the records on her website.[253] The Virginia legislature did not look favorably on this campaign and in 2008, amended its privacy statute to make Ostergren's actions illegal.[254] The state attorney general announced that if Ostergren persisted, she would be prosecuted.[255] The threat prompted Ostergren to request that the law be enjoined on First Amendment grounds.[256]

The case raises questions similar to those raised by retroactive classification. As in retroactive classification, the government in Ostergren's case disclosed sensitive information to the public and then sought to prevent its further dissemination by prohibiting republication.[257] The statute prohibiting publication of the Social Security numbers imposed an obligation of confidentiality on members of the public just as retroactive

---

248 615 F.3d 263 (4th Cir. 2010).

249 *Id.* at 266-67.

250 *Id.* at 267.

251 *Id.* at 267, 285.

252 *Id.* at 268.

253 *Id.* The website still displays the Social Security numbers of Jeb Bush, Porter Goss, Tom Delay, and many other officials inside and outside of Virginia. *See Examples of "Public" Records with SSNs . . . Including Legislators' and Clerks of Circuit Courts*, VA. WATCHDOG, http://www.opcva.com/watchdog/RECORDS.html (last visited Feb. 27, 2015), *archived at* http://www.perma.cc/S45R-GT2K.

254 VA. CODE ANN. § 59.1-443.2(A)(1) (2014); *Ostergren*, 615 F.3d at 266, 269.

255 *Ostergren*, 615 F.3d at 269.

256 *Id.* At least one person has been convicted for using Ostergren's website to commit identity theft. *Id.*

257 While the government did not author these records, it did disclose the Social Security numbers by making the unredacted records available.

classification does in the national security context. And, as with retroactive classification, the ban on republishing the Social Security numbers went into effect even though the information remained easily accessible in the public domain.

When Ostergren's case made it to the Fourth Circuit, the court held that Virginia's Social Security number statute was unconstitutional.[258] The court's reasoning is significant because it both supports and undermines the rationales underlying retroactive classification. Virginia argued that publishing Social Security numbers was not protected speech and, in the alternative, that "the state interest in preserving citizens' privacy . . . justifie[s] barring Ostergren's speech."[259] Ostergren invoked *Daily Mail Publishing*, *Florida Star*, and *Bartnicki*, among other First Amendment precedent, in arguing that strict scrutiny should apply.[260] The Fourth Circuit held that, in some cases, publishing Social Security numbers would not receive First Amendment protection, but in Ostergren's case, the Social Security numbers were "integral to her message" about government privacy practices—"[i]ndeed, they *are* her message."[261]

The court then applied strict scrutiny, asking whether the statute was "narrowly tailored to a state interest of the highest order."[262] On the state interest prong, the Fourth Circuit said that protecting Social Security numbers "may certainly constitute 'a state interest of the highest order,'" though it declined to decide whether it constituted one in this case because it found the statute not narrowly tailored.[263] This dicta is useful for our purposes because, if protecting Social Security numbers can qualify as a state interest of the highest order, then protecting the government's top secrets could certainly qualify as well.

It was the narrow tailoring analysis, however, that proved key to the Fourth Circuit's decision. Again, this analysis is relevant to our inquiry because it both supports and undermines the case for retroactive classification. It supports retroactive classification insofar as the court rejected Ostergren's claim that once the government disclosed information to the public, the government was powerless to control the information's further dissemination.[264] The Fourth Circuit approvingly cited an exchange from the proceedings below where the district court challenged Ostergren's

258 *Ostergren*, 615 F.3d at 286-87.
259 *Id.* at 270.
260 *Id.* at 273-76.
261 *Id.* at 272.
262 *Id.* at 275.
263 *Id.* at 280.
264 *Id.* at 281.

use of the disclosure principle.[265] In that exchange, the district court asked what would happen if the federal government accidentally disclosed all Social Security numbers in the country.[266] Ostergren insisted that, under *Cox Broadcasting*, the government could not prevent the republication of those numbers.[267] The court forcefully disagreed:

> Are you saying that Congress couldn't come in with a statute and say, you can't replicate these things? What they would do is try to take the system that had gone wrong, fix what they can fix, knowing that there are people who have already gotten into the database that spilled accidentally, but knowing the damage is somewhat limited and saying we are going to stop it right here, and the way we're going to stop it is making it unlawful for you, anybody, to take this information that's been accidentally spilled and use it.[268]

The hypothetical remedy the court suggested—barring the reproduction of the leaked numbers—sounds just like retroactive classification. While *Florida Star* and its kin hold that disclosure is disclosure and that disclosed information cannot be further controlled, the Fourth Circuit seems to endorse a different view. Indeed, it accepted as a given that the government could claw back information that it inadvertently released, at least in the hypothetical concerning Social Security numbers. This clawback of information is the reason retroactive classification developed: to address errant declassification and disclosure of classified information. In this respect, *Ostergren* supports the idea that retroactive classification is a legitimate governmental power.

However, there is also much within the opinion that can be seen to oppose retroactive classification. After all, the Fourth Circuit held that the statute that allowed this analogue to retroactive classification was not narrowly tailored enough to be constitutional.[269] The court's central concern was the constitutionality of forcing Ostergren to respect the confidentiality of these records "when Virginia currently makes those same records available . . . without having redacted [Social Security numbers]."[270] The court put much emphasis on the fact that fifteen counties did not even finish running the redaction software that had proven largely successful in

---

265 *Id.*

266 *Id.*

267 *Id.* According to Ostergren, *Cox Broadcasting* stands for the proposition that "when the Government makes something available, they are responsible for controlling the dissemination of information. They can't make someone else do it." *Id.* at 281 n.14.

268 *Id.* at 281 n.14.

269 *Id.* at 285-87.

270 *Id.* at 286.

erasing Social Security numbers from the online records.[271] The court also found that, rather than prosecuting republication, a more narrowly tailored solution to the privacy problem would be to "direct[] clerks not to make land records available [online] . . . until after [Social Security numbers] have been redacted."[272] The Fourth Circuit concluded that, in light of the state's own lackadaisical approach to fixing the problem, punishing Ostergren's speech was not the least restrictive alternative—a requirement of strict scrutiny.[273]

This narrow tailoring analysis likely previews an argument the defense would make in a retroactive-classification prosecution. The defendant would argue that there must be a better way to protect classified data. Indeed, the defense would emphasize the well-documented sloppiness of the classification system, a system that "leaks like a sieve"[274] and that a Senate committee recently declared was "not trusted on the inside any more than it is on the outside."[275] Following *Ostergren*, a court reviewing a retroactive-classification prosecution might well conclude that a more narrowly tailored method for preventing the release of government secrets would be for the government to take proper care of the secrets in the first place. This narrow-tailoring analysis would undermine the viability of a retroactive-classification prosecution.

In the end, however, while the Fourth Circuit held that Ostergren could not be punished, what is significant is how close the decision was.[276] If Virginia had been more diligent in redacting the records, the statute may well have withstood First Amendment scrutiny.[277] And, in a retroactive classification case, the federal government would be able to show that it had been more diligent in protecting its secrets than Virginia was in protecting Social Security numbers. Notwithstanding some high-profile failures in the classification system, the government's substantial efforts to protect national security secrets could convince a court that enforcing the retroactive classification rules is the least restrictive means of protecting government secrets.

---

271 *Id.*

272 *Id.*

273 *Id.* at 286-87.

274 *See, e.g.*, Pozen, *supra* note 134, at 513.

275 Preserving American Access to Information Act, S. 1464, 113th Cong. § 2 (2013).

276 *Ostergren*, 615 F.3d at 290.

277 *Id.* at 286-87.

C. *Police Officer Personal Information, Unexecuted Arrest Warrants, and Rape Victims' Names*

Other analogies to retroactive classification can be found in the criminal justice system, including instances where the government attempts to restrict the publication of information that it has already disclosed by its own hand. The Supreme Court cases discussed in Section II.B largely concern this type of information, such as rape victims' names and juvenile defendants' identities. However, even after the Supreme Court's pronouncements about the right to publish such information where it is lawfully obtained, lower courts continue to wrestle with how much the government can do to protect information in the public record.

Both Washington and Florida have criminalized the publication of police officers' phone numbers, home addresses, and other personal information.[278] In both states, websites critical of the police managed to locate this sensitive information in public records and post it online.[279] When the websites were threatened with legal action, they brought First Amendment challenges. The district courts concluded in both cases that publication of such information, when derived from public records, merited First Amendment protection.[280] Significantly, in striking down both statutes, the courts emphasized that the government had been the one responsible for making this information part of the public record. As the Washington district court held, "when the government itself injects personal identifying information into the public domain, it cannot credibly take the contradictory position that one who compiles and communicates that information offends a compelling state interest."[281] The Florida district court employed the same reasoning.[282] These police-information cases follow the contours of *Cox Broadcasting* and *Florida Star* in holding that, once the government discloses information in a public record, it cannot control the information's further dissemination. Under this reasoning, a retroactive-classification prosecution would not survive First Amendment scrutiny.

---

278 Washington criminalized publication with intent "to harm or intimidate" of an officer's "residential address, residential telephone number, birthdate, or social security number." WASH. REV. CODE § 4.24.680 (2002); *see also* Sheehan v. Gregoire, 272 F. Supp. 2d 1135, 1139 (W.D. Wash. 2003). Florida criminalized malicious publication of an officer's home address or telephone number. FLA. STAT. § 843.17 (2013); Brayshaw v. Tallahassee, 709 F. Supp. 2d 1244, 1247 (N.D. Fla. 2010).

279 *Brayshaw*, 709 F. Supp. 2d at 1247; *Sheehan*, 272 F. Supp. 2d at 1139 & n.2, 1142, 1144-45.

280 *See, e.g.*, *Brayshaw*, 709 F. Supp. 2d at 1249.

281 *Sheehan*, 272 F. Supp. 2d at 1147.

282 *Brayshaw*, 709 F. Supp. 2d at 1250.

Some state courts adopted the same position in different contexts. In *State v. Stauffer Communications*, the Kansas Supreme Court announced a categorical ban on punishing those who publish facts in the public record.[283] In that case, the First Amendment protection was apparently so strong that the court did not even perform the strict scrutiny analysis.[284] *Stauffer Communications* involved a Kansas statute that made it a crime to reveal the contents of an arrest warrant prior to the warrant's execution.[285] Nonetheless, the unexecuted warrants were available for public inspection in the clerk of the court's office.[286] A reporter used these unexecuted warrants to obtain and publish the names of two murder suspects, both of whom fled the state.[287] The reporter was convicted of violating the statute, but the Kansas Supreme Court threw out the conviction.[288] Relying in part on *Cox Broadcasting*, the court held that the U.S. Constitution and the Kansas Bill of Rights "forbid the imposition of criminal sanctions for truthful reporting of facts gleaned from public records."[289] The government's disclosure of the information in a public record thus protected all later disclosures from punishment.

Even as the Kansas Supreme Court went beyond *Cox Broadcasting* and *Florida Star* in announcing a categorical bar to such prosecutions, the Colorado Supreme Court went against those cases in upholding a prior restraint in the rape case against basketball star Kobe Bryant.[290] In *People v. Bryant*, a court reporter transcribed the proceedings of an in camera rape-shield hearing and marked the transcript confidential.[291] The reporter then accidentally sent the transcripts to an email distribution list that included media organizations, such as the Associated Press, ESPN, and the *Denver Post*.[292] When the error was detected—and before the news organizations could publish the information—the trial court issued an injunction barring the media from publishing any information derived from the transcripts.[293] A majority on the Colorado Supreme Court upheld the injunction.[294]

---

283 592 P.2d 891, 897 (Kan. 1979).
284 *Id.* at 896.
285 *Id.* at 893.
286 *Id.*
287 *Id.*
288 *Id.* at 897.
289 *Id.* at 894-95.
290 *See* People v. Bryant, 94 P.3d 624, 627 (Colo. 2004).
291 *Id.* at 627.
292 *Id.* at 625-27.
293 *Id.* at 626.
294 *Id.* at 638.

This case is relevant to the study of retroactive classification because it shows the malleability of the line between public and secret. In distinguishing this case from *Florida Star*, another case involving an inadvertent disclosure of information concerning a rape victim, the Colorado Supreme Court insisted that the information here was still private, even after the reporters received it. "[I]t is absolutely essential to our analysis that these transcripts are still private," the court explained.[295] Elsewhere, the court stated that the "information has not yet become public"[296] and, again, that "the contents of the *in camera* transcribed proceedings were not publicly available."[297]

How can a document emailed to reporters at seven news organizations, themselves members of the public, still be private? On the one hand, it is clear what the court was trying to say: the information could still be considered secret, even after the errant mailing, because it had not been disclosed to a mass audience—the prior restraint had kicked in before the media organizations could publish the information. On the other hand, this definition of private seems rather strained. The transcripts were in the hands of journalists, who were themselves members of the public and who represented an audience of many millions more. Arguably, disclosing the documents to those reporters meant that the information was no longer secret.

Clearly, though, the Colorado Supreme Court did not agree. Its reasoning rejects the all-or-nothing approach to public disclosure. The *Bryant* court asserted that a document disclosed to members of the public could still be considered private if the members of the public who possessed the document—in this case, the media—can be intimidated out of further disseminating the information.[298] This is the same logic relied upon by retroactive classification: information, once disclosed to the public, can be made secret again simply by threatening those in possession of it with prosecution if they disclose it further. The fact that the Colorado Supreme Court embraced this reasoning lends support to the idea that other courts might be willing to do the same in the context of retroactive classification, especially when the sensitive information concerns a matter of national security.

---

295 *Id.* at 636.
296 *Id.* at 635 n.10.
297 *Id.* at 635.
298 *Id.* at 638.

D. *Tax Return Information*

The Internal Revenue Code provides another analogy supporting retroactive classification. The tax code makes it a felony for anyone "to whom any return or return information . . . is disclosed . . . to print or publish in any manner not provided by law any such return or return information."[299] There are numerous cases involving Internal Revenue Service (IRS) agents who leak information to reporters,[300] but our retroactive-classification inquiry is not concerned with such leaks. Instead, the analogy to retroactive classification arises in cases where the government discloses tax return information through official channels, either in court or in response to a FOIA request, and that disclosure then becomes the basis for further disclosures. In these cases, courts must grapple with whether the re-publication of tax return information contained in the public record can still be prosecuted.

In the first scenario, the circuits are split on whether an IRS agent can be punished for disseminating tax return information *after* that information has been documented in public court records. The Tenth Circuit held that such actions by an IRS agent can be punished, noting that "the fact that [the agent] had given prior 'in court' testimony . . . which likely removed [the pieces of information] from their otherwise 'confidential' cloak" does not insulate the agent from liability if he later on discloses that information.[301] The Ninth Circuit reached the opposite conclusion, holding that, "[o]nce tax return information is made a part of the public domain, the taxpayer may no longer claim a right of privacy in that information."[302] The Seventh Circuit took yet another approach, holding that the court must look to the "immediate source" of the information to determine if there is a right to privacy.[303] Under this approach, if the "immediate source is a public document lawfully prepared by an agency that is separate from the Internal Revenue Service and has lawful access to tax returns"—a document such as a tax court opinion—then the agent cannot be punished for republishing such information.[304]

---

299 I.R.C. § 7213(a)(3) (2012).

300 *See, e.g.*, *In re* Seper, 705 F.2d 1499, 1500, 1502 (9th Cir. 1983); Erhard v. United States, No. 93-0725, 1994 WL 196755, at *1 (D.D.C. Mar. 29, 1994).

301 Rodgers v. Hyatt, 697 F.2d 899, 906 (10th Cir. 1983). In his defense, the IRS agent argued that "there can be no reasonable expectation of privacy to matters which are of public record." *Id.* at 902.

302 Lampert v. United States, 854 F.2d 335, 338 (9th Cir. 1988).

303 Thomas v. United States, 890 F.2d 18, 21 (7th Cir. 1989).

304 *Id.*

The question raised by these cases is the one at the core of retroactive classification: Can the government restrict the dissemination of information that it has placed in a public record? In answering yes, the Tenth Circuit lends support to retroactive classification by holding that, even if the information is available to the public, the IRS officer can still be punished for republishing it. In answering no, the Ninth Circuit opposes retroactive classification by holding that the tax information cannot be controlled once it is in the public record. And the Seventh Circuit, in looking to the "immediate source," only complicates the issue by requiring courts to judge whether the immediate source is a public document or a confidential one. The trouble is that a retroactively classified document is both public and confidential. The fact that the courts are divided on this question makes the challenges to a retroactive-classification prosecution seem less insurmountable.

Arguably, a tighter analogy to retroactive classification exists in the second scenario, where tax information is accidentally disclosed in response to a FOIA request. The question in this scenario is whether the recipient of this tax information can be prosecuted for republishing it. This question arose in 2012 when the IRS responded to a FOIA request by producing confidential tax documents belonging to several conservative groups that had applied for tax-exempt status.[305] When ProPublica, the news organization that made the FOIA request, asked the IRS why it had released these documents, the IRS admitted there had been a mistake.[306] The IRS then threatened to prosecute ProPublica under section 7213(a)(3) of the Internal Revenue Code if the reporters published the tax information.[307] ProPublica published the information nonetheless, and no prosecution ensued. But this episode shows yet another instance in which the government has invoked a version of retroactive classification. Even though the IRS had disclosed the information through official FOIA channels, the agency apparently felt legally entitled to threaten prosecution for republication.

---

305 Kim Barker & Justin Elliott, *IRS Office That Targeted Tea Party Also Disclosed Confidential Docs From Conservative Groups*, PROPUBLICA (May 13, 2013), http://www.propublica.org/article/irs-office-that-targeted-tea-party-also-disclosed-confidential-docs, *archived at* http://perma.cc/XM72-N66K.

306 *Id.*

307 *Id.*; *see* Email from Kim Barker, Reporter, ProPublica, to author (Jan. 7, 2014, 3:11 PM) (on file with author).

E. *Court Records and Transcripts*

The judiciary also employs a form of retroactive classification when it seals court records and transcripts containing information that has already been disclosed in open proceedings. Certain types of sealing actions are specifically permitted by statute. Many states, for instance, have allowed people to petition for the removal of their Social Security numbers and bank account information from court records,[308] or for the sealing and expungement of old criminal court records.[309]

Outside of these specific statutory provisions, however, courts have been reluctant to retroactively seal information presented in open court, especially once that information has been widely disseminated.[310] The Second Circuit made this point in a case where a judge's published order improperly revealed confidential settlement information: "[H]owever confidential it may have been beforehand, subsequent to publication it was confidential no longer. . . . We simply do not have the power, even were we of the mind to use it if we had, to make what has thus become public private again."[311] Similarly, the Fourth Circuit overturned a judicial gag order prohibiting two reporters from publishing grand jury information that a trial judge had inadvertently disclosed in open court.[312] These cases are in line with the Supreme Court's decisions in *Nebraska Press* and *Oklahoma Publishing*, both of which held that information, once disclosed in court, cannot be suppressed.[313]

Nonetheless, some courts do allow retroactive sealing of records, even outside the statutory provisions. Retroactive sealing has been used to redact important information blurted out during testimony or otherwise incautiously revealed. A Delaware court, for example, retroactively sealed portions of a transcript when a witness testified about the valuation of a family-owned company—a valuation that had been subject to a

---

308 *See, e.g.*, FLA. STAT. ANN. § 119.0714 (West 2014); MO. S. CT. OPERATING R. 2.05 (West 2014); TEX. GOV'T CODE ANN. § 552.147 (West 2013).

309 *See, e.g.*, COLO. REV. STAT. ANN. § 24-72308 (2014); 18 PA. CONS. STAT. ANN. § 9122 (2014); 20 ILL. COMP. STAT. 2630/5.2 (2014).

310 *See* Nat'l Polymer Prod., Inc. v. Borg-Warner Corp., 641 F.2d 418, 421 (6th Cir. 1981) ("[W]e begin with the well-established principle of American jurisprudence that the release of information in open trial is a publication of that information and, if no effort is made to limit its disclosure, operates as a waiver of any rights a party had to restrict its further use."); *see also, e.g.*, Littlejohn v. Bic Corp., 851 F.2d 673, 680 (3d Cir. 1988); Level 3 Commc'ns, LLC v. Limelight Networks, Inc., 611 F. Supp. 2d 572, 588 (E.D. Va. 2009); Flohrs v. Eli Lilly & Co., No. 12-2439, 2013 WL 4773515, at *2 (D. Kan. 2013).

311 Gambale v. Deutsche Bank AG, 377 F.3d 133, 144 (2d Cir. 2004).

312 *See In re* Charlotte Observer, 921 F.2d 47, 48-50 (4th Cir. 1990).

313 *See supra* notes 209-215 and accompanying text.

confidentiality order.[314] In ordering the retroactive sealing, the court noted the "almost metaphysical aura" of the debate "about whether once something is said in open court it becomes part of the public domain."[315] Also figuring into the judge's decision was the fact that everyone present in the courtroom had been a party to the action and was thus already bound by the confidentiality order in the case.[316] If a member of the public had been present, the judge explained, "that might have been the end of the debate."[317]

Another example occurred in a Pennsylvania federal court when a prosecutor filed with the court—and simultaneously posted on his office's website—a sentencing memorandum that revealed confidential grand jury material.[318] The district court sealed the filing, ordered the document removed from the prosecutor's website, and instructed the prosecutor "to make all reasonable efforts to retrieve copies of the document that had been disseminated."[319] Notably, this retroactive sealing occurred despite the fact that news organizations had already received and published the documents.[320]

Retroactive sealing of court records is significant to retroactive classification because it forces courts to think about the definition of the public record. Is a single disclosure of a document, perhaps to only one person, enough to make the information public? The *Florida Star* Court would say yes.[321] Retroactive classification would say no. Indeed, retroactive classification's "reasonably recovered" standard is premised on the assumption that a document is not *really* public until it is widely disseminated.[322] The fact that Social Security numbers and criminal convictions can be removed from court files that have been open to the public for decades suggests the courts believe in a retroactive classification

---

314 *See In re* Trust for Gore, No. 1165, 2010 WL 5644675, at *3 (Del. Ch. Jan. 6, 2011).

315 *Id.* at *3.

316 *Id.*

317 *Id.* Other cases have also allowed retroactive sealing. *See* TriQuint Semiconductor, Inc. v. Avago Techs. Ltd., No. 09-1531, 2012 WL 1432519 at *3 (D. Ariz. Apr. 25, 2012); Richardson v. Mylan Inc., No. 09-1041, 2011 WL 837148 at *2-3 (S.D. Cal. Mar. 9, 2011). *But see* Eugene Volokh, *Lawyer Seeking Order that "Will Compel . . . Volokh to Remove His . . . Blog [Post]"*, VOLOKH CONSPIRACY (Jan. 17, 2011, 9:51 PM), http://www.volokh.com/2011/01/17/lawyer-seeking-order-that-will-compel-volokh-to-remove-his-blog-post, *archived at* http://perma.cc/64VC-3SLK (criticizing a motion to retroactively seal a court filing and stating that, "under the logic of *Florida Star v. B.J.F.*, once a document is made part of the public record, it can't then be withdrawn from the public record and sealed away in a manner that prevents public comment").

318 United States v. Smith, 123 F.3d 140, 145 (3d Cir. 1997).

319 *Id.* at 145.

320 *Id.* at 144-46.

321 *See supra* notes 216-225.

322 *See supra* subsection I.C.3.

of sorts, at least when it comes to their own records. If the courts believed that information, once disclosed in court, becomes irretrievably part of the public record, they would not allow these retroactive redactions and expungements.

But the courts' position is not entirely clear. As noted above, courts generally recoil from some forms of retroactive sealing, such as, for example, blotting out testimony that reveals trade secrets.[323] The important thing to note, however, is that, under the right circumstances, courts are willing to make a secret out of information that has already been released to the public. All in all, then, the cases involving the retroactive sealing of court records tend to support retroactive classification.[324]

F. *Freedom of Information Act*

Freedom of Information Act (FOIA) case law also challenges the idea that a document released to the public necessarily remains public. Under FOIA, agencies may invoke one of nine statutory exemptions to avoid releasing a document.[325] However, the question that often arises in these cases is whether an agency can invoke these exemptions if it has previously released the document to the public. In other words, does the agency's release of a document waive the agency's ability to withhold the document later on? This question touches on the issue at the heart of retroactive classification: can information previously disclosed by the government be treated as secret? Perhaps not surprisingly, the circuits have taken different approaches to this difficult question.[326]

The leading case in the D.C. Circuit, *Cottone v. Reno*, involved a defendant's FOIA request for wiretap recordings that were played at his criminal trial.[327] Under federal law, wiretap recordings are statutorily protected from disclosure,[328] which allowed the Justice Department to

---

323 *See supra* note 310.

324 An important distinction is that retroactive sealing of court records does not affect the legality of republishing the information that one comes across; it affects only the *availability* of that information in the public record. Retroactive classification, on the other hand, bars anyone with possession of the document from disseminating it further.

325 5 U.S.C. § 552(b)(1)–(9) (2012).

326 *See* Sydney Hutchins, Comment, *The Plaintiff's Last Chance: FOIA's Waiver Doctrine* 3-4 (Seton Hall Law eRepository, Paper 126, 2013), *available at* http://erepository.law.shu.edu/student_scholarship/126.

327 193 F.3d 550, 552-54 (D.C. Cir. 1999).

328 *Id.* at 553 (citing Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2521 (1994 & Supp. IV 1998))). The Justice Department also invoked an exemption that protects personal privacy, but the D.C. Circuit remanded that question to the trial court. *Id.* at 556.

invoke the FOIA exemption for material "specifically exempted from disclosure by statute."[329] But the D.C. Circuit held that the exemption could not be used in this case, noting that "materials normally immunized from disclosure under FOIA lose their protective cloak once disclosed and preserved in a permanent public record."[330] At first, this opinion appears to be at odds with retroactive classification because it affirms the idea that disclosed information can no longer be protected. But the opinion supports retroactive classification in acknowledging, later on, that documents in the public record can be "destroyed, placed under seal, or otherwise removed from the public domain," at which point they can be withheld under FOIA.[331] In other words, the public domain can be shrunken, which is the core claim of retroactive classification.

The Second Circuit has dealt with the public-domain doctrine somewhat differently. It stated that an agency cannot invoke a FOIA exemption "if identical information is truly public" because, in such a case, the "exemption cannot fulfill its purposes."[332] But "truly public," for the Second Circuit, was not simply a function of whether the information was preserved in a "permanent public record." Rather, it was a measure of how readily accessible or "freely available" the record was.[333] The Second Circuit would thus allow an agency to invoke an exemption even if the agency had already disclosed the information to the public *and* even if the information was permanently in the public domain, so long as that information was not *easily* accessible. Interestingly, this ease-of-accessibility formulation parallels the "reasonably recovered" standard of retroactive classification in that the more widely disseminated the information, the less the government may do to control it.

The most extreme position on this issue was taken by the Tenth Circuit in *Prison Legal News v. Executive Office for U.S. Attorneys*.[334] This case involved a FOIA request for photos and video documenting the murder of a federal prisoner.[335] The photos and the video were shown at the trials of the two inmates accused of murdering him.[336] The prisoners' rights newsletter

---

329 5 U.S.C. § 552(b)(3) (2012); *Cottone*, 193 F.3d at 552-53.

330 *Cottone*, 193 F.3d at 554.

331 *Id.* at 556.

332 Inner City Press/Cmty. on the Move v. Bd. of Governors of Fed. Reserve Sys., 463 F.3d 239, 244 (2d Cir. 2006) (quoting Niagara Mohawk Power Corp. v. U.S. Dep't of Energy, 169 F.3d 16, 19 (D.C. Cir. 1992)).

333 *Id.* at 243-44, 252.

334 628 F.3d 1243 (10th Cir. 2011).

335 *Id.* at 1246.

336 *Id.*

that requested the materials said that the materials' public showing at the two trials meant that they could not be withheld under FOIA.[337] Nonetheless, the government invoked the exemption that protects against invasions of privacy, asserting that the privacy of the victim's family would be harmed by the materials' release.[338] The Tenth Circuit sided with the government, holding that because the photos and video had been shown only to a small audience (those present at the two trials), they were not made public.[339] The court noted that "the limited nature of the prior public disclosure" meant there was still a protectable privacy interest and, as a result, the photos were not in the public record.[340]

This approach to the public record, and to public court records in particular, further undermines the idea that the public record remains inviolable.[341] In this way, the Tenth Circuit's approach embraces retroactive classification's claim that information the government has placed in the public record can still be treated as secret. These public-domain cases confirm the most basic and controversial premise behind retroactive classification: the public record is not a land-of-no-return.[342]

* * *

Where do all these analogies to retroactive classification leave us? The answer is with much less confidence in the First Amendment's power to fight off a prosecution based on retroactively classified documents. Such a prosecution may have seemed ridiculous in light of *Florida Star*'s disclosure principle, but the issue is not so simple. If the retroactive classification of Social Security numbers, police officers' home addresses, and court records causes courts to question the protections afforded by the First Amendment, then courts would surely question these protections even more in the context of retroactive classification, where national security interests are at stake. From Social Security number protections to FOIA requests, these

337 *Id.*

338 *Id.* at 1253.

339 *Id.* at 1249-50.

340 *Id.* The Tenth Circuit noted that the petitioners had brought only a FOIA claim, not any right-to-court-documents claim. *Id.* at 1253.

341 *See, e.g.*, Golan v. Holder, 132 S. Ct. 873, 891 (2012) (rejecting the claim that the First Amendment "renders the public domain largely untouchable by Congress," in a case challenging Congress's award of copyright protection to certain works in the public domain).

342 As with retroactively sealed court records, FOIA case law is distinguishable from retroactive classification because the former limits only *access* to the information, while the latter also limits the *use* of the information by members of the public. *See supra* note 324.

cases show that the prospect of a successful prosecution based on retroactively classified documents is far more plausible than it first appears.

But it is not just that these cases make retroactive classification a more plausible threat. They also show that the constitutional issues raised by retroactive classification have broad application beyond the realm of national security. Contrary to scholarly assumptions, the fact that information is contained in the public record does not mean it can be published with impunity. Over the years, as the number of documents in the public record and the ability to publish these documents have both rapidly increased, the courts have been quietly renegotiating the limits on the government's power to control public-record-based speech. Retroactive classification, one of the most extreme examples of this power, illustrates the lengths to which the government may go in its attempt to keep information secret. It shows that the government can attempt the impossible. It can reach back in time to make secret a document that it has already disclosed to the world.

IV. SEPARATION OF POWERS

Beyond its implications for speech and press freedoms, retroactive classification also challenges the separation of powers. This Part explores the separation of powers implications of retroactive classification and unpacks the paradox that members of Congress are both more protected from and more vulnerable to retroactive classification than other members of society.

The separation of powers analysis begins with the fact that the executive branch has used retroactive classification to stymie congressional oversight. As noted above, the Pentagon retroactively classified testimony about the missile defense system even though the testimony had been given in an open session of Congress and published in the *Congressional Record*.[343] "[T]he principal effect of the Department's actions," wrote Representatives Henry Waxman and John Tierney, "will be to prevent members of Congress from being able to issue thorough and thoughtful critiques of Administration actions in a public forum."[344] Retroactive classification also prevented the GAO from including key material in its public report about the missile defense system, thus tampering with the integrity of the GAO's analysis.[345]

---

[343] *See supra* notes 25-29 and accompanying text.

[344] Letter from Henry A. Waxman & John F. Tierney, Sens., to Donald Rumsfeld, *supra* note 3, at 4.

[345] *Id.*

Other cases, too, have raised concerns that retroactive classification was preventing members of Congress from doing their jobs. Senator Chuck Grassley said the retroactive classification he experienced in the Sibel Edmonds affair was "as close to a gag order as you get."[346] In another case, Representative Chris Van Hollen worried about retroactive classification's effect on Congress's ability to stay informed. "I think it is amazing," he said, "that an individual working for the government could be criminally liable for providing to a Member of Congress in an unclassified setting a document that had been published by the U.S. Government."[347] In 2007, retroactive classification so upset members of the House that they overwhelmingly voted for a resolution condemning the practice. [348]

Yet, despite their scorn for retroactive classification, it is clear that members of Congress go along with it. What is not clear is why. After all, the Constitution's Speech or Debate Clause protects them from prosecution for anything they say in the course of their legislative duties.[349] If legislators thought retroactive classification was inappropriate in a particular case, they could just read the classified information into the public record without fear of prosecution. Senator Mike Gravel demonstrated this power with aplomb. On the eve of the *Pentagon Papers* decision, while the *New York Times* and *Washington Post* were still enjoined from publishing the top secret documents, Gravel held a late-night meeting of the Senate Subcommittee on Buildings and Grounds and began reading the top secret documents aloud.[350] Gravel ran out of steam at 1:15 AM, at which point he entered the remaining documents into the record, making the documents public for all the world to see.[351] Gravel was not punished. As the Supreme Court held in a case resulting from the incident, the Speech or Debate Clause prevented Gravel from being questioned, much less prosecuted.[352] Thus, the Constitution would appear to empower other members of Congress to disobey retroactive classification.

But members of Congress have not defied retroactive classification, and this may be because the legislative branch's own rules prevent its members

---

346 Lichtblau, *supra* note 31.

347 *Drowning in a Sea of Faux Secrets Hearing*, *supra* note 4, at 160.

348 *See* 153 CONG. REC. H11,577 (daily ed. Oct. 16, 2007).

349 U.S. CONST. art. I, § 6, cl. 1; *see also* Gravel v. United States, 408 U.S. 606, 615-16 (1972).

350 *Gravel*, 408 U.S. at 609.

351 *Id.*; *Sen. Gravel Reads Documents, Ends Report on War in Tears*, L.A. TIMES, June 30, 1971, at A1. If the Supreme Court had approved the prior restraint on the Pentagon Papers, Gravel's actions would have raised the fascinating question of whether someone could be punished for publishing classified information in the *Congressional Record*.

352 *Gravel*, 408 U.S. at 616.

from releasing classified information. For instance, House Rule XXIII requires members to swear an oath of confidentiality before accessing classified information.[353] The internal rules also set out procedures by which members of Congress can go about disclosing classified information. Under House Rule X(11)(g), for example, the Select Committee on Intelligence can disclose "any information in its possession" if it determines that disclosure is in "the public interest."[354] Before that disclosure can happen, however, the Committee must vote to disclose the information and then give the president five days to object.[355] If the president objects and if the Committee still wants to disclose the information, the Committee must seek a vote of the full House or Senate.[356] Any member of Congress who discloses classified information without following this procedure is subject to "censure, removal from committee membership, or expulsion."[357] In 1975, Representative Michael Harrington of Massachusetts transgressed the House classification rules and found himself not only subject to an Ethics Committee investigation but also barred from further access to classified information.[358]

Because of these internal rules, a retroactive classification order binds the legislative branch even though legislators are immune from prosecution. In fact, members of Congress are arguably more constrained by retroactive classification than those outside government because they can clearly be punished for violating the congressional rules. Journalists and members of the public, by contrast, can be punished only if the statutory and constitutional challenges to an Espionage Act prosecution can be overcome, which we have seen is a question open to debate. Because of Congress's internal rules, retroactive classification allows the executive branch to muzzle congressional debate on an issue even when the executive branch is unable to quiet the press. By gagging Congress and interfering with

---

353 JOHN V. SULLIVAN, CONSTITUTION, JEFFERSON'S MANUAL, AND RULES OF THE HOUSE OF REPRESENTATIVES, H.R. DOC. NO. 111-157, at 931 (2d Sess. 2011) ("Before a Member . . . of the House may have access to classified information, the following oath (or affirmation) shall be executed: 'I do solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its Rules.'").

354 *Id.* at 532. The Senate has a similar provision. *See* MATTHEW MCGOWAN, STANDING RULES, ORDERS, LAWS, AND RESOLUTIONS AFFECTING THE BUSINESS OF THE UNITED STATES SENATE, § 81(8), S. DOC. NO. 112-1, at 150-53 (1st Sess. 2011).

355 H.R. DOC. NO. 111-157, at 532-33.

356 *Id.* at 533-36.

357 *Id.* at 536.

358 *Harrington Barred from Secret Data by Panel in House*, N.Y. TIMES, June 13, 1975, at A17; *see also* James J. Kilpatrick, *Should the House Expel a Member? Secrecy: A Matter of Honor*, L.A. TIMES, June 30, 1975, at B5.

congressional oversight, retroactive classification is an affront to the separation of powers.

V. CONCLUDING NOTE AND SUGGESTIONS FOR REFORM

This Article has demonstrated retroactive classification's grave implications for the freedom of speech, the freedom of the press, and the separation of powers. The Article has shown retroactive classification's strange and unsettling ability to make secrets out of information in the public domain. It has also argued that retroactive classification could be enforced by an Espionage Act prosecution. Though such a prosecution might founder on the rocks of the First Amendment, there are reasons to think that it would not. The retroactive classification of sorts taking place in other areas of the law provides reason to believe that, in the context of national security, the courts would allow retroactive classification to be enforced by criminal prosecution. And the possibility of this prosecution is enough to cause someone in possession of retroactively classified documents to return them or, at least, to refrain from publishing them—in short, it is enough to chill speech. Retroactive classification is thus a First Amendment problem. And, as we have seen, it is a separation-of-powers problem when applied to members of Congress.

But retroactive classification also has troubling implications for the integrity of the public record and for the public's ability to make use of that record. What do we do when the government makes a mistake in releasing what should be confidential information, whether its own, another country's, or an individual citizen's? Do we allow it to tear that information out of the public record? Does that answer change if the information still remains available on the Internet, in libraries, or elsewhere in the public domain? Retroactive classification gives a green light to the government's power to control the public domain. This little-known and unconstrained power attacks our basic assumptions about the public record. As the government amasses more and more secrets, and as it gets easier and easier to release them en masse, we will increasingly be faced with the question of how far the government may go to recover this information. The answer, as this Article has shown, will have profound consequences that reach into our everyday lives.

While there are no easy answers to the big questions retroactive classification raises about the government's control of information in the public domain, there are a few reforms that could be employed to address the immediate problems posed by retroactive classification. For example, the president could amend the executive order to include an outright ban on

classifying any document that the government has disclosed to the public. This simple change would wipe out all three types of retroactive classification. It would avoid the metaphysical and constitutional concerns of making a secret out of something in the public domain, while also sending the message that the public may freely make use of the public record without interference from the government—a message that would echo into many other substantive areas of the law.

Far better than an executive order, however, would be for a statute to institute the same reforms. The ban on classifying information disclosed to the public could even include a carve-out for instances of retroactive classification authorized by Congress, such as in the Atomic Energy Act.[359] With or without such carve-outs, congressional intervention is ideal because, no matter how airtight the executive order is in outlawing retroactive classification, the order is only as protective as the whims of the next president. Congressional committees have for years recommended a statutory intervention to reform the classification system, and the Supreme Court has indicated that such an intervention would be constitutional.[360] To the extent retroactive classification offends members of Congress, they have only themselves to blame for not addressing the problem.

But even if Congress cannot get the president's signature on a statutory fix, it could, at the very least, eliminate the separation-of-powers problems by amending the House and Senate rules on the disclosure of classified information. The amended House and Senate rules should simply state that members of Congress are not bound to respect the confidentiality of any classified information that the government has previously disclosed.[361] That would free legislators to disobey retroactive classification without fear of violating the internal rules, thus removing the executive's ability to gag the public deliberations of the House and Senate.

---

359 Pub. L. No. 83-703, 68 Stat. 919 (codified at 42 U.S.C. §§ 2011–2296 (2012)); *see* United States v. Progressive, Inc., 467 F. Supp. 990, 994 (W.D. Wis. 1979) (discussing the restrictions imposed by the Atomic Energy Act of 1954).

360 *See* EPA v. Mink, 410 U.S. 73, 83 (1973).

361 *See supra* notes 353-357 and accompanying text.